

## Sets Theory

Set: A set is a well-defined collection of objects. The objects are called the elements or members of the set. These elements may be anything: numbers, people, letter of the alphabet etc.

e.g. The vowels of alphabets.

Representation of a set:

(i) Roster or Tabular form  $\rightarrow A = \{a, e, i, o, u\}$

(ii) Rule method form or set builder form  $\rightarrow$

e.g. The set of aei, i, o, u can be written as  
 $A = \{n : n \text{ is a vowel of English alphabet}\}$

Null set: A set which contains no elements. Also called as empty set or void set.

$A = \{n : n^2 + 4 \neq 0, n \text{ is a real no.}\}$

It is denoted by symbol  $\emptyset$ .

Subset:  $A \subseteq B$  then if  $n \in A$  then  $n \in B$ .  
If A and B are sets such that every element of A is also an element of B, then A is said to be subset of B and is denoted by  $A \subseteq B$ . In other words,

$A \subseteq B$  if  $n \in A$  and  $n \in B$ .

Equal set: Two sets A and B are said to be equal if every element of A is an element of B and consequently every element of B is an element of A. i.e.  $A \subseteq B$  and  $B \subseteq A$  if it is written as  $A = B$ .

Union: The union of two sets A and B denoted by  $A \cup B$ .

$$A \cup B = \{x : x \in A \text{ or } x \in B\}$$

Intersection: The intersection of two sets A and B is denoted by  $A \cap B$ .

$$A \cap B = \{x : x \in A \text{ and } x \in B\}$$

Complements:  $A^c = A' = U - A$

$$A' = \{x : x \in U \text{ and } x \notin A\}$$

Algebra of Sets:

(a) Idempotent laws. (i)  $A \cup A = A$

(ii)  $A \cap A = A$

Proof  $\Rightarrow$  Let  $x \in A \cup A$ . Then

$$x \in A \cup A \Rightarrow x \in A \text{ or } x \in A$$

$$x \in A \cup A \Rightarrow x \in A \quad A \cup A \subseteq A \quad \text{--- (1)}$$

conversely, let  $x \in A$ . Then

$$x \in A \Rightarrow x \in A \text{ or } x \in A$$

$$\Rightarrow x \in A \cup A$$

$$\text{Thus } A \subseteq A \cup A \quad \text{--- (2)}$$

from eqn (1) + (2) we have —

$$\boxed{A \cup A = A}$$

Demorgan's law:

(a)  $(A \cup B)' = A' \cap B'$

(b)  $(A \cap B)' = A' \cup B'$

Proof:  $\neg \in (A \cup B) \Leftrightarrow \neg \in A$  and  $\neg \in B$ .

$\neg \in (A \cap B)$ ,  $\neg \in A$  or  $\neg \in B$ .

Let  $\neg \in (A \cup B)$ . Then

$\neg \in (A \cup B) \Rightarrow \neg \notin (A \cup B)$  or both are true.

$\Rightarrow \neg \notin A$  and  $\neg \notin B$ .

$\Rightarrow \neg \in A'$  and  $\neg \in B'$ .

$\neg \in (A \cup B) \Rightarrow \neg \in (A' \cap B')$

$\Rightarrow (A \cup B)' \subseteq A' \cap B'$  — (i)

conversely let  $\neg \in A' \cap B'$

$\neg \in A' \cap B' \Rightarrow \neg \in A'$  and  $\neg \in B'$

$\Rightarrow \neg \notin A$  and  $\neg \notin B$ .

$\Rightarrow \neg \notin (A \cup B)$

$\neg \in A' \cap B' \Rightarrow \neg \in (A \cup B)$  — (ii)

$A' \cap B' \subseteq (A \cup B)'$  — (iii)

Thus,  $A' \cap B' = (A \cup B)'$  Proved.

from (i) + (ii) we obtain

(ii) prove that  $A - (B \cap C) = (A - B) \cup (A - C)$ .

