CHAPTER 11

Group Theory

11.1. Introduction

Group theory is one of the most important fundamental concepts of modern algebra. Groups arise naturally in various mathematical situations. They have found wide applications in physical sciences and biological sciences particularly in the study of crystal structure, configuration molecules and structure of human genes.

The structure of a group is one of the simplest mathematical structures. Hence, groups may be considered as the starting point of the study of various algebraic structures. In this chapter, we shall define groups and study some of their basic properties.

11.2. Binary Operations

Let G be a nonempty set. Then $G \times G = \{(a, b) : a \in G, b \in G\}$.

If $f : G \times G \to G$, then f is said to be binary operation on G. Thus a binary operation on G is a function that assign each ordered pairs of elements of G an element of G.

The symbols +, ·, 0, * etc. are used to denote binary operations on a set. Thus + will be a binary operation on G if and only if

$a + b \in G$ for all $a, b \in G$ and $a + b$ is unique.

Similarly * will be a binary operation on G if and only if

$a * b \in G$ for all $a, b \in G$ and $a * b$ is unique.

This is said to be the **closure property** of the binary operation and the set G is said to be closed with respect to the binary operation. For example, addition (+) and multiplication (×) are binary operations on the set N of natural numbers, for, the sum and product of two natural numbers are also natural numbers. Therefore, N is closed with respect to addition and multiplication *i.e.*,

$a + b \in N$ for all $a, b \in N$.

$a \times b \in N$ for all $a, b \in N$.

Note that subtraction is not a binary operation on N, for $5 - 9 = -4 \notin N$ whereas $5 \in N$, $9 \in N$. But subtraction is a binary operation on Z, the set of integers, positive and negative.

The most important of describing a particular binary operation * on a given set is to characterize the element $a * b$ assigned to each pair (a, b) by some property defined in terms of a and b.

A binary operation on a set G is sometimes called a composition in G. For finite set, a binary operation on the set can be defined by means of a table, called the **composite table.** Let S be a set with n distinct elements. To construct a table, the elements of S are arranged horizontally in a row called the initial row or 0-row ; these are again arranged vertically in a column, called the initial column or 0-column. The (i, j) th position in the table is determined by the intersection of the ith row and the jth column. For example, let $S = \{a, b, c\}$. Define * on S by the following table.

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

Table 11.1

To determine the elements of S assigned to $a * b$, we look at the intersection of the row labelled by a and the element headed by b. We see that $a * b = b$. Note that $b * a = a$.

Algebraic Structure

A non-empty set together with one or more than one binary operations is called algebraic structure. For example,

$(N, +)$, $(Z, +)$, $(R, +, .)$ are all algebraic structures. Obviously addition and multiplication are both binary operations on the set R of real numbers. Therefore, $(R, +, .)$ is an algebraic structure equipped with two operations.

Laws of Binary Operations

Associative law: A binary operation * on a set S is said to be associative or to satisfy associate property, if and only if, for any elements $a, b, c \in S$

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

Commutative law: A binary operation * on the elements of the set is commutative or to satisfy commutative property, if and only if, for any two elements a and $b \in S$,

$$a * b = b * a.$$

Example 1. The algebraic structure $(Z, +)$, $(Z, .)$, where the binary operations of addition and multiplication on Z are both associative and commutative since addition and multiplication of integers is both associative and commutative.

Example 2. Let $M_2(R)$ be the set of all 2×2 matrices over R *i.e.*,

$$M_2(R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d, \in R \right\}$$

Since addition and multiplication of 2×2 matrices over R is a 2×2 matrix over R, it follows that both + and . is a binary operation on $M_2(R)$. Hence $(M_2(R), +, .)$ is a algebraic structure. Note that + is both associative and commutative and . is associative, but not commutative.

Example 3. The algebraic structure $(Z, -)$ where $-$ denotes the binary operation of subtraction on Z is neither associative nor commutative since

$$3 - (4 - 5) = 4 \neq -6 = (3 - 4) - 5$$

and also

$$3 - 4 \neq 4 - 3$$

Identity Element

An element e in a set S is called an identity element with respect to the binary operation * if, for any element a in S

$$a * e = e * a = a$$

If $a * e = a$, then e is called the **right identity** element for the operation * and if $e * a = a$, then e is called the **left identity** element for the operation *.

Consider any element x of the set Q of rational numbers with respect to the binary operation addition. Obviously, 0 is the identity element, since $0 + x = x + 0 = x$, for every $x \in Q$.

1 is the identity element of Q for the binary operation multiplication, since $1.x = x.1 = x$, for every $x \in Q$.

It is easily seen that for the set N of natural numbers there is no identity element for addition; but 1 is an identity element with respect to multiplication.

Theorem 11.1. The identity element (if it exists) of any algebraic structure is unique.

Proof. Let, if possible, e and e' be two identity elements of the algebraic structure (S, *). Hence $e, e' \in S$.

Now e is an identity element $\Rightarrow e * e' = e'$.

Again e' is an identity element $\Rightarrow e * e' = e$.

But $e * e' = e'$ and $e * e' = e$ $\Rightarrow e = e'$.

Thus the identity element is unique.

Inverse Element

Consider a set S having the identity element e with respects to the binary operation *. If corresponding to each element $a \in S$ there exists an element $b \in S$ such that $a * b = b * a = e$.

Then b is said to be the inverse of a and is usually denoted by a^{-1}. We say a is invertible.

Consider the set R of real numbers which has 0 as the identity element with respect to the binary operation addition. Then, for any $a \in R$, we see that

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

Thus, for any a of the real number set, $(-a)$ is its inverse. This is called the **additive inverse.**

Similarly, for the set Q of rational numbers, 1 is the identity element for the binary operation of multiplication. Then, for any $a \in Q$ we see that

$$a \,.\, (1/a) = (1/a) \,.\, a = 1.$$

Thus, for any a (non-zero) of the rational number set, its reciprocal is its inverse. This is called the **multiplicative inverse.**

Note that the inverse of the identity element is the identity element itself.

Theorem 11.2. For an associative algebraic structure, the inverse of every invertible element is unique.

Proof. Let (S, *) be an associative structure with identity element e. Let x be an invertible element of S. If possible, let y, z be two inverses of x. We then have

$$x * y = e = y * x \quad \ldots (1)$$

$$x * z = e = z * x. \quad \ldots (2)$$

and

Now $(y * x) * z = e * z$ from (1)

$= z$ (e is the identity) $\ldots (3)$

so that $(y * x) * z = z$

and $y * (x * z) = y * e$ from (2)

$= y$ (e is the identity) $\ldots (4)$

Thus $y * (x * z) = y$

Since the composition * is associative, we have

$$(y * x) * z = y * (x * z).$$

Then from (3) and (4), we have $y = z$, showing that the inverse of every invertible element is unique.

Note. It may be noted that while an identity element is the same for all element x in S, an inverse of an element x is determined by the given element x.

From the composite table, one can conclude

(i) **Closure property :** If all the entries in the table are elements of S, then S is closed for *.

(iii) Commutative law : If every row of the table coincides with the corresponding column, then * is commutative on S.

(iv) Identity element : If the row headed by an element a_1 of S coincides with the top row, then a_1 is the identity element.

(v) Inverses : If the identity element e is placed in the table at the intersection of the row headed by a and the column headed by b, then $a^{-1} = b$ and $b^{-1} = a$.

Example 4. Show that the binary operation * defined on $(R, *)$ where $x * y = \max(x, y)$ is associative.

Solution. $(x * y) * z = \max(x, y) * z$

$= \max(\max(x, y), z) = \max(x, y, z)$

Again $x * (y * z) = x * \max(y, z)$

$= \max(x, \max(y, z))$

$= \max(x, y, z)$

Hence $(x * y) * z = x * (y * z)$

Thus, * is associative.

Example 5. Show that the binary operation * defined on $(R, *)$ where $x * y = x^y$ is not associative.

Solution. $(x * y) * z = x^y * z$

$= (x^y)^z = x^{yz}$

Again $x * (y * z) = x * y^z$

$= x^{yz}$

Since $x^{yz} \neq x^{yz}$, $(x * y) * z \neq x * (y * z)$

Thus, * is not associative.

Example 6. Prepare the composition table for multiplication on the element in the set $A = \{1, w, w^2\}$, where w is the cube root of unity. Show that multiplication satisfies the closure property, associative law, commutative law and 1 is the inverse element. Write down the multiplicative inverse of each element.

Solution. Since w is a cube root of unity, $w^3 = 1$. We can operate on various elements and prepare the table as below.

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

From the table we can conclude that

(i) Closure property : Since all the entries in the table are in A so closure property is satisfied.

(ii) Associative law : Since multiplication is associative on complex numbers and A is a set of complex numbers, so multiplication is associative on A.

(iii) Commutative law : Since 1st, 2nd and 3rd rows coincide with 1st, 2nd and 3rd columns respectively, so multiplication is commutative on S.

(iv) Identity element : Since row headed by 1 is same as the initial row, 1 is the identity element.

(v) **Inverses :** Clearly $1^{-1} = 1$; $w^{-1} = w^2$; $(w^2)^{-1} = w$

Example 7. Let the binary operation * be defined on $S = \{a, b, c, d\}$ by means of composite Table 11.2.

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

Table 11.2

(*a*) Compute $c * d$, $b * b$, $(a * b) * c$ and $[(a * c) * e)] * a$ from the table.

(*b*) is * commutative ? why ?

Solution. (*a*) $c * d = b, b * b = c$

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

and $[(a * c) * e] * a = (c * e) * a = a * a = a$

(*b*) No, since $b * e = c$ and $e * b = b$ and hence $b * e \neq e * b$.

Example 8. Let Z be the set of integers, show that the operation * on Z defined by $a * b = a + b + 1$ for all $a, b \in Z$ satisfies the closure property, associative law and the commutative law. Find the identity element. What is the inverse of an integer a ?

Solution. Since Z is closed for addition, as we have

$$a + b \in Z \text{ for all } a, b \in Z$$
$$\Rightarrow a + b + 1 \in Z$$
$$\Rightarrow a * b \in Z$$

So * is a binary operation on Z.

Again, $a * b = a + b + 1$

$= b + a + 1$ (by commutative law of addition on Z)

$= b * a$ for all $a, b \in Z$

Hence * is commutative.

Again, $(a * b) * c = (a + b + 1) * c$

$= (a + b + 1) + c + 1 = (a + b + c) + 2$

and $a * (b * c) = a * (b + c + 1)$

$= a + (b + c + 1) + 1 = (a + b + c) + 2$

Thus $(a * b) * c = a * (b * c)$ for all $a, b, c \in Z$

Hence, * is associative.

Now, if e is the identity element in Z for *, then for all $a \in Z$

$$a * e = a \Rightarrow a + e + 1 = a$$
$$\Rightarrow e = -1 \in Z$$

So, -1 is the identity element for * in Z.

Let the integer a have its inverse b. Then,

$$a * b = -1 \Rightarrow a + b + 1 = -1$$
$$\Rightarrow b = -(2 + a)$$
$$\Rightarrow \text{So, the inverse of } a \text{ is } -(2 + a).$$

11.3. Group

Let (G, *) be an algebraic structure, where * is a binary operation, then (G, *) is called a group under this operation if the following conditions are satisfied.

1. **Closure law:** The binary * is a closed operation *i.e.*, $a * b \in G$ for all $a, b \in G$.
2. **Associative law:** The binary operation * is an associative operation *i.e.*, $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.

3. **Identity element:** There exists an identity element *i.e.*, for some $e \in G$, $e * a = a * e = a, a \in G$.

4. **Inverse element:** For each a in G, there exists an element a' (the inverse of a) in G such that $a * a' = a' * a = e$.

Many books do not mention the first property as this is a consequence of the definition of binary operation.

A group G is said to be **Abelian** if the commutative law holds *i.e.*, $a * b = b * a$ for all $a, b \in G$.

A group with addition binary operation is known as **additive group** and that with multiplication binary operation is known as **multiplicative group.**

Example 9.

(*i*) The set R of real numbers, for the binary operation of addition, is a group, with 0 as identity element and $(-a)$ as the inverse of a. The same is true of the set Z of integers or the set Q of all rational numbers or the set C of complex numbers.

(*ii*) The set R* of non-zero real numbers, for the binary operation of multiplication, is group with 1 as identity element, and $1/a$ as the inverse of a. The same is true of the set Q* of non-zero rational numbers or the set C* of non-zero complex numbers.

(*iii*) The set Z^+ of positive integers with operation + is not a group. There is no identity element for + in Z^+. The set Z^+ with operation multiplication is not a group. There is an identity element 1, but no inverse of 3.

Example 10. *Prove that the fourth roots of unity 1, – 1, i, – i form an abelian multiplicative group.*

Solution. Let $G = \{1, -1, i, -i\}$. We form the composite table as

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

Table 1.3

Closure Property : Since all the entries in the table are the elements of G and hence G is closed with respect to multiplication.

Associative Law : $a\,(bc) = (ab)\,c$ for all values of a, b, c in G.

For example $1\,[(-1)\,i] = -i = [1\,(-1)]\,i$

Commutative Law : $ab = ba$ for all a, b in G.

From the composition table it is clear that elements in each row are the same as elements in the corresponding column so that $ab = ba$.

Identity element : $1 \in G$ is identity element as $1.a = a.1 = a$. It can be seen from the first row and first column of the table.

Inverses : Inverses of $1, -1, i, -i$ are $1, -1\,.\,i, -i$ respectively and all those belong to G. Hence it follows that G is an abelian multiplicative group.

Example 11. *Show that the set of all positive rational numbers forms an abelian group under the composition defined by* $a * b = (ab)/2$

Solution. Let Q^+ denote the set of all positive rational numbers. We have to show that $(Q^+, *)$ is a group under the composition $a * b = (ab)/2$.

Closure Property : Since for every element $a, b \in Q^+$, $(ab)/2$ is also in Q^+, therefore Q^+ is closed with respect to operation *.

Associative Law : For $a, b \in Q^+$, we have

$$(a * b) * c = (ab/2) * c \Rightarrow (ab/2)\, c/2 = a/2\, (bc/2) = a * (bc/2) = a * (b * c)$$

Commutative Law : For $a, b \in Q^+$, we have

$$a * b = (ab)/2 = (ba)/2 = b * a$$

Identity Element : Let e be the identity element in Q^+, such that $e * a = a = a * e$.

Now $$e * a = a \Rightarrow (ea)/2 = a \Rightarrow (a/2)\,(e - 2) = 0$$

$$\Rightarrow e = 2, \text{ since } a \in Q^+ \Rightarrow a > 0$$

But $2 \in Q^+$ and we have $2 * a = (2a)/2 = a = a * 2$ for all $a \in Q^+$

Inverses : Let a be any element of Q^+. If the number b is to be the inverse of a, then we must have

$$b * a = e = 2 \Rightarrow (ba)/2 = 2 \Rightarrow b = 4/a \in Q^+$$

We have $$(4/a) * a = 4a/2a = 2 = a * (4/a)$$

Therefore, $4/a$ is the inverse of a. Thus each element of Q^+ is invertible.

Hence $(Q^+, *)$ is an abelian group.

Example 12. Show that the set $\{1, 2, 3, 4, 5\}$ is not a group under addition and multiplication modulo 6.

Solution. Let $G = \{1, 2, 3, 4, 5\}$. The operation addition modulo 6 is denoted by $+_6$. We can operate $+_6$ on the elements in G and prepare the composition table as

In the system $(G, +_6)$.

$2 +_6 5 = 1$. For $2 + 5 = 7 = 1 \times 6 + 1$

$1 +_6 4 = 5$. For $1 + 4 = 5$

$3 +_6 5 = 2$. For $3 + 5 = 8 = 1 \times 6 + 2$ etc.

Hence the composition table is

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

Since all the entries in the composition table do not belong to G, in particular $0 \notin G$.

Hence G is not closed w.r.t. $+_6$. Consequently $(G, +_6)$ is not a group.

(*ii*) The operation multiplication modulo 6 is denoted by $\times_6$.

In the system $(G, \times_6)$.

$2 \times_6 5 = 4$. For $2 \times 5 = 10 = 1 \times 6 + 4$

$3 \times_6 4 = 0$. For $3 \times 4 = 12 = 2 \times 6 + 0$.

Hence the composition table is:

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

From the composition table, it is clear that all the entries in the composition table do not belong to G, in particular $0 \notin G$. Hence G is not closed w.r.t. $\times_6$.

Consequently $(G, \times_6)$ is not a group.

Example 13. Show that the matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

form a multiplicative abelian group.

Solution. Let $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, D = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, $G = \{A, B, C, D\}$.

$$A.A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0+1 & 0+0 \\ 0+0 & 0+1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = A,$$

$$AB = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1+0 & 0+0 \\ 0+0 & 0+1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = B.$$

Similarly AC = C, AD = D, BB = A etc.

Hence we find the composition table as

×	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

(*i*) **Closure property :** We can see that all entries in the composition table are the elements of G and hence G is closed w.r.t. matrix multiplication.

(*ii*) **Associative law :** Multiplication is associative in G. Since associative law holds in case of matrix multiplication, *i.e.*,

$$(AB)\,C = A\,(BC).$$

(*iii*) **Commutative law :** The entries in the first, second, third and fourth columns of the composition table coincide with the corresponding entries in the first, second, third and fourth row. This shows that G is commutative.

(*iv*) **Existence of Identity :** From the composition table it follows that

$$AA = A,\ AB = B,\ AC = C,\ AD = D$$

Thus there exists an identity element A in G.

(*v*) **Existence of Inverse :** From the composition table it can be seen that

$$AA = A,\ BB = A,\ CC = A,\ DD = A$$

Thus every element is its own inverse.

Hence the set of four matrices form a multiplicative group which is commutative as well *i.e.*, $(G, .)$ is an abelian group.

Example 14. Let $G = \{(a, b) \mid a, b \in R, a \neq 0\}$. Define a binary operation * on G by

$$(a, b) * (c, d) = (ac, bc + d)$$

for all $(a, b), (c, d) \in G$. Show that $(G, *)$ is a group.

Solution.

Closure Property : Let (a, b) and (c, d) be any two members of G. Then $a \neq 0$ and $c \neq 0$. Therefore, $ac \neq 0$. Consequently $(a, b) * (c, d) = (ac, bc + d)$ is also a member of G. Hence G is closed with respect to the given composition.

Associative law : Let (a, b), (c, d) and (e, f) be any three members of S. Then

$$\begin{aligned}[(a, b) * (c, d)] * (e, f) &= (ac, bc + d) * (e, f) \\ &= ([ac]\, e, [bc + d]\, e + f) \\ &= (ace, bce + de + f).\end{aligned}$$

$$\begin{aligned}\text{Also } (a, b) * [(c, d) * (e, f)] &= (a, b) \times (ce, de + f) \\ &= (a\,[ce], b\,[ce] + de + f) \\ &= (ace, bce + de + f).\end{aligned}$$

Hence the given composition * is associative.

Identity element : Suppose (x, y) is an element of G such that $(x, y) * (a, b) = (a, b)\ \forall$ $(a, b) \in G$

Then $(xa, ya + b) = (a, b)$. Hence $xa = a$ and $ya + b = b$.

These give $x = 1$ and $y = 0$. Now $(1, 0) \in G$

Therefore, $(1, 0)$ is the identity element

Inverse element : Let (a, b) be any member of G. Let (x, y) be a member of G such that $(x, y) \times (a, b) = (1, 0)$.

Then $(xa, ya + b) = (1, 0)$. Hence $xa = 1$, $ya + b = 0$.

These give $x = 1/a$, $y = -b/a$.

Since $a \neq 0$, therefore, x and y are real numbers.

Also $x = \dfrac{1}{a} \neq 0$. Thus $\left(\dfrac{1}{a}, -\dfrac{b}{a}\right)$ is the inverse of (a, b).

Hence G is a group.

Note. In the above group, we have

$$(a, b) * (c, d) = (ac, bc + d)$$

and $$(c, d) * (a, b) = (ca, da + b).$$

Thus, in general, $(a, b) * (c, d) \neq (c, d) * (a, b)$ *i.e.*, the composition is not commutative and hence the group is not abelian.

Example 15. Let Q be the set of positive rational numbers which can be expressed in the form $2^a 3^b$, where a and b are integers prove that the algebraic structure $(Q, .)$ is a group where . is multiplication operator.

Solution.

Closure property: Let $q_1 = 2^a 3^b$, $q_2 = 2^c 3^d \in Q$ where $a, b, c, d, \in Z$, the set integers.

Here $q_1 \cdot q_2 = (2^a 3^b) \cdot (2^c 3^d) = 2^{a+c} \cdot 3^{b+d} \in Q$

Since $a + c, b + d \in Z$. Therefore Q is closed with respect multiplication operator.

Associative law: Let $q_1 = 2^a 3^b$, $q_2 = 2^c 3^d$, $q_3 = 2^e 3^f \in Q$

We have

$$\begin{aligned}q_1 \cdot (q_2 \cdot q_3) &= 2^a 3^b \cdot (2^c 3^d \cdot 2^e 3^f) \\ &= 2^a\, 3^b \,.\, (2^{c+e}\, 3^{d+f}) \\ &= 2^{a+(c+e)} \,.\, 3^{b+(d+f)} \\ &= 2^{(a+c)+e} \,.\, 3^{b+(d+f)}\end{aligned}$$

$$= 2^{a+(c+e)}.3^{(b+d)+f} \quad \text{(Since addition is associative in Z)}$$
$$= (2^{a+c} \cdot 3^{b+d}) \cdot 2^e 3^f$$
$$= (2^a 3^b \cdot 2^c 3^d) \cdot 2^e 3^f$$
$$= (q_1 \cdot q_2) \cdot q_3$$

Identity element: Let $q = 2^a 3^b \in Q$, there exists an identity element e such that $q \cdot e = q$.

Now $2^a 3^b \cdot e = 2^a 3^b \Rightarrow e = 2^0 3^0$ where $0 \in Z$.

since $2^a 3^b \cdot 2^0 3^0 = 2^{a+0} 3^{b+0} = 2^a 3^b$

Inverse Element: Let $q = 2^a 3^b \in Q$. If p is the inverse of q, then we must have

$$q \cdot p = e$$
$$\Rightarrow \quad 2^a 3^b \cdot p = 2^0 3^0 \quad \therefore \quad p = 2^{-a} 3^{-b} \text{ since}$$
$$q \cdot p = 2^a 3^b \cdot 2^{-a} 3^{-b} = 2^{a-a} 3^{b-b} = 2^0 3^0 \text{ and } -a, -b \in Z$$

There $(Q_1, \cdot)$ is a group.

Example 16. Prove that the set

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

is a finite abelian group of order 5 under addition modulo 5 as composition.

Solution. To test the nature of the system $(G, +_5)$ where $G = \{0, 1, 2, 3, 4\}$

$2 +_5 4 = 1$ for $2 + 4 = 6 = 1 \times 5 + 1$

$3 +_5 4 = 2$ for $3 + 4 = 7 = 1 \times 5 + 2$

$4 +_5 4 = 3$ for $4 + 4 = 8 = 1 \times 5 + 3$ etc.