Proof: let  $\neg \in A - (B \cap C)$  Then

$\neg \in A - (B \cap C) \Rightarrow \neg \in A$  and  $\neg \notin (B \cap C)$

$\neg \in A - (B \cap C) \Rightarrow \neg \in A$  and  $(\neg \in B \text{ or } \neg \in C)$

$\Rightarrow \neg \in A$  and  $\neg \in B$  or  $\neg \in A$  and  $\neg \in C$

$\Rightarrow \neg \in (A \cup B)$

$\Rightarrow \neg \in (A - B) \text{ or } \neg \in (A - C)$

$\Rightarrow \neg \in (A - B) \cup (A - C)$

$\Rightarrow \neg \in (A - B) \cup (A - C)$

Also,  $\neg \in (A - B) \cup (A - C)$

thus,  $A - (B \cap C) = (A - B) \cup (A - C) + (A - B) \cap (A - C)$

## Venn Diagrams

A Venn diagram is a pictorial representation of sets which are used to show relationship between sets A and operations on them.

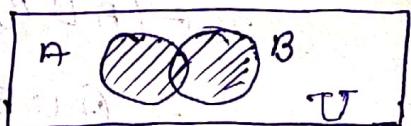
### Set Operations

### Symbol

### Venn Diagram

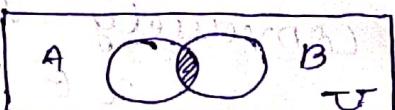
1. The union of set A and set B.

$$A \cup B$$



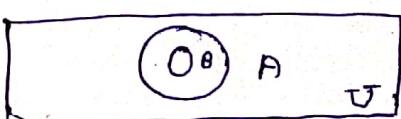
2. The intersection of set A and set B.

$$A \cap B$$



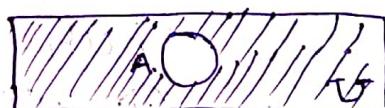
3. Set B is proper subset of A.

$$B \subset A$$



4. The complement of set A.

$$A' \text{ or } A^c$$



Example: Let  $A = \{1, 2, 3, 4, 5, 6\}$ ,  $B = \{3, 6, 8, 10, 12, 18\}$  and

$$C = \{2, 3, 5, 6, 10, 18\}$$

$$\text{then } A \cup B = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 18\}$$

$$A \cap B = \{3, 6\}, \text{ by } A - B = \{1, 2, 4, 5\}$$

# For any two sets A and B we have the following formula

$$\textcircled{1} \quad n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

$$\textcircled{2} \quad n(A - B) + n(A \cap B) = n(A)$$

or

$$n(B - A) + n(A \cap B) = n(B)$$

Ex. In a class of 25 students, 12 have taken mathematics, 8 have taken mathematics but not biology. Find the no. of students who have taken mathematics and biology and those who have taken biology but not mathematics.

Solu.  $n(A \cup B) = 25$   $n(A) = 12$   $n(A - B) = 8$   $n(A \cap B) = ?$   $n(B - A) = ?$

$$n(A - B) + n(A \cap B) = n(A)$$

$$8 + n(A \cap B) = 12$$

$$\boxed{n(A \cap B) = 4}$$

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

$$25 = 12 + n(B) - 4$$

$$17 = n(B)$$

$$n(B - A) + n(A \cap B) = n(B)$$

$$n(B - A) + 4 = 17$$

$$\boxed{n(B - A) = 13}$$

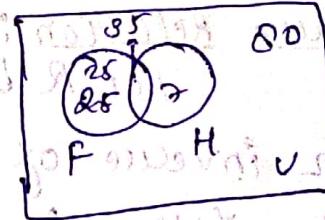
Ex. Out of 80 students in a class 60 play football, 53 play hockey and 35 both the games. How many students do not play these games?

Solu.

Total no. of students who play both games :  $100 - (25 + 35 + 18)$

$$= 80 - 78 = 2$$

(Relation)



# Cartesian product

A and B

ordered pair  $(a, b)$

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$$

Ex.  $A = \{a, b\}$   $B = \{1, 2\}$

then  $A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2)\}$   $\therefore A \times B \neq B \times A$

$$B \times A = \{(1, a), (1, b), (2, a), (2, b)\}$$

Let  $A$  and  $B$  be two sets. A relation from  $A$  to  $B$  is a subset of the cartesian product  $A \times B$ . If  $a \in A$  and  $b \in B$ , we say  $a$  is related to  $b$  by  $R$  i.e.  $(a, b) \in R$ .   
 $a R b$  read as ' $a$  is related to  $b$ ' or ' $a$  is related by  $R$  to  $b$ '.  $a R b$  iff  $a$  is not related to  $b$ .

e.g. Let  $A = \{2, 3, 4\}$  and  $B = \{3, 4, 5\}$ . List the elements of each relation  $R$  defined below and domain of Range.