We have the following composition table :

$+_5$	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

From the table, we see that (*i*) the given composition is binary (*ii*) 0 is the identity element (*iii*) every element has an inverse. Thus the inverses of 0, 1, 2, 3, 4 are 0, 4, 3, 2, 1 respectively. The composition is associative and commutative.

Hence the given set is a finite abelian group of order 5 under addition modulo 5.

Elementary Properties of Groups

We now prove some elementary properties of groups.

Theorem 11.3. (Cancellation Law). If $(G, *)$ is a group and a, b, c are in G, then

(*i*) $a * b = a * c \Rightarrow b = c$ (left cancellation law)

(*ii*) $b * a = c * a \Rightarrow b = c$ (right cancellation law)

Proof. (*i*) Since $a^{-1} \in G$, operating on the left with a^{-1}, we have

$$a^{-1} * (a * b) = a^{-1} * (a * c)$$
or
$$(a^{-1} * a) * b = (a^{-1} * a) * c$$
or
$$e * b = e * c$$
or
$$b = c.$$

(*ii*) We have $b * a = c * a$

Operating on the right by a^{-1}, we get

or $b * e = c * e$

or $b = c$

Hence $b * a = c * a \Rightarrow b = c$

Theorem 11.4. The left identity is also the right identity, *i.e.*,

$$e * a = a = a * e \text{ for all } a \in G.$$

Proof. If a^{-1} be the left inverse of a, then

$$a^{-1} * (a * e) = (a^{-1} * a) * e$$

or $a^{-1} * (a * e) = e * e$

$= e$

$= a^{-1} * a.$

Thus, $a^{-1} * (a * e) = a^{-1} * a$

$\boxed{a * e = a.}$ by Theorem 11.3

Hence e is also the right identity element of a group.

Theorem 11.5. The left inverse of an element is also its right inverse *i.e.*,

$$a^{-1} * a = e = a * a^{-1}.$$

Proof. Now $a^{-1} * (a * a^{-1}) = (a^{-1} * a) * a^{-1}$ (associativity)

$= e * a^{-1}$

$= a^{-1} * e$ by Theorem 11.4

Thus $a^{-1} * (a * a^{-1}) = a^{-1} * e$

Therefore, $a * a^{-1} = e$ by Theorem 11.3

Thus the left inverse of an element in a group is also its right inverse.

Theorem 11.6. In a group (G, *)

(*i*) the equation $a * x = b$ has a unique solution $x = a^{-1} * b$

(*ii*) the equation $y * a = b$ has a unique solution $y = b * a^{-1}$, where $a, b \in G$.

Proof. If possible, let the equation $a * x = b$ have two solutions x and x' in G. Then

$$a * x = b \text{ and } a * x' = b.$$

Therefore, $a * x = a * x'$, where $a, x, x' \in G$.

By left cancellation law, we have $x = x'$, $\therefore$ $a * x = b$ has unique solution in G.

Again, assuming $x = a^{-1} * b$, we have

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

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

$= e * b$ (e being the identity element)

$= b.$

This shows that $x = a^{-1} * b$ satisfies the equation $a * x = b$.

The second part can similarly be proved.

Theorem 11.7. In a group (G, *)

(*i*) $(a^{-1})^{-1} = a$ *i.e.*, the inverse of the inverse of an element is equal to the element;

(*ii*) $(ab)^{-1} = b^{-1} a^{-1}$ *i.e.*, the inverse of the product of two elements is the product of the inverses in the reverse order.

Proof. (*i*) Let e be the identity element for * in G.

Then we have $a * a^{-1} = e$, where $a^{-1} \in G$.

Also $(a^{-1})^{-1} * a^{-1} = e$.

Therefore, $(a^{-1})^{-1} * a^{-1} = a * a^{-1}$.

Thus, by right cancellation law, we have $(a^{-1})^{-1} = a$.

(*ii*) Let a and $b \in G$ and G is a group for *, then

$a * b \in G$ (closure).

Therefore, $(a * b)^{-1} * (a * b) = e$.

Let a^{-1} and b^{-1} be the inverses of a and b respectively, then $a^{-1}, b^{-1} \in G$. ... (1)

Therefore, $(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b$ (associativity)

$= b^{-1} * e * b = b^{-1} * b = e$ ... (2)

From (1) and (2) we have $(a * b)^{-1} * (a * b) = (b^{-1} * a^{-1}) * (a * b)$

$(a * b)^{-1} = b^{-1} * a^{-1}$. by right concellation law.

Example 17. Prove that if $a^2 = a$, then $a = e$, a being an element of a group.

Solution. Let a be an element of a group G such that $a^2 = a$.

To prove that $a = e$.

$$a^2 = a \Rightarrow a.a = a \Rightarrow (aa)\, a^{-1} = aa^{-1}$$
$$\Rightarrow a\,(aa^{-1}) = e. \qquad (\because aa^{-1} = e)$$
$$\Rightarrow ae = e \Rightarrow a = e. \qquad (\text{since } ae = a.)$$

Example 18. Show that if every element of a group (G, o) be its own inverse, then it is an abelian group.

Is the converse true ?

Solution. Let $a, b \in G$, then $a \circ b \in G$ (closure).

Hence, by the given condition, we have

$$a \circ b = (a \circ b)^{-1}$$
$$= b^{-1} \circ a^{-1}$$
$$= b \circ a, \text{ since } a^{-1} = a \text{ and } b^{-1} = b.$$

Thus $a \circ b = b \circ a$, for every $a, b \in G$.

Therefore, it is an abelian group.

The converse is not true. For example, (R, +), where R is the set of all real numbers, is an abelian group, but no element except 0 is its own inverse.

Example 19. Show that if a, b are arbitrary elements of a group G, then $(ab)^2 = a^2b^2$ if and only if G is abelian.

Solution. Let a and b be arbitrary elements of a group G. Suppose $(ab)^2 = a^2\, b^2$. ... (1)

To prove G is abelian, we have to show that

$$ab = ba$$
$$(ab)^2 = a^2b^2 \Rightarrow (ab)\,(ab) = (aa)\,(bb)$$
$\Rightarrow a\,(ba)\,b = a\,(ab)\,b$, by associative law

$\Rightarrow (ba)\,b = (ab)\,b$, by left cancellation law

$\Rightarrow ba = ab$, by right cancellation law.

Again, suppose G is abelian so that

$$ab = ba \ \forall \ a, b \in G \quad \ldots (2)$$

To prove that $(ab)^2 = a^2b^2$

$$(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b, \quad \text{by (2)}$$
$$= (aa)(bb) = a^2b^2.$$

Hence proved.

Example 20. G is a group and there exist two relatively prime positive integers m and n such that $a^m b^m = b^m a^m$ and $a^n b^n = b^n a^n$ for all $a, b, \in G$. Prove that G is Abelian.

Solution. Since m and n are relatively prime, gcd $(m, n) = 1$, we get $mx + ny = 1$ for some $x, y \in Z$.

Now
$$(a^m b^n)^{mx} = a^m (b^n a^m)^{mx-1} b^n$$
$$= a^m (b^n a^m)^{mx} (b^n a^m)^{-1} b^n$$
$$= (b^n a^m)^{mx} a^m a^{-m} b^{-n} b^n$$
$$= (b^n a^m)^{mx}. \quad \ldots (1)$$

Similarly it can be proved that
$$(a^m b^n)^{ny} = (b^n a^m)^{ny} \quad \ldots (2)$$

From (1) and (2) we get
$$a^m b^n = (a^m b^n)^{mx + ny}$$
$$= (b^n a^m)^{mx + ny} = b^n a^m. \quad \ldots (3)$$

Finally
$$ab = a^{mx + ny} b^{mx + ny}$$
$$= a^{mx} (a^{ny} b^{mx}) b^{ny}$$
$$= a^{mx} b^{mx} a^{ny} b^{ny} \quad \text{by (3)}$$
$$= b^{mx} a^{mx} b^{ny} a^{ny} \quad \text{by hypothesis}$$
$$= b^{mx + ny} a^{mx + ny} \quad \text{by (3)}$$
$$= ba.$$

Hence G is Abelian.

Order of an Element

The order of an element g in a group G is the smallest positive integers n such that $g^n = e$. If no such integer exists, we say g has infinite order. The order of an element g is denoted by $o(g)$.

So, to find the order of a group element g, one need only compute the sequence of products g, g^2, g^3, ... until one reach the identity for the first time. The exponent of this product is the order of g. If the identity never appears in the sequence, then g has infinite order.

Example 21. Let $G = \{1, -1, i, -i\}$ be a multiplicative group. Find the order of every element.

Solution. 1 is the identity element in G.

(*i*) $1^1 = 1 \Rightarrow o(1) = 1$.

(*ii*) $(-1)^2 = 1$, $(-1)^n \neq 1$ for any positive integer $n < 2$

Hence $o(-1) = 2$.

(*iii*) $(i)^4 = 1$ and $(i)^n \neq 1$ for any positive integer $n < 4$.

Hence $o(i) = 4$.

(*iv*) $(-i)^4 = 1$ and $(-i)^n \neq 1$ for any positive integer $n < 4$.

Hence $o(-i) = 4$.

Example 22. Find the order of every element in the multiplicative group $G = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$

Solution. The identity element of the given group is $a^6 = e$.

$a^6 = e \Rightarrow o(a) = 6$

$(a^2)^3 = a^6 = e \Rightarrow o(a^2) = 3$

$(a^3)^2 = a^6 = e \Rightarrow o(a^3) = 2$

$(a^4)^3 = a^{12} = (a^6)^2 = e^2 = e \Rightarrow o(a^4) = 3$

$(a^5)^6 = (a^6)^5 = e^5 = e \Rightarrow o(a^5) = 6.$

and $(a^5)^n \neq e$ for any $n < 6$

$(a^5)^1 = a^6 = e \Rightarrow o(a^6) = 1.$

Thus the orders of elements $a, a^2, a^3, a^4, a^5, a^6$ are 6, 3, 2, 3, 6, 1 respectively.

Example 23(*i*). In a group (G, o), a is an element of order 30. Find the order of a^5 and a^{12}.

Solution. Given $o(a) = 30$ so $a^{30} = e$, the identity element. Let $o(a^5) = n$. So, $(a^5)^n = e$ i.e., $a^{5n} = e$ where n is the least positive integer. Hence 30 is a divisor of $5n$. $\therefore n = 6$. Hence $o(a^5) = 6$.

Example 23(*ii*). *In a group G for a, b ∈ G, o(a) = 5, b ≠ e and $aba^{-1} = b^2$. Show that o(b) is 31.*

Solution.

$$(ab\,a^{-1})^2 = (ab\,a^{-1})(ab\,a^{-1}) = ab(a^{-1}a)ba^{-1} = abeba^{-1}$$
$$= abba^{-1} = ab^2a^{-1} = a(ab\,a^{-1})a^{-1} \ (\because aba^{-1} = b^2)$$
$$= a^2\,ba^{-2}$$
$$(ab\,a^{-1})^4 = (ab\,a^{-1})^2\,(ab\,a^{-1})^2 = (a^2\,ba^{-2})\,(a^2\,ba^{-2})$$
$$= a^2b\,(a^{-2}\,a^2)\,ba^{-2} = a^2\,be\,ba^{-2} = a^2\,b^2\,a^{-2} \ (\because a^0 = e)$$
$$= a^2(ab\,a^{-1})\,a^{-2} = a^3\,ba^{-3}$$

Similarly, $(ab\,a^{-1})^8 = a^4\,b\,a^{-4}$ and $(ab\,a^{-1})^{16} = a^5b\,a^{-5}$

$$(ab\,a^{-1})^{16} = ebe^{-1} \ (\because o(a) = 5 \text{ i.e., } a^5 = e)$$
$$= be \ (\because e^{-1} = e)$$
$$= b$$

Thus $(b^2)^{16} = b \Rightarrow b^{32} = b$ or $b^{31}\,b.b^{-1} = bb^{-1}$

$\therefore$ $b^{31}.e = e \Rightarrow b^{31} = e$

so, $o(b) = 31$

11.4. Groupoid, Semigroup and Monoid

Let (S, *) be an algebraic structure in which S is a non-empty set and * is a binary operation on S. Thus S is closed with the operation *. Such a structure consisting of a non-empty set S and a binary operation defined in S is called a **groupoid.**

An algebraic structure (S, *) is called a **semigroup** if the following conditions are satisfied:

1. The binary operation * is a closed operation *i.e.*, $a * b \in S$ for all $a, b \in S$. (closure law).
2. The binary operation * is an associative operation *i.e.*, $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$. (associative law).

An algebraic structure (S, *) is called a **monoid** if the following conditions are satisfied:

1. The binary operation * is a closed operation. (closure law).
2. The binary operation * is an associative operation (associative law).
3. There exists an identity element, *i.e.*, for some $e \in S$, $e * a = a * e = a$ for all $a \in S$.

Thus a monoid is a semigroup (S, *) that has an identity element.

For example,

(*i*) If N be a set of natural numbers, then (N, +) is groupoid because the set N is closed under addition. But the set of odd integers is not a groupoid under addition operation since 3 + 3 = 6 do not belong to the set of odd integers and hence is not closed.

(*ii*) If Z be a set of all integers, then (Z, +) and (Z, .) are semi group as these two operations are closed and associative in Z.

(*iii*) N, the set of positive integers, and * is the operation of least common multiple (l.c.m) on N, (N, *) is a semigroup, it is also commutative.

Solution. For $a, b \in N$, define $a * b$ = l.c.m (a, b). Clearly $a * b \in N$ and for $a, b, c, \in N$.

$$\begin{aligned}(a * b) * c &= (\text{l.c.m. } (a, b)) * c \\ &= \text{l.c.m. } [\text{l.c.m. } (a, b), c] \\ &= \text{l.c.m. } [a, b, c] \\ &= \text{l.c.m. } [a, \text{l.c.m. } (b, c)] \\ &= a * (b * c).\end{aligned}$$

Hence * is associative. Hence $(N, *)$ is a semigroup. Clearly, $a * b$ = l.c.m (a, b) = l.c.m (b, a) $= b * a$ for all $a, b \in N$. Hence * is commutative.

The structure (Z, +) is a monoid with identity element 0 and (Z, .) is a monoid with 1 as the identity element. [P(S), ∪] is a monoid with φ as identity element.

We note that every group (G, *) is a semigroup. A semigroup (S, *) is commutative if * is commutative *i.e.*, $a * b = b * a$ for all $a, b \in$ S. A semi group (S, *) which is not commutative is called non-commutative. The set of integers (Z, +) and (Z, .) are commutative semigroups, where the binary operation on Z are usual addition and multiplication of integers.

The next three theorems give necessary and sufficient conditions for a semigroup to be a group.

Theorem 11.8. A semigroup (S, *) is a group if and only if

(*i*) there exists $e \in$ S such that $e * a = a$ for all $a \in$ S and

(*ii*) for all $a \in$ S there exists $b \in$ S such that $b * a = e$.

Proof: Suppose (S, *) is a semigroup that satisfies (*i*) and (*ii*). Then for $b \in$ S, there exists $c \in$ S such that $c * b = e$ by (*ii*).

Now $a = e * a = (c * b) * a = c * (b * a) = c * e$

and $a * b = (c * e) * b = c * (e * b) = c * b = e$

Hence $a * b = e = b * a$. Also $a * e = a * (b * a) = (a * b) * a = e * a = a$.

Thus, $a * e = a = e * a$. This shows that e is the identity element of S. Now since $a * b = e = b * a$, we have $b = a^{-1}$. Therefore, (S, *) is a group.

The converse can be proved from the definition of a group.

Theorem 11.9. A semi group {S, *} is a group if and only if for $a, b \in$ S each of the equations $a * x = b$ and $y * a = b$ has a solution in S for x and y.

Proof: If S is a group, then by theorem 11.6, the equation $a * x = b$ and $y * a = b$ have solutions in S.

Conversely, suppose the given equations have solutions in S. Let the equation $y * a = a$ have a solution $e \in$ S. Then $e * a = a$. For any $b \in$ S, if t (depending on a and b) be the solution of the equations $a * x = b$, then $a * t = b$.

Now, $e * b = e * (a * t) = (e * a) * t = a * t = b$.

Consequently, $e * b = b$, for all $b \in$ S $\Rightarrow e$ is a left identity in S.

Next, a left inverse of an element $a \in$ S is given by the solution $y * a = e$ and the solution belongs to S.

Hence, for each $a \in$ S, there exist a left inverse in S. Thus S is a group.

Theorem 11.10. A finite semi-group (S, *) is a group if and only if (S, *) satisfies the cancellation laws (*i.e.*, $a * c = b * c$ implies $a = b$ and $c * a = c * b$ implies $a = b$ for all $a, b, c \in$ S).

Proof: Let (S, *) be a finite semi-group satisfying cancellation law *i.e.*,

$$a * b = b * c \Rightarrow b = c$$

and

$$b * a = c * a \Rightarrow b = c$$

Let $S = \{a_1, a_2, \ldots\ldots, a_n\}$ where a_i are all distinct element of S.

Consider now the elements $a_1 * a_1, a_1 * a_2, \ldots\ldots, a_1 * a_n$.

These elements belong to S and are distinct. If they are not distinct, let, $a_1 * a_i = a_1 * a_j$.

Then, by cancellation law, $a_i = a_j$, which contradicts the fact $a_i \neq a_j$.

Then composite elements $a_1 * a_1, a_1 * a_2 \ldots\ldots, a_1 * a_n$, being all distinct, they are the n given elements of S in some order. This shows that the equation $a * x = b$ for $a, b \in S$ has a solution in S.

Similarly, by forming the products $a_1 * a_1, a_2 * a_1, \ldots\ldots, a_n * a_1$, it can be shown that the equation $y * a = b$ for $a, b \in S$ has a solution in S.

Thus $\{S, *\}$ is a semi-group in which each of the equations $a * x = b$ and $y * a = b$ has a solution in S for all $a, b \in S$.

Hence by Theorem 11.9 $\{S, *\}$ is a group.

Free Semi-group

Let $A = \{a_1, a_2\ldots\ldots, a_n\}$ be a non empty set. A word ω on A is a finite sequence of its elements. For example.

$u = aab\ aabb = a^2ba^2b^2$ and $v = aaccbccab = a^2c^2b\ c^2ab$ are words on $A = \{a, b, c\}$

The length of a word w denoted by L (w) is the number of elements in w.

Thus L $(u) = 7$ and L $(v) = 9$.

Let A* consists of all words that can be formed from the alphabet A. Let α and β be elements of A*. If $\alpha = a_1\ a_2 \ldots\ldots\ a_m$ and $\beta = b_1 b_2 \ldots\ldots\ b_n$, then

$$\alpha\beta = a_1\ a_2 \ldots\ldots a_m\ b_1 \ldots\ldots b_n$$

Thus if α, β and γ are any elements of A*, then it is easy to see $\alpha\ (\beta.\ \gamma) = (\alpha \cdot \beta) \cdot \gamma$.

So * is an associative binary operation, and (A *) is a semi-group. The semi-group (A *) is called the free semi-group generated by A.

Let (S, *) be a group and B be a non-empty subset of S. If B is closed under operation *, then B is called a **sub semi-group** of (S, *). Since the elements of B are also elements of S, the associative law automatically holds for the elements of B.

Examples

(*i*) Let A and B denote, respectively, the set of even and odd positive integers. Then (A, ×) and (B, ×) are sub semi groups of (N, ×) since A and B are closed under multiplication. On the other hand, (A, +) is a sub semi group of (N +) since A is closed under addition, but (B, +) is not a sub semi group of (N, +) since B is not closed under addition.

(*ii*) Consider the free semi group K on the set $A = \{a, b\}$. Let L consist of all even words, that is, words with even length. The concatenation of two such words is also even. Thus L is a sub semi group of K.

11.5. Subgroup

Let (G, *) be a group and H is a subset of G. (H, *) is said to be subgroup of G if (H, *) is also group by itself.

Now every set is a subset of itself. Therefore, if G is a group, then G itself is a subgroup of G. Also if e is the identity element of G. Then the subset of G containing only identity element is also a subgroup of G. These two subgroups (G, *) and $(\{e\}, *)$ of the group (G, *) are called **improper or trivial subgroups**, others are called proper or nontrivial subgroups.

Example 24

(*i*) The multiplicative group $\{1, -1\}$ is a subgroup of the multiplicative group $\{1, -1, i, -i\}$

(*ii*) The additive group of even integers is a subgroup of the additive group of all integers.

(*iii*) The set Q^+ of all non-zero positive rational numbers is a subgroup of the multiplicative group Q^* of all non-zero rational numbers.

Important Theorems

Theorem 11.11. The identity element of a sub group is the same as that of the group.

Proof: Let H be the subgroup of the group G and e and e' be the identity elements of G and H respectively.

Now, if $a \in H$, then $a \in G$ and $ae = a$, since e is the identity element of G.

Again $a \in H$, then $ae' = a$, since e' is the identity element of H.

Thus $ae = ae'$ which gives $e = e'$

Theorem 11.12. The inverse of any element of a subgroup is the same as the inverse of the same regarded as an element of the group.

Proof: Let H be the subgroup of the group G, and let e be the common identity element.

Let $a \in H$. Suppose b is the inverse of a in H and c is the inverse in G. Then we have $ba = e$ and $ca = e$.

Hence, in G we have $ba = ca \Rightarrow b = c$

Note. Since the identity of H is the same as that of G, it is easy to see that the order of an element of H is the same as the order of that element regarded as a member of G.

The next two theorems provide simple tests that suffice to show that a subset of a group is a subgroup.

Theorem 11.13. (two step subgroup test) A non-empty subset H of a group G is a subgroup of G if and only if

(*i*) $a \in H, b \in H \Rightarrow a * b \in H$

(*ii*) $a \in H \Rightarrow a^{-1} \in H$ where a^{-1} is the inverse of a in G.

Proof: The condition is necessary. Suppsoe H is a subgroup of G. Then H must be closed with respect to operation * *i.e*, $a \in H, b \in H \Rightarrow a * b \in H$.

Let $a \in H$ and let a^{-1} be the inverse of a in G. Then the inverse of a in H is also a^{-1}. Since H itself is a group, therefore, each element of H must possess inverse. Therefore, $a \in H \Rightarrow a^{-1} \in H$.

Thus the condition is necessary.

The Condition is Sufficient

We observe that the binary operation * in G is also a binary operation in H. Hence H is closed under the operation.

As the elements of H is also the elements of G and the elements of G satisfy the associative law for the binary operation, therefore, the elements of H will also satisfy the associative law.

Now $a \in H \Rightarrow a^{-1} \in H$

From the condition (*i*), we have $a \in H, a^{-1} \in H \Rightarrow aa^{-1} \in H = e \in H$ which shows the existence of identity element in H.

Thus all the conditions are satisfied, H is a subgroup of G.

Theorem 11.14. The necessary and sufficient condition for a non-empty sub-set H of a group (G, *) to be a subgroup is

$$a \in H, b \in H \Rightarrow a * b^{-1} \in H,$$

where b^{-1} is the inverse of b in G.

Proof: Let H be a sub-group and $a \in H$, $b \in H$. Since H is a sub-group and $b \in H$, b^{-1} must exist and will belong to H.

Now $a \in H$, $b^{-1} \in H \Rightarrow a * b^{-1} \in H$, by closure property.

Thus the condition is necessary.

To prove that this condition is also sufficient, we assume that

$$a \in H, b \in H \Rightarrow a * b^{-1} \in H.$$

We are to show that H is a sub-group of G.

By the given condition, we have

$$a \in H, a^{-1} \in H \Rightarrow e * a^{-1} \in H$$
$$\Rightarrow e \in H,$$

where e is the identity element.

Again, we have $e \in H$, $a \in H \Rightarrow e * a^{-1} \in H$

$$\Rightarrow a^{-1} \in H,$$

where a^{-1} is the inverse of a.

Now, if $b \in H$, then $b^{-1} \in H$.

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

$$\Rightarrow a * b \in H \text{ (closure property).}$$

Now, $H \subset G$ and the associative law holds good for G, as G is a group. Hence it is true for the elements of H! Thus all postulates for a group are satisfied for H. Hence H is a subgroup of G.

Example 25. Let G be the additive group of all integers and H be the subset of G consisting of all positive integers. Then H is closed with respect to addition *i.e.*, the composition in G. But H is not a subgroup of G since the identity $0 \notin H$.

Example 26. Let $G = \{.....3^{-2}, 3^{-1}, 1, 3, 3^2, ...\}$ be the multiplicative group consisting of all integral powers of 3. Let $H = \{1, 3, 3^2, ...\}$. Then $H \subset G$ and H is closed with respect to multiplication, But H is not a subgroup of G since the inverse of 3 *i.e.*, 3^{-1} does not belong to H.

Theorem 11.15. The intersection of any two sub-groups of a group (G, *) is again a sub-group of (G, *).

Proof: Let H_1 and H_2 form any two sub-groups of (G, *).

We have $H_1 \cap H_2 \neq \phi$, since at least the identity element is common to both H_1 and H_2

Let $a \in H_1 \cap H_2$ and $b \in H_1 \cap H_2$.

Now $a \in H_1 \cap H_2 \Rightarrow a \in H_1$ and $a \in H_2$

$b \in H_1 \cap H_2 \Rightarrow b \in H_1$ and $b \in H_2$

Since H_1 and H_2 from sub-groups under the group (G, *), we have

$$a \in H_1, b \in H_1 \Rightarrow a * b^{-1} \in H_1,$$
$$a \in H_2, b \in H_2 \Rightarrow a * b^{-1} \in H_2$$

Finally, $ab^{-1} \in H_1$, $ab^{-1} \in H_2 \Rightarrow a * b^{-1} \in H_1 \cap H_2$

Thus we see,

$a \in H_1 \cap H_2$, $b \in H_1 \cap H_2 \Rightarrow a * b^{-1} \in H_1 \cap H_2$

Therefore, $H_1 \cap H_2$ forms a sub-group under (G, *)

Note: The union of two subgroups is not necessarily a subgroup.

For example, let G be the additive group of integers.

Then $H_1 = \{....., -6, -4, -2, 0, 2, 4, 6, ...\}$ and

$H_2 = \{....., -12, -9, -6, -3, 0, 3, 6, 9, 12.....\}$

are both subgroups of G.

Now $H_1 \cup H_2 = \{....., -4, -3, -2, 0, 2, 3, 4, 6, ...\}$

Obviously $H_1 \cup H_2$ is not closed with respect to addition as $2 \in H_1 \cup H_2$, $3 \in H_1 \cup H_2$ but $2 + 3 = 5 \notin H_1 \cup H_2$. Therefore, $H_1 \cup H_2$ is not a subgroup of G.

Cosets

Let H be a subgroup of a group G and let $a \in G$. Then the set $\{a * h : h \in H\}$ is called the left coset generated by a and H and is denoted by aH.

Similarly the set $Ha = \{h * a : h \in H\}$ is called the right coset and is denoted by Ha. The element a is called a representative of aH and Ha.

It is evident that both aH and Ha are subsets of G.

If e be the identity element of G, then $e \in H$ and $He = H = eH$. Therefore, H itself is a right as well as a left coset.

In general $aH = Ha$, but in the abelian group, each left coset coincides with the corresponding right coset.

If the group operation be addition, then the right coset of H in G generated by a is defined as

$$H + a = \{h + a : h \in H\}.$$

Similarly, the left coset $a + H = \{a + h : h \in H\}$.

Index of a subgroup in a group. If H is a subgroup of a group G, the number of distinct right (left) cosets of H in G is called the index of H in G and is denoted by [G : H] or by i_G (H).

Example 27. Let G be te additive group of integers *i.e.*,

$G = \{... -3, -2. -1, 0, 1, 2, 3, ...\}$.

Let H be the subgroup of G obtained on multiplying each element of G by 3. Then

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

Since the group G is abelian any right coset will be equal to the corresponding left coset. Let us form the right cosets of H in G.

We have $0 \in G$ and

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

Again $1 \in H$ and $H + 1 = \{...., -8, -5, -2, 1, 4, 7, 10, ...\}$.

Then $2 \in G$ and $H + 2 = \{..., -7, -4, -1, 2, 5, 8, 11, ...\}$.

We see that the right cosets H, H + 1 and H + 2 are all distinct and moreover these are disjoint *i.e.*, have no element common.

Now $3 \in G$ and $H + 3 = \{...., -6, -3, 0, 3, 6, 9, 12, ...\}$.

We see that H + 3 = H. Also we observe that $3 \in H$.

Again $4 \in G$ and $H + 4 = \{...., -5, -2, 1, 4, 7, 10, 13,....\} = H + 1$

Thus there exists three disjoint right cosets namely H, H + 1, H + 2.

The union of all right cosets of H in G will be equal to G. i.e.

$G = H \cup (H + 1) \cup (H + 2)$

The index of H in G is 3.

Properties of Cosets

Let H be a subgroup of G, and a and b belong to G, Then,

1. $a \in aH$
2. $aH = H$ if and only if $a \in H$
3. $aH = bH$ or $aH \cap bH = \phi$
4. $aH = bH$ if and only if $a^{-1}b \in H$,

Analogous results hold for right cosets.

Proof 1. $a = ae \in aH$, e is the identity element of G.

2. If e be the identity in G and so is in H, then

$$aH = H \Rightarrow ae \in H$$

$$aH = H \Rightarrow a \in H \quad \ldots (1)$$

i.e., if $a \in H$ and $h \in H$ then

Again, $$a \in H \Rightarrow ah \in H \ \forall\ h \in H$$

$$aH \subset H$$

$\therefore$ Also $a \in H \Rightarrow a^{-1} H$, H being a sub-group of the group G, satisfies group axioms.

$\Rightarrow a^{-1} h \in H \ \forall\ h \in H$ by closure law in H

$\Rightarrow a\,(a^{-1} h) \in H \ \forall\ h \in H$ by closure law in H

$\Rightarrow h \in aH \ \forall\ h \in H$

$\therefore$ $H \subset aH$

So $aH \subset H$ and $H \subset aH \Rightarrow aH = H$

Next $$a \in H \Rightarrow aH = H \quad \ldots (2)$$

Hence $$aH = H \Leftrightarrow a \in H \text{ by (1) and (2).}$$

3. Let H be a sub-group of a group G and let aH and bH be two of its left cosets. Assume that $aH \cap bH \neq \phi$ and let c be the common element of the two cosets.

Then we may write $c = ah$ and $c = bh'$, for $h, h' \in H$.

Therefore $ah = bh'$, giving $a = bh'\, h^{-1}$.

Since H is a sub-group, we have $h'\, h^{-1} \in H$.

Let $$h'\, h^{-1} = h'' \text{ so that } a = bh''.$$

Hence $$aH = (bh'')\, H = b\,(h''\, H) = bH, \text{ since } h''\, H = H.$$

Hence the two left cosets aH and bH are identical if $aH \cap bH \neq \phi$.

Thus either $aH \cap bH = \phi$ or $aH = bH$.

4. We have,

$$aH = bH \Rightarrow a^{-1}\, aH = a^{-1}\, bH$$

$$\Rightarrow (a^{-1}\, a)\, H = (a^{-1}\, b)\, H$$

$$\Rightarrow eH = (a^{-1}\, b)H, \ e \text{ being the identity in G and so in H.}$$

$$\Rightarrow H = (a^{-1} b)H$$

$\therefore$ $$aH = bH \Rightarrow a^{-1}\, b \in H \quad \ldots (1)$$

Also, if $a^{-1}\, b \in H$, then

$$bH = e\,(bH) = (aa^{-1})\,(bH) = a\,(a^{-1} b)H = aH \quad \ldots (2)$$

(1) and (2) follow that $aH = bH \Leftrightarrow a^{-1}\, b \in H$.

Normal Subgroup

A subgroup H of a group G is said to be a normal subgroup of G if $Ha = aH$ for all $a \in G$.

Clearly every subgroup of an Abelian group is a normal subgroup. To verify that a subgroup is normal one can use the following theorem.

Theorem 11.16. A subgroup H of a group G is normal if and only if $g^{-1}\, hg \in H$ for every $h \in H$, $g \in G$.

Proof: Let H be a normal subgroup of G. Let $h \in H$, $g \in G$

Then $$Hg = gH \text{ (Definition of normal subgroup)}$$

Now $$hg \in Hg = gH$$

so $$hg = gh_1 \text{ for some } h_1 \in H.$$

i.e., $$g^{-1} hg = h_1 \in H.$$

Conversely let H be such that

$$g^{-1}hg \in H \ \forall \ h \in H, g \in G.$$

Consider $a \in G$ For any $h \in H$, $a^{-1}h\,a \in H$

Therefore, $ha = a(a^{-1}ha) \in aH.$

Consequently $Ha \subseteq aH.$

Let $b = a^{-1}$

then $b^{-1}hb \in H$

But $b^{-1}hb = (a^{-1})^{-1}ha^{-1} = aha^{-1}$

This gives $aha^{-1} \in H$

so that $ah = (aha^{-1})\,a \in Ha$

which proves that $aH \subseteq Ha.$

Hence $aH = Ha.$

This theorem shows that, equivalently a subgroup H of a group G can be defined to be a normal subgroup if

$$g^{-1}hg \in H \ \forall \ h \in H, g \in G.$$

Example 28. Consider the group $(Z, +)$. Let $H = \{3n : n \in Z\}$ show that H is a subgroup of Z.

Solution. It is a subgroup of Z since

(*i*) H is non-empty.

(*ii*) Let $x, y \in H$. Then there exist $p, q \in Z$ such that $x = 3p, y = 3q$.

Now $xy^{-1} = 3p - 3q = 3(p - q)$ where $p - q \in Z$.

Thus $xy^{-1} \in H$

Hence H is a subgroup of Z.

Example 29. Let G be a group. For a fixed element of G, let $G_x = \{a \in G : ax = xa\}$. Show that G_x is a subgroup of G for all $x \in G$.

Solution. Since (*i*) $ex = xe$, $e \in G_x$. Therefore, $G_x \neq \phi$.

(*ii*) $a, b \in G_x \Rightarrow ax = xa$ and $bx = xb$.

Now $(ab)\,x = abx,$

$= axb, \quad (\because bx = xb)$

$= xab, \quad (\because ax = xa)$

$= x(ab).$

This shows $ab \in G_x$. Hence G_x satisfies the closure axiom.

(*iii*) $a \in G_x \Rightarrow ax = xa.$

$\Rightarrow a^{-1}(ax)\,a^{-1} = a^{-1}(xa)\,a^{-1}.$

$\Rightarrow a^{-1}axa^{-1} = a^{-1}xaa^{-1},$

$\Rightarrow exa^{-1} = a^{-1}xe,$

$\Rightarrow xa^{-1} = a^{-1}x,$

$\Rightarrow a^{-1} \in G_x.$

Thus the inverse of each element of G_x is in G_x.

Order of a group. The number of elements in a group is called the *order* of the group.

The order of a group G is denoted by $o(G)$. A group of finite order is called a *finite group*. By using the concept of cosets we prove a theorem due to Langrange which expresses a relationship between the order of a finite group and the order of its subgroup.

Lagrange's Theorem

Theorem 11.18. The order of each sub-group of a finite group G is a divisor of the order of the group G.

Proof. Let H be any sub-group of order m of a finite group G of order n. We consider the left coset decomposition of G relative to H.

We first show that each coset a H consists of m different elements.

Let $$H = \{h_1, h_2, ..., h_m\}.$$

Then $a\,h_1, a\,h_2, ..., a\,h_m$ are the m members of a H, all distinct.

For, we have

$$a\,h_i = a\,h_j \Rightarrow h_i = h_j, \text{ by cancellation law in G.}$$

Since G is a finite group, the number of distinct left cosets will also be finite, say k. Hence the total number of elements of all cosets is $k\,m$ which is equal to the total number of elements of G.

$$n = mk. \qquad \ldots (1)$$

Hence, this shows that m, the order of H, is a divisor of n, the order of the group G.

Note. The converse of Lagrange's theorem is not true.

Cor. 1. If G be a finite group of order n and $n \in$ G, then

$$a^n = e.$$

Let o $(a) = m$ which implies $a^m = e$.

Now, the sub-set H of G consisting of all the integral powers of a is a sub-group of G and the order of H is m.

Then, by the above theorem, m is a divisor of n.

Let $n = mk$, then

$$a^n = a^{mk} = (a^m)^k = e^k = e.$$

SOLVED EXAMPLES

Example 30. If H is a subgroup of G such that $x^2 \in H$ for every $x \in G$, then prove that H is a normal subgroup of G.

Solution. For any $g \in$ G, $h \in$ H; $(gh)^2 \in$ H and $g^{-2} \in$ H.

Since H is a subgroup, $h^{-1}\,g^{-2} \in$ H and so $(gh)^2\,h^{-1}\,g^{-2} \in$ H. This gives that $gh\,gh\,h^{-1}\,g^{-2} \in$ H, *i.e.*, $ghg^{-1} \in$ H. Hence H is a normal subgroup of G.

Example 31. If G be an abelian group with identity e, then prove that all elements x of G satisfying the equation $x^2 = e$ form a sub-group H of G.

Solution. Let $H = \{x : x^2 = e\}$.

Now $x^2 = e \Rightarrow x = x^{-1}$.

Therefore, if $x \in$ H, then x^{-1} also belongs to H.

Furthermore $e^2 = e$.

Hence the identity element of G also belongs to H.

Let $x, y \in$ H.

Then, since G is abelian, we have

$$\begin{aligned} xy &= yx \\ &= y^{-1}x^{-1}, \text{ as } x^{-1} = x \text{ and } y^{-1} = y \\ &= (xy)^{-1}. \end{aligned}$$

Therefore, $(xy)^2 = e$.

Hence $xy \in$ H and H is a sub-group of G.

Example 32. For any two subgroups H and K of a group G following hold:

(1) $H \cap K$ is a subgroup of G.

(2) If H is normal in G then $H \cap K$ is normal in K.

(3) If H and K are both normal in G, then $H \cap K$ is normal in G.

Solution. (1) Since $e \in H \cap K$, $H \cap K$ is non-void.

Now $a, b \in H \cap K \Rightarrow a, b \in H$ and $a, b \in K$

$\Rightarrow ab^{-1} \in H$ and $ab^{-1} \in K$

$\Rightarrow ab^{-1} \in H \cap K$.

Hence $H \cap K$ is a subgroup of G.

(2) Let H be normal in G. Let $x \in K$, $a \in H \cap K$.

Then $x^{-1} ax \in K$ since $x, a \in K$.

Further $x^{-1} ax \in H$ since H is normal and $a \in H$. Consequently $x^{-1} ax \in H \cap K \; \forall \; x \in K$, $a \in H \cap K$.

Hence $H \cap K$ is a normal subgroup of K.

Example 33. If H is a subgroup of index 2 in a group G, then H is a normal subgroup of G.

Solution. Suppose H is a subgroup of index 2 in a group G so that number of distinct right (or left) cosets of H in G is 2.

To prove that H is normal in G, it suffices to show that

$Hx = xH \quad \forall \; x \in G$.

Let $x \in G$ be arbitrary. Then $x \in H$ or $x \notin H$.

If $x \in H$, then $Hx = xH = H$ and so $Hx = xH$

If $x \notin H$, then index of H is 2 says that right coset (left coset) decomposition contains only two cosets

$\therefore \; G = He \cup Hx$, $G = eH \cup x\,H$

Hence $H \cup Hx = G = H \cup xH \quad \Rightarrow xH = G - H = Hx$

$\Rightarrow xH = Hx$

$\therefore$ In either case $Hx = xH$, meaning thereby H is normal in G.

11.6. Cyclic Group

A Group G is called a cyclic group if, for some $a \in G$, every element of G is of the form a^n, where n is some integer i.e., $G = \{a^n : n \in Z\}$. The element a is then called a generator of G.

If G is a cyclic group generated by a, it is denoted by $G = <a>$. The elements of G are in the form

$\ldots\ldots a^{-2}, a^{-1}, a^0, 0, a, a^2, a^3 \ldots\ldots$

There may be more than one generator of a cyclic group. Every cyclic group has at least two generators, generator and inverse of it.

Example 34. The set of integers with respect to + *i.e.*, $(Z, +)$ is a cyclic group, a generator being 1.

Solution. We have $1^0 = 1$, $1^1 = 1$, $1^2 = 1 + 1 = 2$, $1^3 = 1 + 1 + 1 = 3$ and so on.

Similarly 1^{-1} = inverse of $1 = -1$

$1^{-2} = (1^2)^{-1} = -2$, $1^{-3} = (1^3)^{-1} = (3)^{-1} = -3$ and so on.

Thus each element of G can be expressed as some integral power of 1.

Similarly we can show that -1 is also a generator.

Example 35. *The multiplicative group $\{1, w, w^2\}$ is a cyclic group.*

Solution. We have $w^0 = 1$, $w^1 = w$, $w^2 = w^2$, $w^3 = 1$

and $(w^2)^0 = 1$, $(w^2)^1 = w^2$, $(w^2)^2 = w^4 = w$

Thus each element of the group can be expressed as some integral powers of w and w^2. Hence the group is a cyclic group with generators w and w^2.

Example 36. The group $(G, +_6)$ is a cyclic group where $G = \{0, 1, 2, 3, 4, 5\}$.

Solution. We see that

$1^1 = 1$, $1^2 = 1 +_6 1 = 2$, $1^3 = 1 +_6 1^2 = 3$, $1^4 = 1 +_6 1^3 = 1 +_6 3 = 4$, $1^5 = 1 +_6 1^4 = 1 +_6 4 = 5$, $1^6 = 0$

Thus $G = \{1^0, 1^2, 1^3, 1^4, 1^5, 1^6 = 0\}$

Hence G is a cyclic group and 1 is a generator.

Similarly, it can be shown that 5 is another generator.

Some Important Properties of Cyclic Groups

Theorem 11.18. Every cyclic group is an abelian group.

Solution. Let G be a cyclic group and let a be a generator of G so that

$$G = \langle a \rangle = \{a^n : n \in Z\}$$

If g_1 and g_2 are any two elements of G, there exist integers r and s such that $g_1 = a^r$ and $g_2 = a^s$. Then

$$g_1 g_2 = a^r a^s = a^{r+s} = a^{s+r} = a^s \cdot a^r = g_2 g_1$$

So, G is abelian.

Note: 1. The symmetric group S_3 is not cyclic, since it is not abelian.

The dihedral group D_4 is not cyclic, since it is not abelian.

2. An abelian group is not necessarily a cyclic group. For example, Klein's 4-group V is abelian but it is not cyclic.

Theorem 11.19. If a is a generator of a cyclic group G, then a^{-1} is also a generator of G.

Proof. Let $G = \langle a \rangle$ be a cyclic group generated by a. Let a^r be any element of G, where r is some integer. We can write $a^r = (a^{-1})^{-r}$. Since $-r$ is also some integer, therefore each element of G, is generated by a^{-1}. Thus a^{-1} is also a generator of G.

Theorem 11.20. If a cyclic group G is generated by an element a of order n, then a^m is a generator of G if and only if the greatest common divisor of m and n is 1 *i.e.*, if and only if m and n are relative primes.

Proof. Suppose m is relatively prime to n. Consider the cyclic subgroup $H = \{a^m\}$ of G generated by a^m. Obviously $H \subseteq G$ since each integral power of a^m will also be an integral power of a.

Since m is relatively prime to n, therefore, there exist two integers r and s such that $rm + sn = 1$.

So $a^{rm+sn} = a^1$

$\Rightarrow a^{rm} \cdot a^{sn} = a$

$\Rightarrow (a^m)^r = a$; since $a^{sn} = (a^n)^s = e^s = e$

So, each integral power of a will also be some integral power of a^m. Therefore, $G \subseteq H$. Hence $H = G$ and a^m is a generator of G.

Conversely, suppose a^m is a generator of G. Let the greatest common divisor of m and n be d and $d \neq 1$ *i.e.*, $d > 1$. Then m/d and n/d must be integers.

Now $(a^m)^{n/d} = (a^n)^{m/d} = e^{m/d} = e$, Obviously n/d is a positive integer less than n itself. Thus $o(a^m) < n$. Therefore a^m can not be a generator of G because the order of a^m is not equal to the order of G. Hence d must be equal to 1. Thus m is prime to n.

Example 37. How many generators are there of the cyclic group G of order 8?

Solution. Let a be generator of G. Then o $(a) = 8$. We can write G = $\{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8\}$

7 is prime to 8, therefore, a^7 is also a generator of G.

5 is prime to 8, therefore, a^5 is also a generator of G.

3 is prime to 8, therefore, a^3 is also a generator of G.

Thus there are only four generators of G *i.e.*, a, a^3, a^5, a^7

Example 38. Show that the group $(\{1, 2, 3, 4, 5, 6\}, \times_7)$ is cyclic. How many generators.

Solution. G be a given group. If there exists an element $a \in G$ such that $o(a) = 6$ *i.e.*, equal to the order of the group G then the group G will be a cyclic group and a will be a generator of G.

Note that $o(3) = 6$ because $3^1 = 3$, $3^2 = 3 \times_7 3 = 2$, $3^3 = 3^2 \times_7 3 = 6$, $3^4 = 6 \times_7 3 = 4$, $3^5 = 4 \times_7 3 = 5$, $3^6 \times_7 3 = 5 \times_7 3 = 1$ *i.e.*, the identity element.

So, G is cyclic and 3 is a generator of G. We can write

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

Now 5 is prime to 6. There 3^5 *i.e.*, 5 is also generator of G.

Infinite Cyclic Group

If H is a cyclic group generated by a subject to all the powers of a are distinct, then $H = \langle a \rangle$ is an infinite cyclic group.

Example 39. Let G be an infinite cyclic group generated by a. Show that

(*i*) $a^r = a^t$ if and only if $r = t$, where $r, t \in Z$.

(*ii*) G has exactly two generators.

Solution. (*i*) Suppose $a^r = a^t$ and $r = t$, Let $r > t$. Then $a^{r-t} = e$. Then $o(a)$ is finite, say, $o(a) = n$. Then G = $\{e, a, \ldots\ldots, a^{n-1}\}$, which is a contradiction since G is an infinite group. The converse is straightforward.