Solution (a)  $a \in A$  is related to  $b \in B$ , i.e.  $a R b$  iff  $a < b$ .

(b)  $a R b$  iff  $a$  and  $b$  are both odd numbers.

Solution (a)  $R = \{(2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5)\}$

$$\text{domain}(R) = \{2, 3, 4\} \quad \text{Range}(R) = \{3, 4, 5\}$$

(b)  $R = \{(3, 3), (3, 5)\}$  domain( $R$ ) = {3} Range( $R$ ) = {3, 5}

### # Types of Relations in a set

#### (i) Inverse Relation:

Let  $R$  be any relation from a set  $A$  to a set  $B$ . Then inverse of  $R$  is denoted by  $R^{-1}$  and is defined by relation from  $B$  to  $A$ .

$$\text{e.g. } R = \{(a, b), (c, d), (e, f)\}$$

$$\text{Then } R^{-1} = \{(b, a), (d, c), (f, e)\}$$

$$[(R^{-1})^{-1} = R]$$

#### # Properties of relations :

#### (ii) Reflexive Relation

A relation  $R$  on a set  $A$  is reflexive if

if  $a \in A$ , for every  $a \in A$  i.e.  $(a, a) \in R$  OR  $\forall a \in A$ ,

$R = \{(n, n) | n \in \mathbb{N}\}$  is a reflexive because  $n \in \mathbb{N} \Rightarrow (n, n) \in R$

② Irreflexive Relation → A relation R on a set A is irreflexive if  $\forall a \in A, (a, a) \notin R.$

e.g. The relation R =  $\{(x, y) \in R^2 : x < y\}$  is irreflexive since  $x < x$  for no  $x \in R.$

③ Symmetric Relation →

A relation R on a set A is symmetric if whenever  $(a, b) \in R$  then  $(b, a) \in R$  i.e.  $aRb \Rightarrow bRa.$

e.g.  $R = \{(x, y) \in R^2 : x^2 + y^2 = 1\}$  is a symmetric relation on R. If  $x^2 + y^2 = 1$ , then  $y^2 + x^2 = 1$ . i.e.  $xRy \Rightarrow yRx$

④ Anti-Symmetric Relation →

If  $aRb$  and  $bRa \Rightarrow a = b$

e.g.  $R = \{(x, y) \in R^2 : x \leq y\}$

⑤ Transitive Relation →

If  $aRb$  and  $bRc \Rightarrow aRc$

e.g. Take  $b \neq c \Rightarrow aRc$  is false

# Equivalence Relation:

A relation on a set A is called an equivalence relation if it is reflexive, symmetric and transitive. That is R is an equivalence relation on A if it has the following properties -

(i)  $(a, a) \in R \quad \forall a \in A$  (reflexive)

(ii)  $(a, b) \in R$  implies  $(b, a) \in R$  (symmetric)

(iii)  $(a, b)$  and  $(b, c) \in R$  implies  $(a, c) \in R$  (transitive).

Ques If  $R$  be a relation on the set of integers  $\mathbb{Z}$  defined by  
 $R_2 \{ (x,y) : x \in \mathbb{Z}, y \in \mathbb{Z}, (x-y) \text{ is divisible by } 6 \}$

Soln Let  $x \in \mathbb{Z}$ . Then  $x-x=0$  and  $0$  is divisible by  $6$ .  
Therefore,  $xR_2 x \forall x \in \mathbb{Z}$ . Hence,  $R$  is reflexive.

Again,  $xR_2 y \Rightarrow (x-y)$  is divisible by  $6$ .

$$\Rightarrow (y-x) \text{ is } 6 \text{ divisible}$$

$$\Rightarrow (y-x)$$

Hence  $R$  is symmetric.

$xR_2 y$  and  $yR_2 z \Rightarrow (x-y)$  and  $(y-z)$  are divisible by  $6$ .

$\Rightarrow [(x-y)+(y-z)]$  is divisible by  $6$ .

$\Rightarrow (x-z)$  is divisible by  $6$ .

$$\Rightarrow xR_2 z$$

Hence,  $R$  is transitive. Thus  $R$  is an equivalence relation.

### Theorem

Let  $R$  and  $S$  be relation from  $A$  to  $B$ , show that

(i) if  $R \subseteq S$  then  $R^{-1} \subseteq S^{-1}$ .