(*ii*) Let $G = \langle b \rangle$ for some $b \in G$. Since $a \in G = \langle b \rangle$ and $b \in G = \langle a \rangle$, $a = b^r$ and $b = a^t$ for some $r, t \in Z$. Thus, $a = b^r = (a^t)^r = a^{rt}$. Hence, by (*i*). $r^t = 1$. This implies that either $r = 1 = t$ or $r = -1 = t$. Thus, either $b = a$ or $b = a^{-1}$. Now from (*i*), $a = a^{-1}$. Therefore, G has exactly two generators.

1.7 Permutation Group

Let A be a finite set. Then a function $f : A \to A$ is said to be a **permutation** of A if

(*i*) f is one – one

(*ii*) f is onto

i.e. A bijection from A to itself is called a permutation of A.

The number of distinct elements in the finite set A is called the **degree** of permutation.

Consider a set $A = \{a_1, a_2, \ldots\ldots, a_n\}$ and let $f : A \to A$ be a bijection function. Then every element of A has a unique image in A, no two distinct elements of A have the same image, and every element of A has a unique pre-image, under f. Thus, the range of f is of the form

$$\text{Ran}(f) = \{f(a_1), f(a_2) \ldots\ldots f(a_n)\}$$

In the notation of relations the function f is given by

$$f = \{(a_1, f(a_1)), (a_2, f(a_2)), \ldots\ldots, (a_n, f(a_n))\}$$

This is written in two line notation as

$$f = \begin{pmatrix} a_1 & a_2 \ldots\ldots a_n \\ f(a_1) & f(a_2) \ldots\ldots f(a_n) \end{pmatrix}$$

Since A is a finite set, its elements can be ordered as the first, the second, ..., the nth. Therefore, it is convenient to take A to be a set of the form $\{1, 2, 3, \ldots, n\}$ for some positive integer n instead of $\{a_1, a_2, a_3, \ldots\ldots a_n\}$.

In general, a permutation f on the set $\{1, 2, 3, \ldots\ldots, n\}$ can be written as

$$f = \begin{pmatrix} 1 & 2 & 3 & \ldots\ldots n \\ f(1) & f(2) & f(3)\ldots\ldots f(n) \end{pmatrix}$$

Obviously, the order of the column in the symbol is immaterial so long as the corresponding elements above and below in that column remain unchanged.

Equality of Two Permutations

Let f and g be two permutations on a set X. Then $f = g$ if and only if $f(x) = g(x)$ for all x in X.

Example 40. Let f and g be given by

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \qquad g = \begin{pmatrix} 3 & 2 & 1 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Evidently $f(1) = 2 = g(1)$, $f(2) = 3 = g(2)$

$f(3) = 4 = g(3)$, $f(4) = 1 = g(4)$

Thus $f(x) = g(x)$ for all $x \in \{1, 2, 3, 4\}$ which implies $f = g$.

Identity Permutation

If each element of a permutation be replaced by itself. Then it is called the identity permutation and is denoted by the symbol I. For example,

$$I = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$$ is an identity permutation.

Product of Permutations (or Composition of Permutation)

The product of two permutations f and g of same degree is denoted by $f \circ g$ or fg, meaning first perform f and then perform g.

$$f = \begin{pmatrix} a_1 & a_2 & a_3 \ldots a_n \\ b_1 & b_2 & b_3 \ldots b_n \end{pmatrix},$$

$$g = \begin{pmatrix} b_1 & b_2 & b_3 \ldots b_n \\ c_1 & c_2 & c_3 \ldots c_n \end{pmatrix}.$$

Then $$f \circ g = \begin{pmatrix} a_1 & a_2 & a_3 \ldots a_n \\ c_1 & c_2 & c_3 \ldots c_n \end{pmatrix}.$$

For, f replaces a_1 by b_1 and then g replaces b_1 by c_1 so that $f \circ g$ replaces a_1 by c_1. Similarly $f \circ g$ replaces a_2 by c_2, a_3 by c_3,.... a_n by c_n.

Clearly $f \circ g$ is also a permutation on S.

It should be observed that the permutation g has been written in such a manner that the second row of f coincides with the first row of g. This is most essential in order to find $f \circ g$.

If we want to write gf, then f should be written in such a manner that the second row of g must coincide with the first row of f.

Example 41. Find the product of two permutations and show that it is not commutative.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \text{and} \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Solution.

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

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

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

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

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

We observe that $fg \neq gf$.

This shows that the product of two permutations is not commutative.

But it can be shown that permutation multiplication is associative.

Let $P_1 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ $P_2 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ $P_3 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$

$$\therefore \quad P_1(P_2P_3) = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\left[\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right]$$

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

and $$(P_1P_2)P_3 = \left[\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right]\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

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

$$\therefore \quad P_1(P_2P_3) = (P_1P_2)P_3$$

Inverse Permutation

Since a permutation is one-one onto map and hence it is inversible, *i.e.*, every permutation f on a set

$$P = \{a_1, a_2 \ldots\ldots, a_n\}.$$

has a unique inverse permutation denoted by f^{-1}.

Thus if $$f = \begin{pmatrix}a_1 & a_2 \ldots\ldots a_n\\ b_1 & b_2 \ldots\ldots b_n\end{pmatrix}$$

then $$f^{-1} = \begin{pmatrix}b_1 & b_2 \ldots\ldots b_n\\ a_1 & a_2 \ldots\ldots a_n\end{pmatrix}.$$

Total Number of Permutations

Let X be a set consisting of n distinct elements. Then the elements of X can be permuted in $n!$ distinct ways. If S_n be the set consisting of all permutations of degree n, then the set S_n will have $n!$ distinct permutations of degree n. This set S_n is called the symmetric set of permutations of degree n.

For example, if $A = \{1, 2, 3\}$, then $S_3 = \{p_0, p_1, p_2, p_3, p_4, p_5\}$ where

$$p_0 = I_H = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} \quad p_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \quad p_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \quad p_3 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

The multiplication table for the composition of permutations in S_3 is as given below:

Multiplication Table for S_3

$\circ$	p_0	p_1	p_2	p_3	p_4	p_5
p_0	p_0	p_1	p_2	p_3	p_4	p_5
p_1	p_1	p_2	p_0	p_5	p_3	p_4
p_2	p_2	p_0	p_1	p_4	p_5	p_3
p_3	p_3	p_4	p_5	p_0	p_1	p_2
p_4	p_4	p_5	p_3	p_2	p_0	p_1
p_5	p_5	p_3	p_4	p_1	p_2	p_0

The table shows that

(*i*) The multiplication of any two permutations of S_3 gives a permutation of S_3. So, S_3 is closed with respect to multiplication.

(*ii*) Associativity law holds for $(p_1\, p_3)\, p_4 = p_5\, p_4 = p_0$ and $p_1\, (p_3\, p_4) = p_1 p_1 = p_0$

(*iii*) Identity element exists, p_0 when composed with any permutation gives that permutation.

(*iv*) Every permutation has its own inverse.

Hence S_3 is a group. It is a non-commutative group since $p_1 p_2 \neq p_2 p_1$, $p_3 p_2 \neq p_2 p_3$

Let A be a set of degree n. Let P_n be the set of all permutations of degree n on A. Then $(P_n, *)$ is a group, called a **permutation group** and the operation * is the composition (multiplication) of permutations. This is proved in the following theorem.

Theorem 11.21. The set P_n of all permutation on n symbols is finite group of order $n!$ with respect to the binary composition of permutations. For $n \leq 2$, P_n is abelian and for $n > 2$ it is always non-abelian.

Proof Let $X = \{a_1, a_2, a_3, \ldots\ldots, a_n\}$ is a finite set. Since the different arrangements of the elements of X are $n!$, then the number of distinct permutations of degree n will be $n!$. If P_n is the set of all such permutations, then P_n has $n!$ distinct elements.

Closure Property : Let f and g be any two permutations in P_n where

$$f = \begin{pmatrix} b_1 & b_2 & b_3 & \ldots & b_n \\ c_1 & c_2 & c_3 & \ldots & c_n \end{pmatrix} \text{and } g = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ b_1 & b_2 & b_3 & \ldots & b_n \end{pmatrix}$$

be any two permutations of degree n. Then,

$$fg = \begin{pmatrix} b_1 & b_2 & \ldots & b_n \\ c_1 & c_2 & \ldots & c_n \end{pmatrix} \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ c_1 & c_2 & \ldots & c_n \end{pmatrix}$$

Since, $c_1, c_2, \ldots, c_n$ are also of arrangement of n elements $a_1, a_2, \ldots a_n$ of X, then fg is a permutation of degree n.

Thus $fg \in P_n$ for all $f, g \in P_n$

Hence, P_n is closed for the composition known as product of two permutations.

Associativity

Let $f = \begin{pmatrix} c_1 & c_2 & \ldots & c_n \\ d_1 & d_2 & \ldots & d_n \end{pmatrix}$, $g = \begin{pmatrix} b_1 & b_2 & \ldots & b_n \\ c_1 & c_2 & \ldots & c_n \end{pmatrix}$ and $h = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix}$

be any three permutations of degree n, then

$$fg = \begin{pmatrix} c_1 & c_2 & \dots & c_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix}\begin{pmatrix} b_1 & b_2 & \dots & b_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix} = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix}$$

$$(fg)\,h = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix} \quad \dots (1)$$

Also $$gh = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix}$$

$$f(gh) = \begin{pmatrix} c_1 & c_2 & \dots & c_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix} \quad \dots (2)$$

Now from (1) and (2), we get $(fg)\,h = f(gh)$

Hence, the composition is associative in P_n

Existence of Identity

The identity permutation of degree n is the identity element of P_n.

Let $f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$ and $I = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$

Then $$fI = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} = f$$

Also $$If = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} = f$$

Thus $fI = If = f$

Existence of Inverse

Let $f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$ be a permutation of degree n then the permutation

$f^{-1} = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$ is also a permutation of degree n.

Now, $$f f^{-1} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}\begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} = I$$

Also, $$f^{-1} f = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} = I$$

Therefore, f^{-1} is the inverse of f.

Therefore $(P_n, *)$ is a group of order $n!$ with respect to composition of permutations. For $n=1$, the set P_n has only one element and for $n = 2$, the number of elements in P_n is 2.

We know that every group of order one or of order two is abelian. Thus $(P_n, *)$ is a abelian group for $n \le 2$.

For $n > 2$, $(P_n, *)$ is not an abelian group as composition of permutation is not a commutative operation *i.e.* $fg \neq gf$.

The group $(P_n, *)$ is also called **symmetric group** of degree n and denoted by S_n.

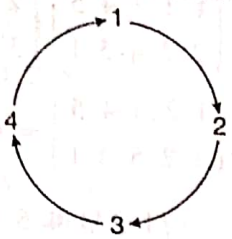
Cyclic Permutations

A permutation which replaces n objects cyclically is called a cyclic permutation of degree n.

Let us consider the permutation.

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

This assignment of values could be presented schematically as follows.



Such diagrams are cumbersome, we leave out the arrows and simply write S = (1 2 3 4). We read the new symbol in cyclical order from left to right as follows : 1 is replaced by 2, 2 is replaced by 3, 3 is replaced by 4, and 4 is replaced by 1.

Thus the meaning of the symbol is to replace each number which follows and the last number by the first.

Note that (1 2 3 4) = (2 3 4 1) = (3 4 1 2) = (4 1 2 3). Thus a circular permutation may be denoted by more than one rowed symbols.

The number of elements permuted by a cycle is said to be its **length** and the **disjoint cycles** are those which have no common elements. A cycle of length one means that the image of an element is the element itself and represents identity permutation. Cycles of length one are generally omitted.

Every permutation of a finite set can be expressed as a cycle or as a product of disjoint cycles *e.g.*,

$$t = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix}$$

is written as $t = (1, 2)\ (3, 4, 6)\ (5)$

The cycle (1, 2) has length 2. The cycle (3, 4, 6) has length 3 and the cycle (5) has length 1 and none of them have a symbol common and hence they are disjoint cycles.

Transpositions

A cyclic permutation such as (a, b) which interchanges the symbols leaving all other unchanged is called a transposition. In other words, transposition is cycle of length two of the form (a, b) *i.e.*, it is a mapping which maps each object onto itself excepting two, each of which is mapped on the other *e.g.*, (1, 2) is a transposition.

Every permutation can be resolved as a product of finite number of transpositions but the decomposition is not unique. However, for a given permutation the number of transpositions is always even or always odd.

The process consists of two steps:

(*i*) Express the permutation as a product of disjoint cycles.

(*ii*) Express each cycle as a product of transpositions.

Even and Odd Permutations

A permutation is said to be even or odd according as it can be expressed as a product of even or odd number of transpositions.

SOLVED EXAMPLES

Example 42. If $A = (1\ 2\ 3\ 4\ 5)$ and $B = (2\ 3)\ (4\ 5)$, find AB

Solution. We have $AB = (1\ 2\ 3\ 4\ 5)\ (2\ 3)\ (4\ 5)$

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

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

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} = (1\ 3\ 5).$$

Example 43. Express the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix}$ as a product of transpositions.

Solution. First we express the given permutation as a product of disjoint cycles. Here 1 is moved to 6 and then 6 to 1, giving the cycle (1, 6). Then 2 is moved to 5, which is moved to 3 which is moved to 2, giving (2, 5, 3). This takes care of all the elements except 4 which is left fixed. Thus

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = (1\,6)\,(2\,5\,3)$$

Multiplication of disjoint cycles is clearly commutative, so the order of the factors (1, 6) (2, 5, 3) is not important.

Example 44. Show that the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix}$ is odd, while the permutation

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix}$ is even.

Solution. We have $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix} = (1\ 5)\ (2\ 6\ 3)$

$$= (1\ 5)\ (2\ 6)\ (2\ 3)$$

Thus the given permutation can be expressed as the product of an odd number of transpositions and hence the permutation is an odd permutation.

Again $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (1\ 6)\ (2\ 3\ 4\ 5)$

$$= (1\ 6)\ (2\ 3)\ (2\ 4)\ (2\ 5)$$

Since it is a product of an even number of transpositions, the permutation is an even permutation.

Example 45. *Find the inverse of the permutation*

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

Solution. Let the inverse of the given permutation be

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ x & y & z & u & v \end{pmatrix}$$

Then $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ x & y & z & u & v \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

i.e., $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ y & z & x & v & u \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

$\therefore x = 3, y = 1, z = 2, u = 4, v = 5$

Hence the required inverse is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$.

f is a norm

Factor or Quotient Group

If H is a normal subgroup of a group G, then the set of all left cosets of G forms a group with respect to the multiplication of left coset and defined as

$$(aH)\,(bH) = (ab)\,H$$

called the factor group or quotient group of G by N and is denoted by G/N *i.e.* $G/H = \{gH : g \in G\}$.

One can similarly define multiplication of right cosets as $(H/a)(H/b) = H(ab)$ which makes the set of right cosets of H in G a group, also called the *factor group* of G by H. It is easy to observe that the factor groups obtained by left cosets and also by right cosets are isomorphic.

Theorem 11.26. Every homomorphism image of group G is isomorphic to some quotient group of G.

Proof. Let G′ be the homomorphic image of the group G, and f be the corresponding homomorphism.

Let K be the kernel of this homomorphism. Then K is a normal subgroup of G. We shall prove that

$G/k \cong G'$.

If $a \in G$, then $Ka \in G/K$ and $f(a) \in G'$. Consider the mapping

$\varphi : G/K \to G'$ such that $\varphi(Ka) = f(a)$, $\forall\ a \in G$.

First we shall show the mapping φ is well defined, *i.e.*, if $a, b \in G$ and $Ka = Kb$. Then $\varphi(Ka) = \varphi(Kb)$.

We have

$$Ka = Kb \Rightarrow ab^{-1} \in K$$
$$\Rightarrow f(ab') = e' \qquad \text{(the identity of G′)}$$
$$\Rightarrow f(a)\, f(b^{-1}) = e'$$
$$\Rightarrow f(a)\, (f(b))^{-1} = e'$$
$$\Rightarrow f(a)\, (f(b))^{-1}\, f(b) = e'\, f(b)$$

CHAPTER 12

Rings and Fields

12.1. Introduction

In the previous chapter, we studied group which is an algebraic structure with one binary operations. In this chapter we shall study ring which is an algebraic structure equipped with two binary operations. Our familiar examples of sets of numbers show that a study of sets on which two binary operations have been defined is of great importance. From the point of view of computer algebra and various applications such as complexity theory and coding theory, we need to look at more exotic systems such as rings and fields.

12.2. Ring

A ring $(R, +, .)$ is a set R together with two binary operations + (addition) and . (multiplication) defined on R such that the following axioms are satisfied :

(R_1) $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$.

(R_2) $a + b = b + a$ for all $a, b \in R$.

(R_3) There exists an element 0 in R such that $a + 0 = a$ for all $a \in R$.

(R_4) For all $a \in R$, there exists an element $-a \in R$ such that

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

(R_5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.

(R_6) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in R$. (Left distributive law)

(R_7) $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ for all $a, b, c \in R$. (Right distributive law)

We call 0, the **zero element** of the ring $(R, +, .)$.

That is, an algebraic system $(R, +, .)$ is called a ring if

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

(ii) $(R, \cdot)$ is semigroup *i.e.* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.

(iii) The operation is distributive over the operation +.

A ring R is called **commutative** if $a \cdot b = b \cdot a$ for all $a, b \in R$. It follows that a ring R is commutative if and only if the semigroup (R, .) is commutative. In a ring, an element $e \in R$ is called an unit (identity) element if $ea = a = ae$ for all $a \in R$. An unit element of a ring R (if it exists) is an element of the semigroup $(R, \cdot)$. The unit of a ring (if it exists) is generally denoted by 1. A ring R is called a ring with unity if it has an unit element.

The following are some examples of rings.

1. The set Z of integers under ordinary addition and multiplication is a commutative ring with unity 1. The unit elements of Z are 1 and – 1.

2. The set 2Z of even integers under ordinary addition and multiplication is a commutative ring without unity since there is no even integer e such that $e \times y = y \times e = y$ for all even integers y.

3. The set $Z_n = \{0, 1, 2, ..., n-1\}$ under addition and multiplication modulo n is a commutative ring with unity 1.

4. The set $M_2(Z)$ of 2×2 matrices with integer elements is a non commutative ring with unity.

5. $R = \{a + b\sqrt{-5} : a\ b \in Z\}$ is a ring for the usual addition and multiplication of complex numbers. It is a commutative ring with unit element $1 = 1 + 0\sqrt{-5}$.

Some Elementary Properties of a Ring

Let a, b and c belong to a ring R. Then

1. $a.0 = 0.a = 0$
2. $a.(-b) = (-a).b = -(a.b)$
3. $(-a).(-b) = a.b$
4. $a.(b-c) = a.b - a.c$ and $(b-c).a = b.a - c.a$

Proof. 1. We have $a.0 + a.a = a\,.\,(0 + a)$, right distributive law

$= a\,.\,a$, since $0 + a = a$

$= 0 + a\,.\,a$

Hence, by the right cancellation law, $a\,.\,0 = 0$

Similarly, by using the left distributive law, we can show that

$0\,.\,a = 0$

2. We have $a\,.\,(-b + b) = a\,.\,(-b) + a\,.\,b$, right distributive law

i.e. $a\,.\,0 = a\,.\,(-b) + a\,.\,b$, $(-b)$ is the additive inverse of b.

$0 = a\,.\,(-b) + a\,.\,b$ from (1) above.

Therefore $a\,.\,(-b)$ is an additive inverse of $a\,.\,b$.

Hence $a\,.\,(-b) = -(a\,.\,b)$.

Similarly, by using the left distributive law, we can easily show

That $(-a)\,.\,b = -(a\,.\,b)$.

3. From the two results of 2 we have

$(-a)\,.\,(-b) = -[(-a)\,.\,(b)] = -[-(a\,.\,b)] = a\,.\,b$,

since the inverse of the inverse of an element is the element itself in any group *i.e.* $-(-x) = x$

4. We have $a\,.\,(b-c) = a\,.\,[b + (-c)]$

$= a\,.\,b + a\,.\,(-c)$, right distributive law

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

$= a\,.\,b - a\,.\,c$.

Similarly, using the left distributive law, we can show that,

$(b-c)\,.\,a = b\,.\,a - c\,.\,a$.

Example 1. Prove that if $a, b \in R$ then $(a + b)^2 = a^2 + ab + ba + b^2$.

Solution. We have

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

$= a(a+b) + b(a+b)$ [by right distributive law]

$= (aa + ab) + (ba + bb)$ [by left distributive law]

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

Example 2. If R is a system satisfying all the conditions for a ring with unit element with the possible exception of $a + b = b + a$, prove that the axiom $a + b = b + a$ must hold in R and that R is thus a ring.

Solution. Since 1 is an element of R, we have

$$(a+b)(1+1) = a(1+1) + b(1+1) \quad \text{[by right distributive law]}$$
$$= (a1 + a1) + (b1 + b1) = (a+a) + (b+b) \quad \ldots(i)$$

Also
$$(a+b)(1+1) = (a+b)1 + (a+b)1. \quad \text{by left distributive law}$$
$$= (a+b) + (a+b) \quad \ldots(ii)$$
[$\because$ 1 is the unit element]

From (i) and (ii), we get

$$(a+a) + (b+b) = (a+b) + (a+b)$$
$$\Rightarrow \quad [(a+a)+b] + b = [(a+b)+a] + b \quad \text{[by associativity of addition]}$$
$$\Rightarrow \quad (a+a) + b = (a+b) + a \quad \text{[by right cancellation law for addition in R]}$$
$$\Rightarrow \quad a + (a+b) = a + (b+a) \quad \text{[by associativity of addition in R]}$$
$$\Rightarrow \quad (a+b) = b + a \quad \text{[by right cancellation law for addition in R]}$$

Thus addition is commutative in R. Hence R is a ring.

Example 3. If in a ring R with unity, $(xy)^2 = x^2y^2$ for all $x, y \in R$, then R is commutative.

Solution. Since 1 is an element of R, for all $x, y \in R$

$$[x(y+1)]^2 = x^2(y+1)^2$$
$$\Rightarrow \quad [x(y+1)][x(y+1)] = x^2(y+1)(y+1)$$
$$\Rightarrow \quad (xy+x)(xy+x) = x^2[y(y+1)+1(y+1)]$$
$$\Rightarrow \quad [xy(xy+x) + x(xy+x)] = x^2(y^2+y+y+1)$$
$$\Rightarrow \quad (xy)^2 + xyx + x^2y + x^2 = x^2y^2 + 2x^2y + x^2 \quad \ldots(1)$$
$$\Rightarrow \quad xyx = x^2y$$

Replacing x by $x + 1$, we get

$$(x+1)y(x+1) = (x+1)^2y$$
$$\Rightarrow \quad (xy+y)(x+1) = (x^2+2x+1)y$$
$$\Rightarrow \quad (xy+y)x + (xy+y)1 = x^2y + 2xy + y$$
$$\Rightarrow \quad xyx + yx + xy + y = x^2y + 2xy + y$$
$$\Rightarrow \quad yx = xy \quad \text{since } xyx = x^2y \text{ by (1)}$$

Hence R is a commutative ring.

Example 4. If R is a ring such that $a^2 = a \; \forall \; a \in R$ porve that

(i) $a + a = 0 \; \forall \; a \in R$ i.e., each element of R is its own additive inverse.

(ii) $a + b = 0 \Rightarrow a = b$. *(iii) R is a commutative ring.*

Solution. (i) $a \in R \Rightarrow a + a \in R$.

Now
$$(a+a)^2 = (a+a) \quad \text{[by assumption } a^2 = a\text{]}$$
$$\Rightarrow \quad (a+a)(a+a) = a+a \quad \text{[by left distibutive law]}$$
$$\Rightarrow \quad (a+a)a + (a+a)a = a+a \quad \text{[by right distibutive law]}$$
$$\Rightarrow \quad (a^2+a^2) + (a^2+a^2) = a+a \quad \because a^2 = a$$
$$\Rightarrow \quad (a+a) + (a+a) = a+a$$
$$\Rightarrow \quad (a+a) + (a+a) = (a+a) + 0 \quad \because a + 0 = a$$
$$\Rightarrow \quad (a+a) = 0 \quad \text{[by left cancellation law for addition in R]}$$
$$\Rightarrow$$

(*ii*) $a + b = 0 \Rightarrow a + b = a + a$ using (*i*)

$\Rightarrow b = a$ [by left cancellation law]

$\Rightarrow a = b$

(*iii*) We have

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

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

$\Rightarrow (a + b)a + (a + b)b = a + b$ [by left distributive law]

$\Rightarrow (a^2 + ba) + (ab + b^2) = a + b$ [by right distributive law]

$\Rightarrow (a + ba) + (ab + b) = a + b$ $\because a^2 = a, b^2 = b$

$\Rightarrow (a + b) + (ba + ab) = (a + b) + 0$

[by commutativity and associativity of addition]

$\Rightarrow ba + ab = 0$ [by left cancellation law]

$\Rightarrow ab = ba.$ by (*ii*)

$\therefore$ R is commutative ring.

CHAPTER 8

Function

8.1. Introduction

In this chapter we study a particular class of relations called functions. Function plays an important role in Mathematics, Computer Science and many applications. We are primarily concerned with discrete functions which transform a finite set into another finite set. Computer output can be considered as a function of the input. A compiler transforms a program into a set of machine language instructions (the object program). Functions can also be used for counting and establishing the cardinality of sets. We discuss here the basic properties of functions, several types and their applications.

8.2. Function

A function is a special case of relation. To be specific, let A, B be two non-empty sets and R be a relation from A to B, then R may not relate an element of A to an element of B or it may relate an element of A to more than one element of B. But a function relates each element of A to a unique element of B.

Definition

Let A and B be two non-empty sets. A function f from A to B is a set of ordered pairs

$$f \subseteq A \times B$$

with the property that for each element x in A there is a unique element y in B such that $(x, y) \in f$. The statement "f is a function from A to B" is usually represented symbolically by

$$f : A \to B \quad \text{or} \quad A \xrightarrow{f} B.$$

A function can be represented pictorially as shown in Fig. 8.1

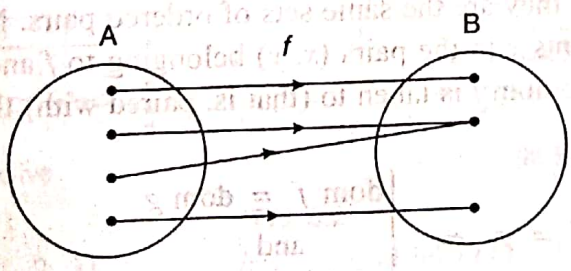


Fig. 8.1

It must be noted here (*i*) that there may be some elements of the set B which are not associated to any element of the set A. (*ii*) That each element of the set A must be associated to one and only one element of the set B.

If f is a function from A to B, then A is called the **domain** of f denoted by dom f, its members are the first co-ordinates of the ordered pairs belonging to f and the set B is called the

co-domain. If $(x, y) \in f$, it is customary to write $y = f(x)$, y is called the **image** of x; and x is a **pre-image** of y. y is also called the value of f at x. The set consisting of all the images of the elements of A under the function f is called the **range** of f. It is denoted by $f(A)$.

Thus range of $f = \{f(x) : \text{for all } x \in A\}$.

Note that range of f is a subset of B (co-domain) which may or may not be equal to B.

Example 1. Let A = {1, 2, 3, 4, 5}, B = {0, 1, 2, 3, 5, 7, 9, 12, 13} and

(*i*) f = {(1, 1), (2, 0), (3, 7), (4, 9), (5, 12)}, then f is a function from A to B because each element of A has a unique image in B and no element of A has two or more images in B. Range of f = {1, 0, 7, 9, 12}

Note that some elements of B are not associated with any element of A.

(*ii*) f = {(1, 3), (2, 3), (3, 5), (4, 9), (5, 9)}, then f is a function from A to B because each element of A has a unique image in B. Range of f = {3, 5, 9}

Note that the second component may repeat

(*iii*) f = {(1, 1), (2, 3), (4,7), (5, 12)}, then f is not a function from A to B because the element 3 of A has no image in B.

(*iv*) f = {(1, 1), (2, 3), (3, 5), (3, 7), (4, 9)}, then f is not a function because the different pairs (3, 5) and (3, 7) have same first component.

It is sometimes convenient to view a function as a rule or formula which, when given an input, produces a single output. If more than one output is produced, the rule is not a function. This can be defined as

A function $f: A \to B$ is a rule or formula that assigns to each element x in A a unique element in B. denoted by $f(x)$. If the domain and range of a function are numbers then the function is typically defined by means of algebraic formula.

For example, $f(x) = x^2$ for $x \in R$ represents a function where R is the set of real numbers and $f: R \to R$. Such functions are called **numeric functions**

Terms such as "transforms", "map", "correspondence", and "operation" are used as synonyms for "function". We may think of f as a kind of programmed machine that exists a unique element of B whenever an element of A is fed in : input x always yield output $f(x)$.

The symbol "f" has no special significance. It is the first letter of the word "function", but any other letter would do as well, *e.g.*, $g(x)$, $h(x)$, ...$\varphi(x)$, $\psi(x)$ etc.

We have defined a function as a set of ordered pairs satisfying certain conditions; accordingly functions f and g are equal if they are the same sets of ordered pairs. Notice that dom f consists of all the first-coordinate elements x in the pairs (x, y) belonging to f and g. The equation $f = g$ also implies that each element $x \in \text{dom } f$ is taken to (that is, paired with) the same element by f as it is by g. It follows that

$$f = g \Leftrightarrow \begin{cases} \text{dom } f = \text{dom } g \\ \text{and} \\ f(x) = g(x) \; \forall \; x \in \text{dom } f \end{cases}$$

In computer jargon: functions f and g are equal if they have the same sets of acceptable input and produce the same output for each piece of input.

8.3. Classification of Functions

Functions can be classified mainly into two groups.

1. **Algebraic function.** A function which consists of a finite number of terms involving powers and roots of the independent variable x and the four fundamental operations of addition, subtraction.

multiplication and division is called algebraic function. Three particular cases of algebraic functions are:

(*i*) **Polynomial functions.** A function of the form $a_0 x^n + a_1 x^{n-1} + ... + a_n$ where n is a positive integer and $a_0, a_1, ..., a_n$ are real constants and $a_0 \neq 0$ is called a polynomial of x in degree n e.g. $f(x) = 2x^3 + 5x^2 + 7x - 3$ is a polynomial of degree 3.

(*ii*) **Rational functions.** A function of the form $\frac{f(x)}{g(x)}$ where $f(x)$ and $g(x)$ are polynomials in x, $g(x) \neq 0$ is called a rational function, e.g., $F(x) = \frac{x^2 + 2x + 1}{x + 2}$

(*iii*) **Irrational functions.** The functions involving radicals are called irrational functions. $f(x) = \sqrt[3]{x} + 5$ is an irrational function.

2. Transcendental functions. A function which is not algebraic is called transcendental function.

(*i*) **Trigonometric functions.** The six functions $\sin x$, $\cos x$, $\tan x$, $\sec x$, $\operatorname{cosec} x$, $\cot x$ where the angle x is measured in radian are called trigonometric functions.

(*ii*) **Inverse trigonometric functions.** The six functions $\sin^{-1} x$, $\cos^{-1} x$, $\tan^{-1} x$, $\cot^{-1} x$, $\sec^{-1} x$, $\operatorname{cosec}^{-1} x$ are called inverse trigonometric functions.

(*iii*) **Exponential functions.** A function $f(x) = a^x$ $(a > 0)$ satisfying the law $a^1 = a$ and $a^x \, a^y = a^{x+y}$ is called the exponential function.

(*iv*) **Logarithm functions.** The inverse of the exponential function is called the logarithm function.

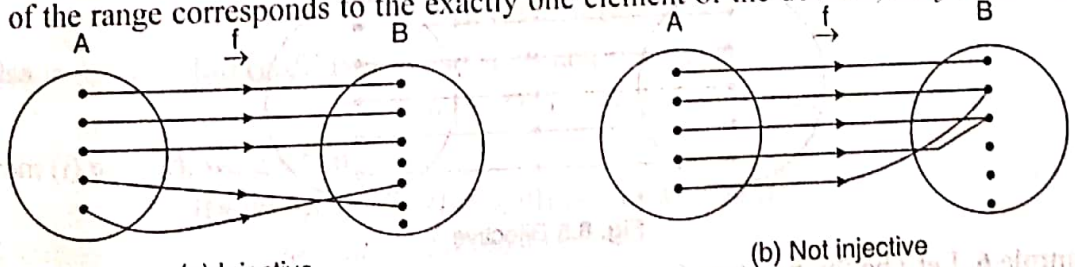
So, if $y = a^x$ $(a > 0, a = 1, x \in R, y > 0)$ then $x = \log_a y$ is called Logarithm function.

8.4. Types of Functions

The functions can be of different types. These functions are important in mathematics and in many applications of computer science.

One-to-one Function. A function from A into B is one-to-one or **injective**, if for all elements x_1, x_2 in A such that $f(x_1) = f(x_2)$. implies $x_1 = x_2$

That is, if no elements of A are assigned to the same element in B or equivalently, if each element of the range corresponds to the exactly one element of the domain, the f is one-to-one.



(a) Injective (b) Not injective

Fig. 8.2

Example 2. Let A = {1, 2, 3}, B = {*a*, *b*, *c*, *d*} and let $f(1) = a$, $f(2) = c$ and $f(3) = d$. Then f is injective since the different elements 1, 2, 3 in A are assigned to the different elements a, c, d respectively in B.

Example 3. If $f(x) = 3x - 1$ is one-to-one function because

$$f(x_1) = f(x_2) \Rightarrow 3x_1 - 1 = 3x_2 - 1 \Rightarrow x_1 = x_2.$$

Many-one Function. A function f from A to B is said to be many-one if and only if two or more elements of A have same image in B.

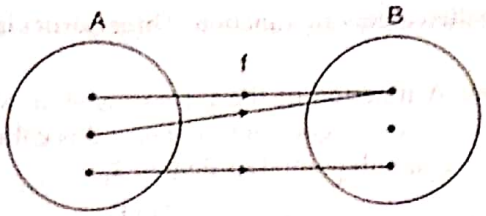


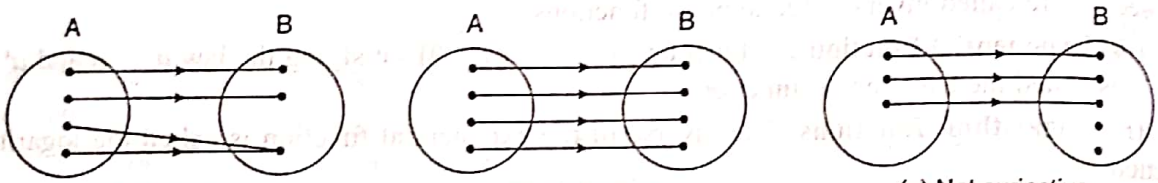
Fig. 8.3 Many-one function

Example 4. Let $f(x) = x^2$, x is any real number and $f: R \to R$, then f is many-one function. For $x = 1$, $f(1) = 1^2 = 1$ and $x = -1$, $f(-1) = (-1)^2 = 1$. Thus we find $f(1) = f(-1) = 1$ which shows that two distinct numbers -1 and 1 are assigned to the same number 1 under f. Therefore, f is many-one function.

Into Function. A function f from A to B is called into function if and only if there exists at least one element in B which is not the image of any element in A, *i.e.*, the range of f is a proper subset of co-domain of f.

Onto Function. A function f from A to B is onto, or **surjective** if every element of B is the image of some element in A, that is, if B = range of f [Figs. 8.4 (*a*) and (*b*)]

In order to check whether $y = f(x)$ from a set A to set B is onto or not, write x in terms of y and see if for every $y \in B$, $x \in A$. If so, it is onto. Otherwise, it is into.



(a) Surjective (b) Surjective (c) Not surjective

Fig. 8.4

Example 5. Let $f(x) = x^2$, x is any real number and $f: R \to R$, then f is not onto. The reason is that we cannot find a real number whose square is negative, then the range of f cannot be equal to R.

Bijective Function. A function f from A to B is said to be bijective if f is both injective and surjective *i.e.*, both one-to-one and onto [Fig. 8.5].

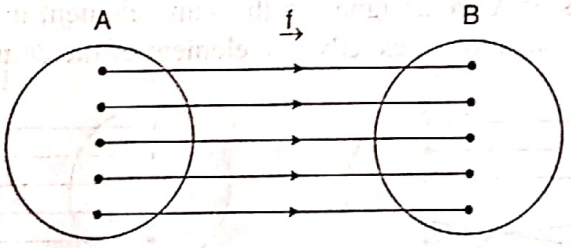


Fig. 8.5 Bijective

Example 6. Let f be the function from A to B where A = {1, 2, 3, 4} and B = {a, b, c, d} with $f(1) = d, f(2) = b, f(3) = c$ and $f(4) = a$, then f is bijective function. f is one-one since the function takes on distinct values. It is also onto since every element of B is the image of some element in A. Hence f is a bijective function.

8.5. Composition of Functions

Let $f: A \to B$ and $g: B \to C$. The composition of f and g, denoted by gof, read as 'g of f' results in a new function from A to C and is given by $(gof)(x) = g(f(x))$ for all x in A. Hence, the composition gof first applies f to map A into B, and it then employs g to map B to C. In other

words, the range space of f becomes the domain space of g, Fig. 8.6 illustrates the composition of the two functions f and g.

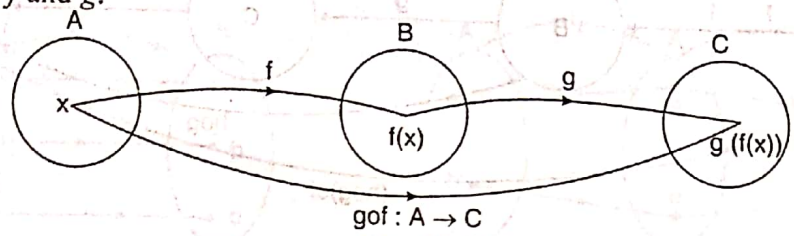


Fig. 8.6

Example 7. Let A = {1, 2, 3}, B = {a, b} and C = {r, s} and f : A → B be defined by $f(1) = a, f(2) = a, f(3) = b$ and g : B → C be defined by $g(a) = s$, $g(b) = r$.

Then gof : A → C is defined by

$$(gof)(1) = g(f(1)) = g(a) = s$$
$$(gof)(2) = g(f(2)) = g(a) = s$$
$$(gof)(3) = g(f(3)) = g(b) = r$$

Example 8. If f : R → R and g : R → R are defined by the formulas

$f(x) = x + 2$ for all x in R and $g(x) = x^2$ for all x in R

Then $(gof)(x) = g(f(x)) = g(x + 2) = (x + 2)^2 = x^2 + 4x + 4$

And $(fog)(x) = f(g(x)) = f(x^2) = x^2 + 2$

Note that $gof \neq fog$ since, for example $(gof)(1) = g(f(1)) = g(1 + 2) = g(3) = 3^2 = 9$, while $(fog)(1) = f(g(1)) = f(1^2) = f(1) = 1 + 2 = 3$.

Thus the composition of function is not commutative. However, the associate law is true for functions under the operation of compositions.

Theorem 8.1 (Associative law of Function Composition) Let f : A → B, g : B → C and h : C → D Then $ho\ (gof) = (hog)\ of$

Proof. Since f : A → B, g : B → C and h : C → D, then gof : A → C and hog : B → D.

Hence $ho\ (gof)$: A → D and $(hog)\ of$: A → D

So $dom\ [ho\ (gof)] = dom\ [(hog)\ of]$

Let $x \in A$, $y \in B$, $z \in C$ such that $f(x) = y$ and $g(y) = z$

Then
$$[(hog)\ o\ f](x) = (hog)[f(x)] = (hog)(y)$$
$$= h[g(y)] = h(z) \quad \ldots (i)$$

Also
$$[ho\ (gof)](x) = [ho\ (gof)(x)] = h[(gof)(x)]$$
$$= h[g(f(x))] = h[g(y)] = h(z) \quad \ldots (ii)$$

From (i) and (ii), we get that

$$[(hog)\ of](x) = [ho\ (gof)](x) \text{ for all } x \text{ in } A.$$
$$\Rightarrow \quad (hog)\ of = ho\ (gof)$$

This completes the proof.

The associative law of function composition can be represented pictorially as shown in Fig. 8.7 and Fig 8.8.

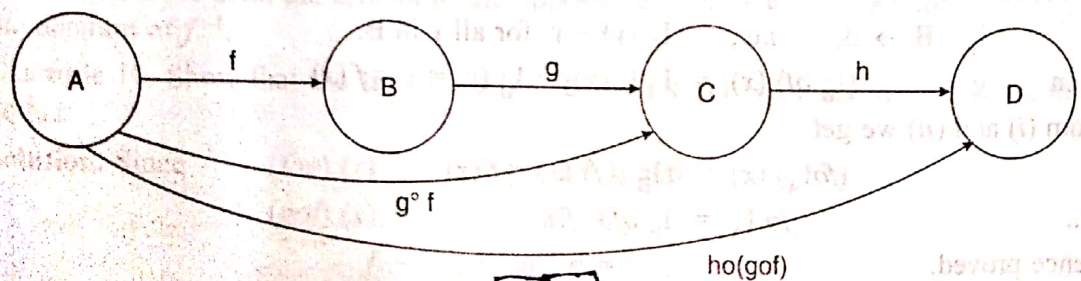


Fig. 8.7

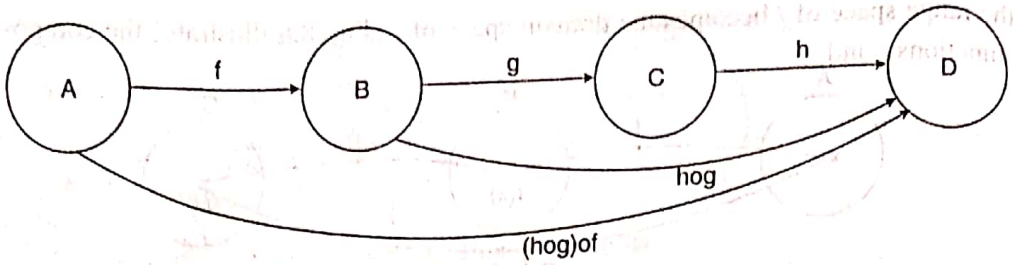


Fig. 8.8

Theorem 8.2. Let $f : A \to B$ and $g : B \to C$ be functions.

(*a*) If f and g are injections then $gof : A \to C$ is an injection.

(*b*) If f and g are surjections then so is gof.

(*c*) If f and g are bijections, then so is gof.

Proof. (*a*) Let $a_1, a_2 \in A$. By definition of composition,

we have $(gof)(a_1) = (gof)(a_2) \Rightarrow g(f(a_1)) = g(f(a_2))$

$\Rightarrow f(a_1) = f(a_2)$ since g is injective

$\Rightarrow a_1 = a_2$ since f is injective

Therefore gof is injective.

(*b*) Let $c \in C$. Then we can find an element an $a \in A$ such that $(gof)(a) = c$. Since g is onto C, there is an element $b \in B$ such that $g(b) = c$. Then, since f is onto B, there exists $a \in A$ such that $f(a) = b$. Thus $(gof)(a) = g(f(a)) = g(b) = c$

(*c*) This part follows immediately from the preceding parts. This completes the proof.

Compositions are closely related to computing, Consider the following two statements

$$y = x + 2;$$
$$z = 3 * y$$

The first value of z depends, of course, on the initial value of x, which makes z a function of x. This function can be interpreted as a composition of the two functions $f(x) = x + 2$ and $g(y) = 3*y$. Thus the sequence of assignment statements can be interpreted as function composition.

Identity Function

The function $f : A \to A$ defined by $f(x) = x$ for every $x \in A$ is called the identity of A and is denoted by I_A.

Theorem 8.3. The composition of any function with the identity function is the function itself, *i.e.*, $(f \circ I_A)(x) = (I_B \circ f)(x) = f(x)$

Proof. Let A and B be two non-empty sets. Let I_A be the identity function on A and let $f : A \to B$. Let $x \in A$ and $y \in B$, so that $y = f(x)$.

So $I_A : A \to A$, *i.e.*, $I_A(x) = x$, for all x in A.

By the definition of the composite function $fo\ I_A : A \to B$, then

$$(fo\ I_A)(x) = f[I_A(x)] = f(x) \quad \ldots (i)$$

Again, let $f : A \to B$ and I_B be the identity function on B.

So $I_B : B \to B$, *i.e.*, $I_B(y) = y$, for all y in B.

Then $(I_B\ of)(x) = I_B[f(x)] = I_B(y) = y = f(x)$ ... (*ii*)

From (*i*) and (*ii*) we get

$$(foI_A)(x) = (I_B \circ f)(x) = f(x)$$

i.e., $fo\ I_A = I_B\ of = f$.

Hence proved.

In particular, if $f: A \to A$, then $fo\ I_A = I_A\ of = f$.