(ii)  $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$

(iii)  $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$

Proof: (i) Let  $R \subseteq S$  if  $(a, b) \in R^{-1}$  then  $(b, a) \in R$ .

$\because R \subseteq S$  so,  $(b, a) \in S$

Then  $(a, b) \in S^{-1}$  - (2)

from (1) & (2)

$$R^{-1} \subseteq S^{-1}$$

(ii) Let  $(a, b) \in (R \cap S)^{-1}$ . Then  
 then,  $(b, a) \in R \cap S$ , so,  $(b, a) \in R$  and  $(b, a) \in S$   
 Next,  $(a, b) \in R$  and  $(a, b) \in S^{-1}$   
 so,  $(a, b) \in (R^{-1} \cap S^{-1})$   
 so,  $(R^{-1} \cap S^{-1}) \subseteq R^{-1} \cap S^{-1} - \textcircled{1}$   
 $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$

conversely, let  $(a, b) \in R^{-1} \cap S^{-1}$  then  $(a, b) \in R^{-1}$  if  $(a, b) \in S$   
 Hence  $(b, a) \in R$  and  $(b, a) \in S$ . so,  $(b, a) \in R \cap S$ . Now we  
 have  $(a, b) \in (R \cap S)^{-1}$ . so,  $R^{-1} \cap S^{-1} \subseteq (R \cap S)^{-1} - \textcircled{2}$

$R \cap S$  contains 0 or 1 or A relations on a set A.

\* Theorem: suppose R and S are relations  
 Prove that (R ∩ S) and (R ∪ S) are reflexive

- (i) if R and S are reflexive,  $R \cap S$  and  $R \cup S$  are symmetric
- (ii) if R and S are symmetric then  $R \cap S$  and  $R \cup S$  are symmetric

# 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. Then composition of R and  
 S, denoted by  $R \circ S$ , is the relation consisting of ordered pairs  
 $(a, c)$  where  $a \in A$ ,  $c \in C$  and for which  $b \in B$  such that  
 $(a, b) \in R$  and  $(b, c) \in S$ . Thus,

$$R \circ S = \{(a, c) \in A \times C : \text{for some } b \in B, (a, b) \in R, (b, c) \in S\}$$

$$R \circ R = R^2 \quad R \circ R \circ R = R^3 \quad a(R \circ S) c$$

Example: let  $A = \{1, 2, 3\}$ ,  $B = \{\alpha, \beta, \gamma\}$ ,  $C = \{x, y, z\}$  and  
 let  $R = \{(1, \alpha), (1, \beta), (\alpha, \beta), (\beta, \gamma)\}$  and  
 $S = \{(\beta, x), (\gamma, y), (\alpha, z)\}$  compute  $R \circ S$ .

Solu  
The ordered pair  $(i, p)$  in  $R$  and  $(p, y)$  is  $S$  produce the ordered pair  $(i, y)$  in  $R \circ S$ .

$(1, 2) \in R$  &  $(2, 3) \in S$  then  $(1, 3) \in R \circ S$

$(2, 1) \in R$  &  $(1, 2) \in S$  then  $(2, 2) \in R \circ S$

$(8, 2) \in R$  &  $(2, 1) \in R$  then  $(8, 1) \in R \circ S$

Thus,  $R \circ S = \{(1, 3), (2, 2), (8, 1)\}$

### Theorems

Let  $A, B, C$  and  $D$  be four non-empty sets. Let  $R_1$  be a relation from  $A$  to  $B$ ,  $R_2$  is a relation from  $B$  to  $C$  and  $R_3$  is a relation from  $C$  to  $D$ . Then

$$(i) (R_1 \circ R_2)^{-1} = R_2^{-1} \circ R_1^{-1}$$

$$(ii) (R_1 \circ R_2) \circ R_3 = R_1 \circ (R_2 \circ R_3)$$

### Proof

(i) Since  $R_1$  is a relation from  $A$  to  $B$  &  $R_2$  is a relation from  $B$  to  $C$ , then  $R_1 \circ R_2$  is a relation from  $A$  to  $C$ . Hence  $R_2 \circ R_1$  is a relation from  $C$  to  $B$ .

$(R_1 \circ R_2)^{-1}$  is a relation from  $C$  to  $A$ . — ①

Again, let  $R_1^{-1}$  is a relation from  $B$  to  $A$ .