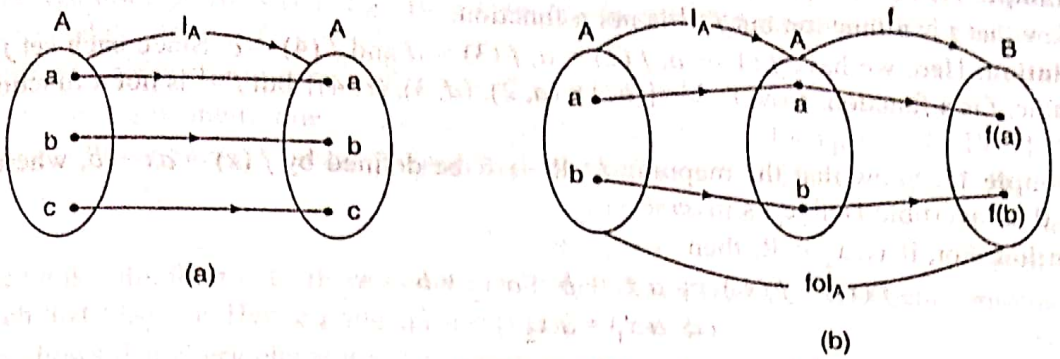


Fig. 8.9

Inverse of a function

Let $f: A \to B$. A map $g: B \to A$ is called the inverse of f if $gof = I_A$ and $fog = I_B$

i.e., $g[f(x)] = x$ for all $x \in A$ and $f[g(y)] = y$ for all $y \in B$

Thus, if $f(x) = y$ then $g(y) = g[f(x)] = x$.

The inverse g of f is denoted by f^{-1}

Thus $f(x) = y \Leftrightarrow x = f^{-1}(y)$

A necessary and sufficient condition for $f: A \to B$ to have the inverse of $f^{-1}: B \to A$ is that f be bijective. Then f takes x to y and f^{-1} takes y to x. Thus for a bijective f, f^{-1} is obtained by 'reversing' arrows. The concept of inverse function is illustrated in the following example.

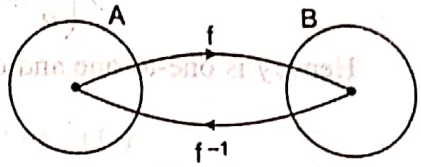


Fig. 8.10

Example 9. Let the function $f: A \to B$ be defined by the diagram as shown in Fig. 8.11

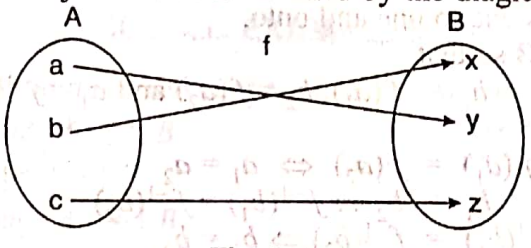


Fig. 8.11

Then f is one to one and onto. Therefore f^{-1}, the inverse function, exists. One can describe $f^{-1}: B \to A$ by the diagram as shown in Fig. 8.12.

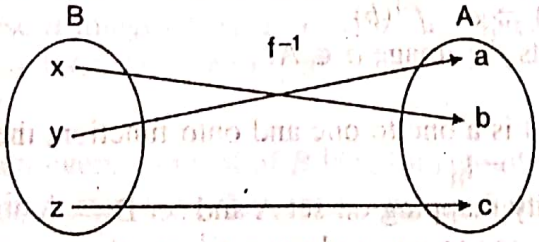


Fig. 8.12

Notice that if we send the arrows in the opposite direction in the diagram of f we essentially have the diagram of f^{-1}.

Example 10. Show that the function $f(x) = x^3$ and $g(x) = x^{1/3}$ for all $x \in R$ are inverses of one another.

Solution. Since $(fog)(x) = f(x^{1/3}) = x = I_x$ and

$(gof)(x) = g(x^3) = x = I_x$

then $f = g^{-1}$ or $g = f^{-1}$

Example 11. Let A = {1, 2, 3, 4} and B = {*a*, *b*, *c*, *d*}, and let $f = \{(1, a), (2, a), (3, d), (4, c)\}$. Show that f is a function but f^{-1} is not a function.

Solution. Here we have $f(1) = a$, $f(2) = a$, $f(3) = d$ and $f(4) = c$. Since each set $f(n)$ is a single value, f is a function. Now $f^{-1} = \{(a, 1), (a, 2), (d, 3), (c, 4)\}$ but f^{-1} is not a function, since $f^{-1}(a) = \{1, 2\}$

Example 12. Show that the mapping $f : \mathrm{R} \to \mathrm{R}$ be defined by $f(x) = ax + b$, where $a, b, x \in \mathrm{R}$, $a \neq 0$ is invertible Define its inverse.

Solution. For, if $x_1, x_2 \in \mathrm{R}$, then

$$f(x_1) = f(x_2) \Rightarrow a x_1 + b = a x_2 + b$$
$$\Rightarrow a x_1 = a x_2$$
$$\Rightarrow x_1 = x_2$$

This proves f is one-to-one.

Again, if $y \in \mathrm{R}$.

$$y = f(x) \Rightarrow y = a x + b$$
$$\Rightarrow x = (y - b)/a$$

Thus for $x \in \mathrm{R}$, there exists $(y - b)/a \in \mathrm{R}$ such that

$$f\left(\frac{1}{a}(y-b)\right) = a\left(\frac{1}{a}(y-b)\right) + b = y - b + b = y$$

Hence f is one-to-one and onto therefore f^{-1} exists and it is defined by

$$f^{-1}(y) = \frac{1}{a}(y - b)$$

Theorem 8.4 If a mapping $f : \mathrm{A} \to \mathrm{B}$ is one-to-one and onto, then prove that inverse mapping $f^{-1} : \mathrm{B} \to \mathrm{A}$ is also one-to-one and onto.

Proof. Here $f : \mathrm{A} \to \mathrm{B}$ is one to one and onto.

$a_1, a_2 \in \mathrm{A}$ and $b_1, b_2 \in \mathrm{B}$ so that

$$b_1 = f(a_1),\ b_2 = f(a_2) \text{ and } a_1 = f^{-1}(b_1),\ a_2 = f^{-1}(b_2)$$

As f is one to one

$$f(a_1) = f(a_2) \Leftrightarrow a_1 = a_2$$

or
$$b_1 = b_2 \Leftrightarrow f^{-1}(b_1) = f^{-1}(b_2)$$

i.e.,
$$f^{-1}(b_1) = f^{-1}(b_2) \Rightarrow b_1 = b_2$$

$\therefore$ f^{-1} is one to one function.

As f is onto.

Every element of B is associated with a unique element of A *i.e.*, for any $a \in \mathrm{A}$ is pre-image of some $b \in \mathrm{B}$ where $b = f(a) \Rightarrow a = f^{-1}(b)$

i.e., for $b \in \mathrm{B}$, there exists f^{-1} image $a \in \mathrm{A}$.

Hence f^{-1} is onto.

Theorem 8.5 If $\mathrm{f} : \mathrm{A} \to \mathrm{B}$ is a one to one and onto function, then

(*a*) $f^{-1}of = \mathrm{I_A}$ and (*b*) $fof^{-1} = \mathrm{I_B}$

where $\mathrm{I_A}$ and $\mathrm{I_B}$ are identity mapping on set A and set B.

Proof: Since $f : a \to \mathrm{B}$ is one to one and onto, f^{-1} exists.

For all $\mathrm{a} \in \mathrm{A}$, $\mathrm{b} \in \mathrm{B}$, we have

$$b = f(a), a = f^{-1}(\mathrm{b})$$
$\Rightarrow$
$$b = f(f^{-1}(b))$$
$$= (fof^{-1})b \text{ for all } b \in \mathrm{B}$$
$\therefore$
$$\mathrm{I_B} = fof^{-1}. \text{ Hence } fof^{-1} \text{ is identity function on B.}$$

Again
$$\mathrm{a} = f^{-1}(b)$$
$$= f^{-1}(f(a)) \text{ for all } a \in \mathrm{B}$$
$$= (f^{-1}of)a$$
$\therefore$
$$\mathrm{I_A} = f^{-1}of. \text{ Hence } f^{-1}of \text{ is identity function on A.}$$

Theorem 8.6 If $f : A \to B$ and $g : B \to C$ be one-to-one onto functions, then $g \circ f$ is also one-to-one onto and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

Proof. Since f is one-to-one, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ for $x_1, x_2 \in R$

Again since g is one-to-one, $g(y_1) = g(y_2) \Rightarrow y_1 = y_2$ for $y_1, y_2 \in R$

Now $g \circ f$ is one-to-one, since $(gof)(x_1) = (gof)(x_2) \Rightarrow g[f(x_1)] = g[f(x_2)]$

$\Rightarrow f(x_1) = f(x_2)$ [g is one-to-one]

$\Rightarrow x_1 = x_2$ [f is one-to-one]

Since g is onto, for $z \in C$, there exists $y \in B$ such that $g(y) = z$. Also f being onto there exists $x \in A$ such that $f(x) = y$. Hence $z = g(y) = g[f(x)] = (gof)(x)$

This shows that every element $z \in C$ has pre image under $g \circ f$. So, $g \circ f$ is onto.

Thus $g \circ f$ is one-to-one onto function and hence $(gof)^{-1}$ exists.

By the definition of the composite functions, $gof : A \to C$. So, $(gof)^{-1} : C \to A$.

Also $g^{-1} : C \to B$ and $f^{-1} : B \to A$.

Then by the definition of composite functions, $f^{-1} og^{-1} : C \to A$.

Therefore, the domain of $(gof)^{-1}$ = the domain of $f^{-1} og^{-1}$.

Now $(gof)^{-1}(z) = x \Leftrightarrow (gof)(x) = z$

$\Leftrightarrow g(f(x)) = z$

$\Leftrightarrow g(y) = z$ where $y = f(x)$

$\Leftrightarrow y = g^{-1}(z)$

$\Leftrightarrow f^{-1}(y) = f^{-1}(g^{-1}(z)) = (f^{-1} og^{-1})(z)$

$\Leftrightarrow x = (f^{-1} og^{-1})(z)$ [$f^{-1}(y) = x$]

Thus $(gof)^{-1}(z) = (f^{-1} og^{-1})(z)$. So $(gof)^{-1} = f^{-1} \circ g^{-1}$.

SOLVED EXAMPLES

Example 13. *Let A and B be finite sets and $f : A \to B$. Then show that*

(i) If f is one-to-one, then $|A| \leq |B|$.

(ii) If f is onto, then $|B| \leq |A|$.

(iii) If f is a bijection, then $|A| = |B|$.

Solution. Let $A = \{a_1, a_2, ...a_n\}$ and $B = \{b_1, b_2, ... b_m\}$

so that $|A| = n$ and $|B| = m$.

(*i*) Suppose f is one-to-noe. Then the n images of the elements of A, *i.e.* $f(a_1), f(a_2), ...f(a_n)$ are all different. Since all these n images belong to B, it must have at least n elements, that is, $|B| \leq n$. But $|A| = n$, so $|B| \geq |A|$. *i.e.*, $|A| \leq |B|$.

Hence proved.

(*ii*) Suppose f is onto. Then every element of B is the image of some element in A. Since the two or more distinct elements in A may have the same image in B, then $|B| \leq n$, *i.e.* $|B| \leq |A|$.

(*iii*) Suppose f is a bijection. Then f is both one-to-one and onto. From (*i*) and (*ii*) it follows $|A| \leq |B|$ and $|B| \leq |A|$. Therefore, $|A| = |B|$.

Example 14. *Let $A = \{1, 2\}$ and $B = \{a, b\}$ find all functions $f : A \to B$ and for each such functions, determine whether it is one-to-one, onto, both, or neither.*

Solution. There are four (2^2) functions $f : A \to B$. They are listed below in tabular form.

x	f_1	f_2	f_3	f_4
1	a	a	b	b
2	a	b	a	b

Here f_1 is defined as $f_1(1) = a$; $f_1(2) = a$. So, the function f_1 is not one-to-one since $f_1(1) = f_1(2) = a$. Similarly, f_3 is not one-to-one since $f_3(1) = f_3(2) = b$. f_2 defined as $f_2(1) = a$ and $f_2(2) = b$ and f_3 defined as $f_3(1) = b$ and $f_3(2) = a$ are one-to-one functions.

The function f_2 and f_3 are onto because its images is $\{a, b\} = B$.

Hence f_2 and f_3 are both one-to-one and onto but f_1 and f_4 are neither one-to-one nor onto.

Example 15. Let f and g be functions from the positive integers to the positive integers defined by $f(n) = n^2$, $g(n) = 2^n$.

Find fof, gog, fog, gof

Solution.

(*i*) $(fof)(n) = f[f(n)] = f(n^2) = (n^2)^2 = n^4$

(*ii*) $(gof)(n) = g[g(n)] = g(2^n) = (2)^{2^n} = 4^n$

(*iii*) $(fog)(n) = f[g(n)] = f(2^n) = (2^n)^2$

(*iv*) $(gof)(n) = g[f(n)] = g(n^2) = 2^{n^2}$

Example 16. Let $A = B = C = R$. Consider the function $f : A \to B$ and $g : B \to C$ defined by

$$f(a) = 2a + 1, \; g(b) = \frac{b}{3}$$

Verify $(gof)^{-1} = f^{-1}og^{-1}$

Solution. The function f: R $\to$ R defined by $f(a) = 2a + 1$ is bijective. Hence f^{-1} exists.

Let $b = f(a) = 2a + 1 \quad \therefore \quad a = \dfrac{b-1}{2}$

Also $f(a) = b \Rightarrow a = f^{-1}(b) \quad \therefore \quad \dfrac{b-1}{2} = f^{-1}(b)$ ...(1)

Also, the function g : R $\to$ R defined by g(b) $= \dfrac{b}{3}$ is bijective. Hence g^{-1} exists.

Let $c = g(b) = \dfrac{b}{3} \quad \therefore \quad b = 3c$

Also $g(b) = c \Rightarrow b = g^{-1}(c) \quad \therefore \quad 3c = g^{-1}(c)$ ...(2)

Now, $gof : A \to C$ is defined by $(gof)(a) = c$

$\therefore \quad g(f(a)) = c \Rightarrow g(2a + 1) = c$

$\therefore \quad \dfrac{2a+1}{3} = c \Rightarrow a = \dfrac{3c-1}{2}$

Also $(gof)(a) = c \Rightarrow a = (gof)^{-1}c$

i.e. $\dfrac{3c-1}{2} = (gof)^{-1}c$

Again $(f^{-1}og^{-1})(c) = f^{-1}(g^{-1}(c)) = f^{-1}(3c)$ using (2)

$= \dfrac{3c-1}{2}$ using (1)

$\therefore \quad (gof)^{-1}c = (f^{-1}og^{-1})c = \dfrac{3c-1}{2}$

Hence $(gof)^{-1} = f^{-1}og^{-1}$ is verified.

Example 17. If the function $f: R \to R$ defined by $f(x) = x^2$, find $f^{-1}(4)$ and $f^{-1}(-4)$.

Solution. $f^{-1}(4) = \{x \in R : f(x) = 4\}$
$= \{x \in R : x^2 = 4\}$
$= \{x \in R : x = \pm 2\} = \{-2, 2\}$
$f^{-1}(-4) = \{x \in R : f(x) = -4\}$
$= \{x \in R : x^2 = -4\}$
$= \{x \in R : x = \pm 2\sqrt{-1}\} = \varphi$ since $\pm 2\sqrt{-1}$ are imaginary numbers.

Example 18. If the function $f: R \to R$ defined by

$$f(x) = \begin{cases} 3x-4 & x > 0 \\ -3x+2 & x \le 0 \end{cases}$$

Determine

(a) $f(0), f(2/3), f(-2)$ (b) $f^{-1}(0), f^{-1}(2), f^{-1}(-7)$

Solution. (a) $f(0) = -3(0) + 2 = 2$

$f(2/3) = 3(2/3) - 4 = -2$

$f(-2) = -3(-2) + 2 = 8$

(b) $f^{-1}(0) = \{x \in R \mid f(x) = 0\}$
$= \{x \in R \mid x > 0 \text{ and } 3x - 4\} \cup \{x \in R \mid x \le 0 \text{ and } -3x + 2 = 0\}$
$= \{x \in R \mid x > 0 \text{ and } x = 4/3\} \cup \{x \in R \mid x \le 0 \text{ and } x = 2/3\}$
$= \{4/3\} \cup \varphi = \{4/3\}$

$f^{-1}(2) = \{x \in R \mid f(x) = 2\}$
$= \{x \in R \mid x > 0 \text{ and } 3x - 4 = 2\} \cup \{x \in R \mid x \le 0 \text{ and } -3x + 2 = 2\}$
$= \{x \in R \mid x > 0 \text{ and } x = 2\} \cup \{x \in R \mid x \le 0 \text{ and } x = 0\}$
$= \{2\} \cup \{0\} = \{0, 2\}$

$f^{-1}(-7) = \{x \in R \mid x > 0$ a: $3x + 4 = -7\} \cup \{x \in R \mid x \le 0 \text{ and } 3x - 2 = 2\}$
$= \{x \in R \mid x > 0 \text{ and } x = -1\} \cup \{x \in R \mid x \le 0 \text{ and } x = 3\}$
$= \varphi \cup \varphi = \varphi$

Example 19. Let the function $f: R \to R$ be defined by

$$f(x) = \begin{cases} 3x-1 & \text{for } x > 3 \\ 2x^2+3 & \text{for } -2 < x \le 3 \\ 3x^2-7 & \text{for } x \le -2 \end{cases}$$

Find out $f^{-1}(5)$.

Solution. $f^{-1}(5) = \{x \in R \mid f(x) = 5\}$
$= \{x \in R \mid x > 3 \text{ and } 3x - 1 = 5\} \cup \{x \in R \mid -2 < x \le 3 \text{ and } 2x^2 + 3 = 5\} \cup$
$\{x \in R \mid x \le -2 \text{ and } 3x^2 - 7 = 5\}$
$= \{x \in R \mid x > 3 \text{ and } x = 2\} \cup \{x \in R \mid -2 < x \le 3 \text{ and } x = \pm 1\} \cup \{x \in R \mid x \le -2 \text{ and } x = \pm 2\}$
$= \varphi \cup \{-1, 1\} \cup \{-2\} = \{-2, -1, 1\}$

Example 20. (a) Let $f: X \to Y$ be an everywhere defined invertible function and A and B be arbitrary non-empty subsets of Y. Show that

(i) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$ (ii) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.

Solution (i) Let $x \in X$, then

$x \in f^{-1}(A \cup B) \Leftrightarrow f^{-1}(x) \in \{A \cup B\}$

$\Leftrightarrow f(x) \in A$ or $f(x) \in B$
$\Leftrightarrow x \in f^{-1}(A)$ or $x \in f^{-1}(B)$
$\Leftrightarrow x \in \{f^{-1}(A) \cup f^{-1}(B)\}$

Therefore, $f^{-1}(A \cup B) = \{f^{-1}(A) \cup f^{-1}(B)\}$

(*ii*) $x \in f^{-1}(A \cap B) \Leftrightarrow f(x) \in \{A \cap B\}$
$\Leftrightarrow f(x) \in A$ and $f(x) \in B$
$\Leftrightarrow x \in f^{-1}(A)$ and $x \in f^{-1}(B)$
$\Leftrightarrow x \in \{f^{-1}(A) \cap f^{-1}(B)\}$

Therefore, $f^{-1}(A \cap B) = \{f^{-1}(A) \cap f^{-1}(B)\}$.

(*b*) Let $f: R \to R$ be a function defined by $f(x) = px + q \ \forall \ x \in R$. Also $fof = I_R$, find the values of p and q.

Solution. Given $(fof)x = I_R(x)$

i.e. $f(f(x)) = x$

or $f(px + q) = x \Rightarrow p(px + q) + q = x$

or $p^2x + pq + q - x = 0$

or $x(p^2 - 1) + q(p + 1) = 0 \ \forall \ x \in R$

or $p^2 - 1 = 0$ and $q(p + 1) = 0$

or $p = \pm 1$ and $q(p + 1) = 0$

when $p = 1$, $q = 0$ or $p = -1$, q is any real value

Hence, either $p = 1$ and $q = 0$ or $p = -1$ and q is any real value.

CHAPTER 7

Relation

7.1. Introduction

The word relation is used to indicate a relationship between two objects. There are many kinds of relationship in the world. We deal with relationship between student and teachers, an employee and his salary, and so on. In mathematics, an example of relation is "less than" which is denoted by $<$, so that x is related to y if $x < y$, two computer programs are related if they share some common data. A relation is often described verbally and may be denoted by a name or symbol but most of these relations have no simple verbal descriptions and no familiar name of symbol to specify their nature or properties. It is defined in terms of the ordered pairs. We note that a relation between two objects can be defined by listing the two objects as an ordered pair. This method of specifying a relation does not require any special symbol or description and so is suitable for any relation between any two sets. In this chapter, we discuss the mathematics of relations defined on sets, various ways of representing relations and explore various properties they may have.

7.2. Relations on Sets

The most direct way to express a relationship between elements of two sets is to use ordered pairs made up of two related elements. Let A and B be two sets as follows:

A = {Calcutta, Patna, Lucknow, Chennai} and B = {West Bengal, Bihar, Uttar Pradesh, Tamilnadu}. There is a relation 'is a capital of' between the elements of the sets A and B. If R is used for the relation 'is a capital of', then the above information can be written as Calcutta R West Bengal, Patna R Bihar, Lucknow R Uttar Pradesh, Chennai R Tamilnadu. Omitting the letter R between the pair of names and writing the pair of names as an ordered pair, the above information can be written as a set of ordered pairs R where

$$R = \{(\text{Calcutta, West Bengal}), (\text{Patna, Bihar}), (\text{Lucknow, Uttar Pradesh}), (\text{Chennai, Tamilnadu})\}$$
$$= \{(x, y): x \in A, y \in B, x \, R \, y\}$$

Thus, the relation 'is a capital of' from a set A to B gives rise to a subset R of $A \times B$ such that $(x, y) \in R$ if and only if $x \, R \, y$.

Definition. Let A and B be two sets. A relation from A to B is a subset of the cartesian product $A \times B$. Suppose R is a relation from A to B. Then R is a set of ordered pairs (a, b) where $a \in A$ and $b \in B$. Every such ordered pair is written as $a \, R \, b$ and read as 'a is related to b by R'. If $(a, b) \notin R$, then a is not related to b by R and is written as $a \not R \, b$. R is called a **binary relation** from A to B since the elements of the set R are ordered pairs. If we use the term relation on its own, then binary relation is implied.

Recall that the Cartesian product $A \times B$ consists of all ordered pairs whose first element is in A and whose second element is in B:

$$A \times B = \{(x, y) : x \in A \text{ and } y \in B\}$$

If A = {1, 2, 5} and B = {2, 4} then

$A \times B = \{(1, 2), (1, 4), (2, 2), (2, 4), (5, 2), (5, 4)\}$

If we take the relationship $x < y$, then some ordered pairs are related and some are not. The subset of A × B whose elements are related is the relation R and is given by

$$R = \{(1, 2), (1, 4), (2, 4)\}$$

If R is a relation from a set A to itself, that is, if R is a subset of $A^2 = A \times A$, then we say R is a relation on A.

Domain and Range

The set $\{a \in A : (a, b) \in R \text{ for some } b \in B\}$ is called the domain of R and denoted by Dom (R).

The set $\{b \in B : (a, b) \in R \text{ for some } a \in A\}$ is called the range of R and denoted by Ran (R).

Thus, the domain of a relation R is the set of all the first element of the ordered pairs which belong to R and the range of R is the set of second elements.

Example 1. Let A = {2, 3, 5}, B = {2, 4, 6, 10}. A relation R from A to B is given as follows:

2R2, 2R4, 2R6, 2R10, 3R6, 5R10

Write R as a set of ordered pairs.

Solution. R = {(2, 2), (2, 4), (2, 6), (2, 10), (3, 6), (5, 10)}

Example 2. Let A = {2, 3, 4} and B = {3, 4, 5}. List the elements of each relation R defined below and the domain and range.

(*a*) $a \in A$ is related to $b \in B$, that is, a R b if, and only if $a < b$.

(*b*) $a \in A$ is related to $b \in B$, that is, a R b if a and b are both odd numbers.

Solution. (*a*) $2 \in A$ is less than $3 \in B$, then 2R3. Similarly, 2R4, 2R5, 3R4, 3R5, 4R5. Therefore,

$$R = \{(2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5)\}$$

$$\text{Dom (R)} = \{2, 3, 4\} \text{ and Ran (R)} = \{3, 4, 5\}$$

(*c*) Since $3 \in A$ and $3 \in B$ are both odd then 3R3. Similarly, 3R5. Therefore,

$$R = \{(3, 3), (3, 5)\}$$

$$\text{Dom (R)} = \{3\} \text{ and Ran (R)} = \{3, 5\}$$

Example 3. Let S = {*x*, *y*} and S^2 is the set of all words of length 2,

(*i*) Find the elements of S^2.

(*ii*) The relation R on S^2 is defined by v R w means that the first letter in v is the same as the first letter in w when v and w are in S^2. Write R as a set of ordered pairs.

Solution.

$$S^2 = \{xx, xy, yx, yy\}$$

$$R = \{(xx, xy), (xy, xx), (yx, yy), (yy, yx)\}$$

Total number of distinct relation from a set A to a set B

Let the number of elements of A and B be m and n respectively. Then the number of elements of A × B is mn. Therefore, the number of elements of the power set of A × B is 2^{mn}. Thus, A × B has 2^{mn} different subsets. Now, every subset of A × B is a relation from A to B. Hence, the number of different relations from A to B is 2^{mn}.

7.3 Some Operations on Sets

Since binary relations are sets of ordered pairs, all set operations can be done on relations. The resulting sets contain ordered pairs and are, therefore, relations. If R and S denote two relations, then R ∩ S, known as intersection of R and S, defines a relation such that

$$x \, (R \cap S) \, y = x \, R \, y \wedge x \, S \, y$$

Similarly, $R \cup S$, known as union of R and S, such that

$$x\,(R \cap S)\,y = x\,R\,y \vee x\,S\,y$$

Also, $x\,(R - S)\,y = x\,R\,y \wedge x\,\$\,y$ where $R - S$ is known as difference of R and S.

and $x\,(R')\,y = x\,R\,y$ where R' is the complement of R.

Example 4. If $A = \{x, y, z\}$, $B = \{X, Y, Z\}$, $C = \{x, y\}$ and $D = \{Y, Z\}$. R is a relation from A to B defined by $R = \{(x, X), (x, Y), (y, Z)\}$ and S is a relation from C to D defined by $S = \{(x, Y), (y, Z)\}$. Find R', $R \cup S$, $R \cap S$ and $R - S$.

Solution. The complement of R consists of all pairs of the cartesian product $A \times B$ that are not R. Thus, $A \times B = \{(x, X), (x, Y), (x, Z), (y, X), (y, Y), (y, Z), (z, X), (z, Y), (z, Z)\}$

Hence
$$R' = \{(x, Z), (y, X), (y, Y), (z, X), (z, Y), (z, Z)\}$$
$$R \cup S = \{(x, X), (x, Y), (y, Z)\}$$
$$R \cap S = \{(x, Y), (y, Z)\}$$
$$R - S = \{(x, X)\}$$

7.4. Types of Relations in a Set

We consider some special types of relations in a set..

Inverse Relation

Let R be any relation from a set A to a set B. The inverse of R, denoted by R^{-1} is the relation from B to A which consists of those ordered pairs which, when reversed, belong to R; that is, $R^{-1} = \{(b, a) : (a, b) \in R\}$. Consequently, $x\,R\,y = y\,R^{-1}\,x$

For example, Let A be the set of all living people. Define relations B and C on A as follows:

$$B = \{(x, y) : x \text{ is a parent of } y\}$$
$$C = \{(y, x) . y \text{ is a child of } x\}$$

Then each of B and C is the inverse of other, written as $B = C^{-1}$ and $C = B^{-1}$.

Similarly, on the set of real numbers, the relation $<$ is the inverse of the relation $>$.

Note the difference between R' and R^{-1}. The relation R' contains all elements not in R, R^{-1} contains all elements of R, except that their order is reversed. For instance, if R is the relation $<$, then R^{-1} is the relation $>$, because $a < b$ if and only if $b > a$. On the other hand, R' is the relation $\geq$ because if $x < y$ is false then $x \geq y$.

Example 5. Let $A = \{2, 3, 5\}$ and $B = \{6, 8, 10\}$ and define a binary relation R from A to B as follows:

For all $(x, y) \in A \times B$, $(x, y) \in R \Leftrightarrow x / y$ (x divides y).

Write each R and R^{-1} as a set of ordered pairs.

Solution. Here $2 \in A$ divides $6 \in B$, then 2 R 6. Similarly, 2 R 8, 2 R 10, 3 R 6, 5 R 10. Therefore,

$$R = \{(2, 8), (2, 10), (3, 6), (5, 10)\}$$

and
$$R^{-1} = \{(8, 2), (10, 2), (6, 3), (10, 5)\}$$

Note that
$$\text{Dom } (R) = \text{Ran } R^{-1} = \{2, 3, 5\}$$
$$\text{Ran } (R) = \text{Dom } R^{-1} = \{8, 10, 6\}$$

Clearly, if R is any relation, then $(R^{-1})^{-1} = R$. Moreover, if R is a relation on A, then R^{-1} is also a relation on A.

Identity Relation

A relation R in a set A is said to be identity relation, generally denoted by I_A, if

$$I_A = \{(x, x) : x \in A\}$$

Example 6. Let A = {1, 2, 3} then I_A = {(1, 1), (2, 2), (3, 3)} is an identity relation in A.

***n*-ary Relation**

Let $\{A_1, A_2, A_3, ..., A_n\}$ be a finite collection of sets. A subset R of $A_1 \times A_2 \times ... \times A_n$ is called an n-ary relation on $A_1, A_2, ..., A_n$.

(*i*) If $R = \phi$ then R is called void or empty relation.

(*ii*) If $R = A_1 \times A_2 \times ... \times A_n$, then R is called the universal relation.

(*iii*) If $A_i = A$ for i, then R is called an n-ary relation on A.

(*iv*) For n = 1, 2, or 3, R is called a unary, binary or ternary relation respectively.

For example,

(*a*) Let A = { 2, 5, 7} and R be a relation defined as a $R\ b (a \neq b)$ if and only if a divides b then we observe that $R = \phi$. $A \times A$ is a void relation.

(*b*) Let Z be the set of all integers, then, the property 'x is an even integer' can be characterised as a relation which is unary. Thus, the relation $R = \{x \in Z; x \text{ is an even}\}$ is unary.

(*c*) Let A = {1, 2, 5, 8} and let R be the relation defined by the property 'x' is less than y, then, R = {(1, 2), (1, 5), (1, 8), (2, 5), (2, 8), (5, 8)} is binary.

(*d*) Let A = {1, 3, 5} and let R be the relation defined by the property '$x + y$ is less than z', then R = {1, 1, 3} is ternary.

(*e*) Let A = {5, 6}, then $R = A \times A$ = {(5, 5), (5, 6), (6, 5), (6, 6)} is a universal relation.

7.5 Properties of Relations

A relation R on a set A satisfies certain properties. These properties are defined as follows:

Reflexive Relation: A relation R on a set A is reflexive if a R a for every $a \in A$, that is, if $(a, a) \in R$ for every $a \in A$. This simply means that each element a of A is related to itself.

For example,

(*a*) If R_1 = {(1, 1), (1, 2), (2, 2), (2, 3), (3, 3)} be a relation on A = {1, 2, 3}, then R_1 is reflexive relation since for every $a \in A$, (a, a) $\in R_1$.

(*b*) If R_2 = {(1, 1), (1, 2), (2, 3), (3, 3)} be a relation on A = {1, 2, 3}, then R_2 is not a reflexive relation since for $2 \in A$, $(2, 2) \notin R_2$.

(*c*) $R_3 = \{(x, y) \in R^2 : x \leq y\}$ is a reflexive relation since $x \leq x$ for any $x \in R$ (a set of real numbers).

Irreflexive Relation: A relation R on a set A is irreflexive if, for every $a \in A$, $(a, a) \notin R$. In other words, there is no $a \in A$ such that $a\ R\ a$. The terms reflexive and irreflexive are extreme cases. Reflexive means that $a\ R\ a$ is true for all a, and irreflexive means that $a\ R\ a$ is true for no a. For example,

(*a*) The relation R_1 = {(1, 2), (1, 3), (2, 1), (2, 3)} on A = {1, 2, 3} is irreflexive relation since $(x, x) \notin R_1$ for every $x \in R_1$ (a set of real numbers).

(*b*) The relation $R_2 = \{(x, y) \in R^2 : x < y\}$ is an irreflexive relation since $x < x$ for no $x \in R$ (the set of real numbers).

Non-reflexive Relation: A relation R on a set A is non-reflexive if R is neither reflexive nor irreflexive *i.e.*, if $a\ R\ a$ is true for some a and false for others. For example,

R = {(1, 2), (2, 3), (2, 2), (3, 1)} on A = {1, 2, 3} is a non-reflexive relation since $2R2$ is true but $1R1$ and $3R3$ are false.

Symmetric Relation: A relation R on a set A is symmetric if whenever $(a, b) \in R$ then $(b, a) \in R$, *i.e.* if $aRb \Rightarrow bRa$. This means if any one element is related to any other element, then the second element is related to the first. For example,

(*a*) $R_1 = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 1), (3, 1)\}$ on $A = \{1, 2, 3\}$ is a symmetric relation.

(*b*) $R_2 = \{(x, y) \in R^2 : x^2 + y^2 = 1\}$ is a symmetric relation on R since if $x^2 + y^2 = 1$ then $y^2 + x^2 = 1$ too, *i.e.* if $(x, y) \in R_2$ then $(y, x) \in R_2$.

Asymmetric Relation : A relation R on a set A is asymmetric if whenever $(a, b) \in R$ then $(b, a) \notin R$ for $a \neq b$ *i.e.*, if $aRb \Rightarrow b \not R a$ This means that the presence of (a, b) in R excludes the possibility of presence of (b, a) in R. For example,

The relation $R_1 = \{(1, 1), (1, 2), (2, 3), (3, 1)\}$ on $A = \{1, 2, 3\}$ is an asymmetric relation.

Antisymmetric Relation: A relation R on a set A is antisymmetric if for all $a, b \in A$ (aRb and bRa) $\Rightarrow a = b$. For example,

(*a*) $R_1 = \{(1, 2), (2, 2), (2, 3)\}$ on $A = \{1, 2, 3\}$ is an antisymmetric relation.

(*b*) $R_2 = \{(x, y) \in R^2 \mid x \leq y\}$ is an antisymmetric relation on R since $x \leq y$ and $y \leq x$ implies $x = y$, then $(x, y) \in R$ and $(y, x) \in R$ implies $x = y$.

(*c*) $R = \{(x, y) \in N \mid x$ is a divisor of $y\}$ is an antisymmetric relation since x divides y and y divides x implies $x = y$.

Note that antisymmetric is not the same as not symmetric. A relation may be symmetric as well as antisymmetric at the same time. For example, the relation $R = \{(1, 1), (3, 3)\}$ is both symmetric and antisymmetric on $A = \{1, 2, 3\}$.

Transitive Relation: A relation R on a set A is transitive if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$, *i.e.* aRb and $bRc \Rightarrow aRc$. This means if one element is related to second and second element is related to a third, then the first is related to the third. For example,

(*a*) The relation 'is parallel to' on the set of lines in a plane is transitive, because if a line x is parallel to the line y and if y is parallel to line z, then x is parallel to z.

(*b*) The relations 'is less than' and 'is greater than' are transitive relations on the set of real numbers. If $a<b$ and $b<c$ implies $a<c$ and if $a>b$ and $b>c$ implies $a>c$ for all real numbers a, b, c.

The following Table summarizes the above properties.

Property	*Meaning*
1. Reflexivity	$(a, a) \in R$, *i.e.* aRa for all $a \in A$
2. Irreflexivity	$(a, a) \notin R$, *i.e.* $a \not R a$ for all $a \in A$
3. Symmetry	$(a, b) \in R \Rightarrow (b, a) \in R$, *i.e.* $aRb \Rightarrow bRa$ for all $a, b \in A$
4. Asymmetry	$(a, b) \in R \Rightarrow (b, a) \notin R$, *i.e.* $aRb \Rightarrow b \not R a$ for all $a, b \in A$
5. Antisymmetry	$(a, b) \in R \wedge (b, a) \in R \Rightarrow a = b$, *i.e.* aRb and $bRa \Rightarrow a = b$ for all $a, b \in A$
6. Transitivity	$(a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$, *i.e.* aRb and $bRc \Rightarrow aRc$. for all $a, b, c \in A$

Example 8. *Give an example of a relation which is:*

(i) reflexive and transitive but not symmetric;

(ii) symmetric and transitive but not reflexive;

(iii) reflexive and symmetric but not transitive;

(iv) Reflexive and transitive but neither symmetric nor antisymmetric.

Solution. Let $A = \{1, 2, 3\}$. Then, it is easy to verify that the relation

(i) $R_1 = \{(1, 1), (2, 2), (3, 3), (1, 3)\}$

is reflexive and transitive but not symmetric, since $(1, 3) \in R_1$ but $(3, 1) \notin R_1$.

(ii) $R_2 = \{(1, 1), (3, 3), (1, 3), (3, 1)\}$

is symmetric and transitive, but not reflexive, since $(3, 3) \notin R_2$.

(*iii*) $R_3 = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3), (3, 2)\}$ is reflexive and symmetric but not transitive, since $(1, 2) \in R_3$ and $(2, 3) \in R_3$ but $(1, 3) \notin R_3$.

(*iv*) Let Z^* be the set of all non-zero integers and R be the relation on Z^* given by $(a, b) \in R$ if a is *a* factor *b*, *i.e.*, if a/b. Since a/a for all $a \in Z^*$; a/b and $b/c \Rightarrow a/c$, hence R is reflexive and transitive. 2/6 but 6/2 is not true; hence R is not symmetric. Again 5/- 5 and – 5/5 but $5 \neq -5$; hence R is not antisymmetric.

Example 9. Prove that if a relation R on set A is transitive and irreflexive, then it is asymmetric.

Solution. We assume that R is not asymmetric then $(b, a) \in R$ whenever $(a, b) \in R$. Since R is transitive, $(a, b) \in R$ and $(b, a) \in R$ implies $(a, a) \in R$. This contradicts the hypothesis that R is irreflexive. Therefore, R is asymmetric when it is transitive and irreflexive.

Example 10. How many reflexive and symmetric relations are there on a set with n elements?

Solution. A relation R on a set A is a subset of A × A. Thus a relation is determined by specifying whether each of the n^2 ordered pairs in A × A is in R. If R is reflexive, each of the n ordered pairs (a, a) for $a \in$ A must be in R. Each of the other $n^2 - n = n(n-1)$ ordered pairs of the form may or may not be in R. By product rule of counting, there are $2^{n(n-1)}$ reflexive relations.

If R is symmetric, each of the n ordered pairs (a, a) for $a \in$ A must be in R and set of pairs of elements of the form (a, b) and (b, a) for $a, b \in$ A must also be in R. There are $n(n-1)/2$ such pairs. By product rule of counting, there are $2^n \cdot 2^{n(n-1)/2} = 2^{n(n+1)/2}$ symmetric relations.

The no. of both reflexive and symmetric relation is $2^{\frac{1}{2}(n^2-n)}$

Equivalence Relation

A relation on a set A is called an equivalence relation or RST relation if it is reflexive, symmetric and transitive. That is, R is an equivalence relation on A if it has the following three properties:

1. $(a, a) \in$ R for all $a \in$ A (reflexive)
2. $(a, b) \in$ R implies $(b, a) \in$ R (symmetric)
3. (a, b) and $(b, c) \in$ R imply $(a, c) \in$ R (transitive)

Example 11. Let R is the relation on the set of strings of Hindi letters such that aRb if and only if $l(a) = l(b)$, where $l(x)$ is the length of the string x. Show that R is an equivalence relation.

Solution. Since $l(a) = l(a)$, it follows that aRa whenever a is a string, so that R is reflexive.

Suppose aRb, so that $l(a) = l(b)$. Then bRa, since $l(b) = l(a)$. Hence, R is symmetric.

Again suppose that aRb and bRc, *i.e.*, $l(a) = b(b)$ and $l(b) = l(c)$. Hence, $l(a) = l(c)$ which implies aRc. Consequently, R is transitive.

Since R is reflexive, symmetric and transitive, it is an equivalence relation.

Example 12. If R be a relation in the set of integers Z defined by

$$R = \{(x, y) : x \in Z, y \in Z, (x - y) \text{ is divisible by } 6\}$$

Then prove that R is an equivalence relation.

Solution. Let $x \in$ Z. Then $x - x = 0$ and 0 is divisible by 6.

Therefore, xRx for all $x \in$ Z.

Hence, R is reflexive.

Again, $xRy \Rightarrow (x - y)$ is divisible by 6

$\Rightarrow -(x - y)$ is divisible by 6

$\Rightarrow (y - x)$ is divisible by 6

$\Rightarrow yRx$.

Hence, R is symmetric.

xRy and $xRz \Rightarrow (x - y)$ is divisible by 6 and $(y - z)$ is divisible by 6

formula for counting the no. of transitive relation in an n element set A.

$\Rightarrow$ $[(x-y)+(y-z)]$ is divisible by 6

$\Rightarrow$ $(x-z)$ is divisible by 6

$\Rightarrow$ $x\mathrm{R}z$.

Hence, R is transitive.

Thus R is an equivalence relation.

Example 13. (*a*) *Consider the following relation on {1, 2, 3, 4, 5, 6}*

$R = \{(i, j) : |i-j| = 2\}$

Is 'R' transitive? Is R reflexive? Is R symmetric ?

Solution. Let $A = \{1, 2, 3, 4, 5, 6\}$

Then $R = \{(i, j) : |i-j| = 2\}$ on A

$= \{(1, 3), (2, 4), (3, 1), (4, 2), (3, 5), (5, 3), (4, 6), (6, 4)\}$

R is not reflexive since $(i, i) \notin R \ \forall\ i \in A$. For example, $(1, 1) \notin R$.

R is symmetric since for all $(i, j) \in R$, (j, i) also $\in R$.

R is not transitive since for all (i, j) and (j, k) $\in$ R, (i, k) does not belong to R. For example, $(2, 4)$ and $(4, 2) \in R$ but $(2, 2) \notin R$.

Hence R is not transitive.

(*b*) Let R be a binary relation defined as

$R = \{(a, b) \in R^2 : (a-b) \leq 3\}$

determine whether R is reflexive, symmetric, antisymmetric and transitive.

Solution. Given, $R = \{(a, b) \in R^2 : (a-b) \leq 3\}$

R is reflexive since $a - a = 0 \leq 3$ for all $a \in R$.

R is not symmetric since $a - b \leq 3 \not\Rightarrow b - a \leq 3$ for all $a, b \in R$.

Here $a, b \in R \Rightarrow a - b \leq 3$

$\Rightarrow b - a \geq 3$.

$\therefore$ $a - b \leq 3$ and $b - a \geq 3$ is possible only if $a = b$

Hence R is antisymmetric.

R is not transitive since $a - b \leq 3$ and $b - c \leq 3$.

$\Rightarrow (a-b) + (b-c) \leq 6$

$\Rightarrow a - c \leq 6 \notin R$

Example 14. Let R be a binary relation on the set of all integers of 0's and 1's such that $R = \{(a, b)$: a and b are strings, that they have the same number of 0's$\}$. Is R reflexive? symmetric? antisymmetric ? transitive? an equivalence relation?

Solution. R is reflexive since $(a, a) \in R \ \forall\ a \notin R$.

R is symmetric since when a and b have the same number of 0's then b and a will also have the same number of 0's. Hence $(a, b) \in R \Rightarrow (b, a) \in R$.

R is transitive since when a and b have the same number of 0's and b and c have the same number of 0's, then a and c will also have the same number of 0's. Hence (a, b) and $(b, c) \in R \Rightarrow (a, c) \in R$.

Thus, R is reflexive, symmetric and transitive and hence an equivalence relation.

R is not antisymmetric since (a, b) and (b, a) belongs to R does not imply $a = b$.

Theorem 7.1. Let R and S be relation from A to B, show that

(*i*) If $\mathrm{R} \subseteq \mathrm{S}$, then $\mathrm{R}^{-1} \subseteq \mathrm{S}^{-1}$

(*ii*) $(\mathrm{R} \cap \mathrm{S})^{-1} = \mathrm{R}^{-1} \cap \mathrm{S}^{-1}$

(*iii*) $(\mathrm{R} \cup \mathrm{S})^{-1} = \mathrm{R}^{-1} \cup \mathrm{S}^{-1}$

Proof. (*i*) Suppose $\mathrm{R} \subseteq \mathrm{S}$. If $(a, b) \in \mathrm{R}^{-1}$, then $(b, a) \in \mathrm{R}$ and also $(b, a) \in \mathrm{S}$ since $\mathrm{R} \subseteq \mathrm{S}$. Again $(b, a) \in \mathrm{S}$ implies $(a, b) \in \mathrm{S}^{-1}$. Therefore, $\mathrm{R}^{-1} \subseteq \mathrm{S}^{-1}$.

(*ii*) Let $(a, b) \in (\mathrm{R} \cap \mathrm{S})^{-1}$. Then $(b, a) \in \mathrm{R} \cap \mathrm{S}$, so that $(b, a) \in \mathrm{R}$ and $(b, a) \in \mathrm{S}$. This implies $(a, b) \in \mathrm{R}^{-1}$ and $(a, b) \in \mathrm{S}^{-1}$. Hence, $(a, b) \in \mathrm{R}^{-1} \cap \mathrm{S}^{-1}$. Therefore,

$$(R \cap S)^{-1} \subseteq R^{-1} \cap S^{-1} \quad \ldots (1)$$

Conversely, let $(a, b) \in R^{-1} \cap S^{-1}$. Then $(a, b) \in R^{-1}$ and $(a, b) \in S^{-1}$. This implies $(b, a) \in R$ and $(b, a) \in S$. So, $(b, a) \in R \cap S$. Hence, $(a, b) \in (R \cap S)^{-1}$. Therefore,

$$R^{-1} \cap S^{-1} \subseteq (R \cap S)^{-1} \quad \ldots (2)$$

From (1) and (2), we have

$$(R \cap S)^{-1} = R^{-1} \cap S^{-1}.$$

(iii) Let $(a, b) \in (R \cup S)^{-1}$. Then $(b, a) \in (R \cup S)$ so that $(b, a) \in R$ or $(b, a) \in S$. This implies $(a, b) \in R^{-1}$ or $(a, b) \in S^{-1}$. Hence, $(a, b) \in R^{-1} \cup S^{-1}$. Therefore,

$$(R \cup S)^{-1} \subseteq R^{-1} \cup S^{-1} \quad \ldots (1)$$

Conversely, let (a, b) $\in R^{-1} \cup S^{-1}$. Then $(a, b) \in R^{-1}$ or $(a, b) \in S^{-1}$. This implies $(b, a) \in R$ or $(b, a) \in S$. So, $(b, a) \in R \cup S$. Hence, $(a, b) \in (R \cup S)^{-1}$. Therefore,

$$R^{-1} \cup S^{-1} \subseteq (R \cup S)^{-1} \quad \ldots (2)$$

From (1) and (2), we have

$$(R \cup S)^{-1} = R^{-1} \cup S^{-1}.$$

Theorem 7.2. Let R be a relation on A. Prove that

(i) If R is reflexive, so is R^{-1}.

(ii) R is symmetric if and only if $R = R^{-1}$.

(iii) R is antisymmetric if and only if $R \cap R^{-1} \subseteq I_A$.

Proof. *(i)* Suppose R is reflexive. Then $(a, a) \in R$ for all $a \in A$. So, $(a, a) \in R^{-1}$ for all $a \in A$. Therefore, R^{-1} is reflexive.

(ii) Suppose R is symmetric. Let $(a, b) \in R^{-1}$. Then $(b, a) \in R$ and hence $(a, b) \in R$ since R is symmetric. Therefore, $R^{-1} \subseteq R$. Similarly, it can be shown that $R \subseteq R^{-1}$. Hence, $R = R^{-1}$.

Conversely, suppose $R = R^{-1}$. Let $(a, b) \in R$. Then $(a, b) \in R^{-1}$ and so $(b, a) \in R$. Hence, R is symmetric. Thus, R is symmetric if and only if $R = R^{-1}$.

(iii) Suppose R is antisymmetric. Let $(a, b) \in R \cap R^{-1}$. Then $(a, b) \in R$ and $(a, b) \in R^{-1}$. Again $(a, b) \in R^{-1}$ implies $(b, a) \in R$. Thus $(a, b) \in R$ and also $(b, a) \in R$. Hence, $b = a$ because R is antisymmetric. This is true for all $(a, b) \in R \cap R^{-1}$. Hence, every element of $R \cap R^{-1}$ is of the form (a, a) where $a \in A$. Therefore, $R \cap R^{-1} \subseteq I_A$.

Conversely, suppose $R \cap R^{-1} \subseteq I_A$. Let $(a, b) \in A \times A$ such that $(a, b) \in R$ and $(b, a) \in R$, *i.e.*, $(a, b) \in R$ and $(a, b) \in R^{-1}$. Then $(a, b) \in R \cap R^{-1}$. Since $R \cap R^{-1} \subseteq I_A$, it follows that $b = a$. Hence, R is antisymmetric.

This proves the theorem.

Theorem 7.3. Suppose R and S are relations on a set A. Prove that

(i) If R and S are reflexive, then $R \cup S$ and $R \cap S$ are reflexive.

(ii) If R and S are symmetric, then $R \cup S$ and $R \cap S$ are symmetric.

(iii) If R and S are transitive, then $R \cap S$ is transitive.

Proof. *(i)* Suppose R and S are reflexive. Then $(a, a) \in R$ and $(a, a) \in S$ for all $a \in A$. Therefore, $(a, a) \in R \cup S$ and $(a, a) \in R \cap S$. Hence, $R \cup S$ and $R \cap S$ are reflexive.

(ii) Suppose R and S are symmetric. By theorem 7.2, we get $R = R^{-1}$ and $S = S^{-1}$. Using $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$, we can write $(R \cup S)^{-1} = R \cup S$ and using $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$, we can write $(R \cap S)^{-1} = R \cap S$. Hence, $R \cup S$ and $R \cap S$ are symmetric.

(iii) Suppose R and S are transitive. Let $(a, b) \in R \cap S$ and $(b, c) \in R \cap S$, then $(a, b) \in R$, $(a, b) \in S$, $(b, c) \in R$ and $(b, c) \in S$. Now $(a, b) \in R$ and $(b, c) \in R$ implies $(a, c) \in R$ and $(a, b) \in S$ and $(b, c) \in S$ implies $(a, c) \in S$. Therefore, $(a, c) \in R \cap S$. Hence, $(a, b) \in R \cap S$ and $(b, c) \in R \cap S$ implies $(a, c) \in R \cap S$. Therefore, $R \cap S$ is transitive.

Note: If R and S are transitive relations on A, then $R \cup S$ need not be a transitive relation on A. For example, if $R = \{(1, 1), (2, 2), (1, 2), (2, 1)\}$ and $S = \{(2, 2), (3, 3), (2, 3), (3, 2)\}$ on $A = \{1, 2, 3\}$, then R and S are transitive but $R \cup S$ is not transitive since $(1, 2) \in R \cup S$ and $(2, 3) \in R \cup S$ but $(1, 3) \notin R \cup S$. Hence, $R \cup S$ is not transitive.

Theorem 7.4. If R and S are equivalence relations on the set A, prove that

(*i*) R^{-1} is an equivalence relation

(*ii*) $R \cap S$ is an equivalence relation.

Proof. (*i*) Let R be an equivalence relation in a set A. Therefore, R is reflexive, symmetric and transitive.

Let $a, b, c \in A$ be arbitrary.

The relation R^{-1} is

(1) reflexive: $(a, a) \in R^{-1}$, since $(a, a) \in R$ for all $a \Rightarrow (a, a) \in R^{-1}$,

(2) symmetric: $(a, b) \in R^{-1}$,

since $(a, b) \in R^{-1} \Rightarrow (b, a) \in R$

$\Rightarrow (a, b) \in R$, as R is symmetric

$\Rightarrow (b, a) \in R^{-1}$

(3) transitive: $(a, b)\,(b, c) \in R^{-1} \Rightarrow (a, c) \in R^{-1}$,

since $(a, b), (b, c) \in R^{-1} \Rightarrow (b, a), (c, b) \in R$

$\Rightarrow (c, b), (b, a) \in R$

$\Rightarrow (c, a) \in R$, as R is transitive

$\Rightarrow (a, c) \in R^{-1}$.

Therefore, R^{-1} is reflexive, symmetric and transitive.

Hence, R^{-1} is an equivalence relation in A.

(*ii*) We have to verify that $R \cap S$ is reflexive, symmetric and transitive.

(1) For all $a \in A$, $(a, a) \in R$ and $(a, a) \in S$, since R and S equivalence relation. Hence, for all $a \in A$, $(a, a) \in R \cap S$.

Hence, $R \cap S$ is reflexive.

(2) $(a, b) \in R \cap S \Rightarrow (a, b) \in R$ and $(a, b) \in S$

$\Rightarrow (b, a) \in R$ and $(b, a) \in S$, since R and S are symmetric being equivalence relations

$\Rightarrow (b, a) \in R \cap S$.

Hence, $R \cap S$ is symmetric.

(3) $(a, b) \in R \cap S, (b, c) \in R \cap S \Rightarrow (a, b) \in R, (b, c) \in R$ and $(a, b) \in S, (b, c) \in S$

$\Rightarrow (a, c) \in R$ and $(a, c) \in S$, is transitive since R and S are transitive being equivalence relations.

Hence $R \cap S$.

Equivalence Classes

If R is an equivalence relation on a set S and $x\ R\ y$, then x and y are called **equivalent** with respect to R. The set of all elements of S that are equivalent to a given element x constitute the **equivalence class** of x, denoted by $[x]_R$. When only one relation is under consideration, the subscript R is deleted and the equivalence class is denoted by $[x]$.

Thus, $$[x] = \{y \in S : y\ R\ x\}$$

The collection of all equivalence classes of elements of S under an equivalence relation R is denoted by S/R, that is,

$$S/R = \{[x] : x \in S\}$$

It is called the **quotient set** of S by R.

For example, the equivalence relation

$R = \{(1, 2), (2, 1), (1, 1), (2, 2), (3, 3), (4, 4)\}$ on $S = \{1, 2, 3, 4\}$ has the following equivalence classes

$$[1] = [2] = \{1, 2\}, \quad [3] = \{3\}, \quad [4] = \{4\}$$

Important properties of equivalence classes

Let A be a non-empty set and R be an equivalence relation defined in A. Let a and $b \in A$ be arbitrary. Then

(*i*) $a \in [a]$; (*ii*) $b \in [a] \Rightarrow [b] = [a]$;

(*iii*) $[a] = [b] \Leftrightarrow (a, b) \in R$; (*iv*) either $[a] = [b]$ or $[a] \cap [b] = \phi$.

The last result shows that either the two equivalent classes are identical or disjoint.

(*i*) R being an equivalence relation, it is reflexive, that is, aRa and

$$[a] = [x : x \in A \text{ and } xRa]$$

From this, we have $aRa \Rightarrow a \in [a]$.

(*ii*) We have $b \in [a] \Rightarrow bRa$.

Suppose $x \in [b]$, then $x \in [b] \Rightarrow xRb$.

Again, R being transitive, xRb and $bRa \Rightarrow xRa \Rightarrow x \in [a]$.

Therefore, $x \in [b] \Rightarrow x \in [a]$, that is, $[b] \subseteq [a]$ ... (1)

Let $y \in [a]$ and be arbitrary.

Then $y \in [a] \Rightarrow yRa$.

But R is symmetric, therefore, $bRa \Rightarrow aRb$.

Hence, yRa and $aRb \Rightarrow yRb$, as R is transitive.

Hence, $y \in [b]$.

Therefore, $y \in [a] \Rightarrow y \in [b]$ ... (2)

Hence, $[a] \subseteq [b]$.

From (1) and (2), we have $[a] = [b]$, if $b \in [a]$.

(*iii*) We assume that $[a] = [b]$.

Since R is reflexive, we have aRa.

Again, $aRa \Rightarrow a \in [a] \Rightarrow a \in [b]$, since $[a] = [b]$

$\Rightarrow aRb$.

Hence, $[a] = [b] \Rightarrow aRb$, that is, $(a, b) \in R$.

Conversely: We assume aRb. Let $x \in [a]$, so that xRa.

But aRb, hence R being transitive,

xRa and $aRb \Rightarrow xRb$.

$\therefore$ $x \in [b]$ and so $x \in [a] \Rightarrow x \in [b]$ ... (1)

$\Rightarrow [a] \subseteq [b]$

Again, let $y \in [b]$ and be arbitrary.

Then, $y \in [b] \Rightarrow yRb$.

But R being symmetric, $aRb \Rightarrow bRa$.

Again, R being transitive, yRb and $bRa \Rightarrow yRa$.

Hence, $y \in [a]$.

Therefore, $y \in [b] \Rightarrow y \in [a]$, that is, $[b] \subseteq [a]$ ... (2)

From (1) and (2), we have $[a] = [b]$.

But $[a] = [b] \Rightarrow aRb$ and $aRb \Rightarrow [a] = [b]$.

$\therefore$ $[a] = [b] \Leftrightarrow aRb$.

(*iv*) Here we assume $[a] \cap [b] \neq \phi$.

This implies that $\exists\, x \in A$ such that $x \in [a] \cap [b]$.

But $x \in [a] \cap [b] \Rightarrow x \in [a]$ and $x \in [b]$

$\Rightarrow xRa$ and xRb

$\Rightarrow a\mathrm{R}x$ and $x\mathrm{R}b$, as R is symmetric

$\Rightarrow a\mathrm{R}b$, as R is transitive

$\Rightarrow [a] = [b]$ [by (*iii*)]

$\therefore$ $[a] \cap [b] \neq \phi \Rightarrow [a] = [b]$.

Partial Order Relation

A relation R on a set S is called a partial order if it is reflexive, antisymmetric, and transitive. That is

1. Reflexivity: aRa for all $a \in S$
2. Antisymmetric: aRb and $bRa \Rightarrow a = b$
3. Transitive: aRb and $bRc \Rightarrow aRc$

A set S together with a partial order R is called a partial order set or a poset and is denoted by (S, R).

For example, the greater or equal ($\geq$) relation is a partial ordering on Z, the set of integers.

Reflexive: Since $a \geq a$ for every integer a, $\geq$ is reflexive.

Antisymmetric: Since $a \geq b$ and $b \geq a$ imply $a = b$, $\geq$ is antisymmetric.

Transitive: Since $a \geq b$ and $b \geq c$ imply $a \geq c$, $\geq$ is transitive.

Hence, $\geq$ is a partial ordering on Z, and (Z, $\geq$) is a poset.

Example 19. Let / be the divides relation R on a set N of positive integers. That is, for all $a, b \in N$, $a / b \Leftrightarrow b = ka$ for some integer k. Prove that / is a partial relation on N.

Solution. Reflexive: We have, $a \in N$, a is a divisor of a, *i.e.*, aRa. Therefore, R is reflexive.

Antisymmetric: If a is a divisor of b then b cannot be a divisor of a unless $a = b$. Thus, aRb and bRa imply $a = b$. Therefore, R is antisymmetric.

Transitive: Finally, a is a divisor of b and b is a divisor of c implies a is a divisor of c. Therefore, R is transitive.

Since R is reflexive, antismmetric and transitive, therefore, R is a partial order relation.

Observe that on the set of all integers, the above relation is not a partial order set as a and $(-a)$ both divide each other without being equal.

7.7. Composition of Relations

Let A, B, C be sets. Let R be a relation from A to B and let S be a relation from B to C. That is R is subset of $A \times B$ and S is a subset of $B \times C$. The composite of R and S, denoted by RoS, is the relation consisting of ordered pairs (a, c) when $a \in A$ and $c \in C$, and for which there exists an element $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S$. Thus,

$$RoS = \{(a, c) \in A \times C : \text{for some } b \in B, (a, b) \in R \text{ and } (b, c) \in S\}$$

That is a (RoS) c if for some $b \in B$ we have a R b and b S c.

Note that RoS is empty if the intersection of the range of R and the domain of S is empty. RoS is non-empty, if there is at least one ordered pair $(a, b) \in R$ such that the second member $b \in B$ of the ordered pair is a first member in an ordered pair in S. For the relation R o S, the domain is a subset of A and the range is a subset of C.

Since the operations of composition is a binary operation on relations, and it produces a relation from two relations, the same operation can be applied again to produce another relation. If R be a relation from A to B, S is a relation from B to C, and P be a relation from C to D, one can find out Ro(SoP) and also (RoS)oP which are relations from A to D. The operation of composition on relation is associative, *i.e.*, Ro(SoP) = (RoS)oP. This fact can easily be deduced as follows.

Let $(a, b) \in R$, $(b, c) \in S$, and $(c, d) \in P$. Then $(b, d) \in (SoP)$ and $(a, d) \in Ro(SoP)$. Again, $(a, c) \in (RoS)$ and $(a, d) \in (RoS)oP$ which shows Ro(SoP) = (RoS)oP.

The composition of a relation with itself is denoted with a power of a relation R. Let R be a relation on the set A. Then RoR is the composition of R with itself and RoR is denoted by R^2. Similarly, $R^3 = R^2oR = RoRoR$ and so on. For any relation R and natural number i one defines R^i as

$$R^o = I, \quad \text{the identity relation}$$
$$R^i = RoR^{i-1}, \quad \text{for } i > 0$$

For example,

$$\text{Parent}^0 = I$$
$$\text{Parent}^1 = \text{Parent}$$
$$\text{Parent}^2 = \text{grandparent}$$
$$\text{Parent}^3 = \text{great} - \text{grandparent}$$

Example 26. Let A = {1, 2, 3}, B = {p, q, r}, C = {x, y, z} and let R = {(1, p), (1, r), (2, q), (3, q)} and S = {(p, y), (q, x), (r, z)}. Compute RoS.

Solution. RoS is constructed using all ordered pairs in R and ordered pairs in S, where the second element of the ordered pair in R agrees with the first element of the ordered pair in S. For example, the ordered pairs (1, p) in R and (p, y) in S produce the ordered pair (1, y) in RoS. All other pairs of RoS are now symmetrically enumerated as follows:

(1, z) in RoS through intermediary r

(2, x) in RoS through intermediary q

(3, x) in RoS through intermediary q

Computing all the ordered pairs in RoS, we get

$$RoS = \{(1, y), (1, z), (2, x), (3, x)\}$$

Example 27. Let R = {(1, 1), (2, 1), (3, 2)}, compute R^2

Solution. $R^2 = RoR = \{(1, 1), (2, 1), (3, 1)\}$

Theorem 7.6. If R_1 and R_2 are relations from A to B and R_3 and R_4 are relations from B to C, then

(*i*) If $R_1 \subseteq R_2$ and $R_3 \subseteq R_4$ then $R_1oR_3 \subseteq R_2oR_4$.

(*ii*) $(R_1 \cup R_2)oR_3 = R_1oR_3 \cup R_2oR_3$.

Proof. (*i*) Let (x, y) $\in R_1oR_3$. Then for some $y \in B$, we have $(x, y) \in R_1$ and $(y, z) \in R_3$. Since, $R_1 \subseteq R_2$ and $R_3 \subseteq R_4$, we also have $(x, y) \in R_2$ and $(y, z) \in R_4$. So, $(x, z) \in R_2oR_4$. This shows that $R_1oR_3 \subseteq R_2oR_4$.

(*ii*) Since $R_1 \subseteq R_1oR_2$, we have $R_1oR_3 \subseteq (R_1 \cup R_2)oR_3$ from (*i*)

Similarly, $R_2oR_3 \subseteq (R_1 \cup R_2)oR_3$ and so $R_1oR_3 \cup R_2oR_3 \in (R_1 \cup R_2)oR_3$.

Consider, $(x, z) \in (R_1 \cup R_2)oR_3$. For some $y \in B$, we have $(x, y) \in R_1 \cup R_2$ and $(y, z) \in R_3$.

Then either $(x, y) \in R_1$ so that $(x, z) \in R_1oR_3$ or else $(x, y) \in R_2oR_3$.

Either way, $(x, z) \in R_1oR_3 \cup R_2oR_3$.

Theorem 7.7. (associative law for relation)

If R is a relation from A to B, S is a relation from B and C and T is a relation from C to D then

$$(RoS)oT = Ro(SoT)$$

Proof. We show that an ordered pair (x, v) in A × D belongs to (RoS)oT if and only if there exist $y \in B$ and $z \in C$ so that

$$(x, y) \in R, (y, z) \in S \text{ and } (x, v) \in T \quad \ldots (1)$$

A similar argument shows that (x, v) belongs to Ro(SoT) if and only if (1) holds. Consider (x, v) in (RoS)oT. Since RoS is a relation from A to C, this means that there exists $z \in C$ such that $(x, z) \in R$ o S and $(z, v) \in T$. Since $(x, z) \in R$ o S there exists $y \in B$ such that $(x, y) \in R$ and $(y, z) \in S$. Thus (1) holds.

Now suppose that (1) holds for an element (x, v) in A × D. Then $(x, y) \in R$ and $(y, z) \in S$ so that $(x, z) \in RoS$. Since also $(z, v) \in T$, we conclude that $(x, v) \in (RoS)oT$.

Now $(y, v) \in SoT$ and $(x, v) \in Ro(SoT)$, which shows that

$$(RoS)oT = Ro(SoT)$$

Theorem 7.8. If R is a relation from A to B and S is a relation from B to C, show that

$$(RoS)^{-1} = S^{-1}oR^{-1}$$

Proof. Since R is a relation from A to B, R^{-1} is a relation from B to A. Similarly, S^{-1} is a relation from C to B. Also the relation $S^{-1}oR^{-1}$ is from C to B. If xRy and ySz, then x (RoS)o z and z $(RoS)^{-1}$ x. But $zS^{-1}y$ and $yR^{-1}x$ so that z $(R^{-1}oS^{-1})$ x. This is true for any $x \in A$ and $z \in C$; hence, the required result.

Theorem 7.9. If R is a relation on a set a, then R is transitive if and only if $R^2 \subseteq R$.

Proof. Let R is transitive and $(x, z) \in R^2$. By definition of R^2 there exists $y \in A$ such that $(x, y) \in R$ and $(y, z) \in R$. Since R is transitive (x, z) is also in R. That is every $(x, z) \in R^2$ is in R. Therefore,

$$R^2 \subseteq R$$

Conversely, suppose $R^2 \subseteq R$. Let (x, y) and $(y, z) \in R$. Then $(x, z) \in R^2$ and hence in R. This proves that R is transitive.

Matrix Representation of Composition

The matrix for the composite of relations can be found using the Boolean product of the matrices. Suppose, R is a relation from A to B and S be a relation from B to C. Suppose that A, B and C have elements m, n and p respectively. The matrices represented by R, S and SoR are denoted by $M_R = [r_{ij}]_{m \times n}$, $M_S = [s_{ij}]_{n \times p}$ and $M_{RoS} = [t_{ij}]_{m \times p}$ respectively. It follows that $t_{ij} = 1$ if and only if $r_{ik} = s_{kj} = 1$ for some k. From the definition of the Boolean product, this means that

$$M_{RoS} = M_R \cdot M_S$$

Theorem 7.10. Let A, B and C be finite sets. Let R be a relation from A to B and S be a relation from B to C. Show that

$$M_{RoS} = M_R \cdot M_S$$

where M_R and M_S represent relation matrices of R and S respectively.

Proof. Let $A = \{a_1, a_2, \ldots\ldots, a_m\}$, $B = \{b_1, b_2, \ldots\ldots, b_n\}$, $C = \{c_1, c_2, \ldots\ldots, c_p\}$. Suppose $M_R = [a_{ij}]$, $M_S = [b_{ij}]$ and $M_{RoS} = [d_{ij}]$. Then $d_{ij} = 1$ if and only if $(a_i, c_j) \in RoS$, which means that for some k, $(a_i, b_k) \in R$ and $(b_k, c_j) \in S$. In other words, $a_{ik} = 1$ and $b_{kj} = 1$ for some k between 1 and n. If $d_{ij} = 0$, then either $(a_i, a_k) \notin R$ or $(a_k, a_j) \notin S$. This condition is identical to the condition needed for $M_R \cdot M_S$ to have a 1 or 0 in position i, j and thus $M_{RoS} = M_R \cdot M_S$.

Note: Due to the above theorem we can conclude the following results:

(*i*) Since the Boolean matrix multiplication is not commutative in general so the composition on relations is not commutative in general.

That is, $$RoS \neq SoR$$

(*ii*) The Boolean matrix is associative so composition on relations is also associative, that is

$$Ro(SoT) = Ro(SoT)$$

(*iii*) The distribution law is valid for Boolean matrix multiplication so composition of relation also satisfies the distributive law, that is

$$(R \cup S)oT = RoT \cup SoT$$

Let M_R and M_S denote respectively the matrices of the relations R and S. Then

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad M_S = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

The matrix of composite relations can be found by using the Boolean product of the matrices

$$M_{RoS} = M_R \cdot M_S = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

The non-zero entries in the matrix tells us which elements are related to RoS.