$R_2^{-1}$  is a relation from  $C$  to  $B$ . — ②

Then  $(R_2^{-1} \circ R_1^{-1})$  is a relation from  $C$  to  $A$ . — ③

Hence from ① & ②,

for  $z \in C$  &  $\{x \in A \mid (z, x) \in R_2^{-1} \circ R_1^{-1}\} = \{x \in A \mid (z, x) \in R_2^{-1}\} \cap \{x \in A \mid (x, z) \in R_1^{-1}\}$

$$\exists (R_2^{-1} \circ R_1^{-1}) \subset \{x \in A \mid (z, x) \in R_2^{-1}\}$$

$\Leftrightarrow \text{iff } y \in B \text{ s.t. } (z, y) \in R_2 \text{ & } (y, z) \in R_1$

$\Leftrightarrow \text{iff } y \in B \text{ s.t. } (y, z) \in R_2 \wedge (z, y) \in R_1$

$\Leftrightarrow \exists y \in B \text{ s.t. } (z, y) \in R_2^{-1} \circ R_1^{-1}$

$\Rightarrow \exists (R_2^{-1} \circ R_1^{-1}) \subset (R_2^{-1} \circ R_1^{-1})$  Hence

$$(R_1 \circ R_2)^{-1} = R_2^{-1} \circ R_1^{-1}$$

Thm. If  $R$  is a relation on set  $A$ , then  $R$  is transitive iff  $R^2 \subseteq R$

Proof: Let  $R$  be transitive and  $(x_1, z) \in R^2$ . But by defn of  $R^2$ ,  $x_1, z \in A$  s.t.  $(x_1, y) \in R$  and  $(y, z) \in R$  so  $(x_1, z) \in R$ . Hence

$$R^2 \subseteq R.$$

conversely, suppose  $R^2 \subseteq R$ . let  $(x_1, y) \in R$   $(y, z) \in R$ . Then  $(x_1, z) \in R^2$  and hence in  $R$ . This proves that  $R$  is transitive.

## #functions

A function is a relation between sets that associates to every element of a first set exactly one element of the second set.

e.g. The following relation is a function

$$\{( -1, 0 ), ( 0, -3 ), ( 1, -3 ), ( 3, 0 ), ( 4, 8 )\}$$

(ii)  $\{( 6, 10 ), ( -2, 3 ), ( 0, 4 ), ( 6, 4 )\} \rightarrow$  Not a function

The statement "f is a function from A to B" is represented by

$$f: A \rightarrow B \text{ or } A \xrightarrow{f} B$$

e.g. let  $A = \{ 1, 2, 3, 4, 5 \}$  and  $B = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 \}$

(i)  $f_1 = \{ ( 1, 1 ), ( 2, 6 ), ( 3, 7 ), ( 4, 9 ), ( 5, 12 ) \}$

$$\text{Range}(f) = \{ 1, 6, 7, 9, 12 \}$$

(ii)  $f_2 = \{ ( 1, 1 ), ( 2, 3 ), ( 4, 7 ), ( 5, 12 ) \}$  then f is not a func<sup>t<sub>2</sub></sup> because

(iii)  $f_3 = \{ ( 1, 1 ), ( 2, 3 ), ( 4, 7 ), ( 5, 12 ) \}$  then f has no image in B.

\* let f and g be two functions. Then f and g are said to be equal if

(i)  $\text{dom } f = \text{dom } g$

(ii) co-domain of f = co-domain of g

and

(iii)  $f(x) = g(x)$  if  $x \in \text{dom } f$

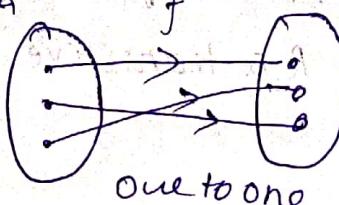
## Types of functions

### (i) One-to-one function:

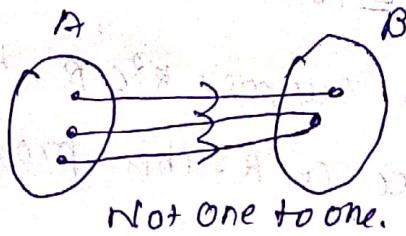
A function from A to B is called one-to-one if  
if for all elements  $x_1, x_2 \in A$  such that  $f(x_1) = f(x_2)$ .

implies  $x_1 = x_2$ .

if  $\exists f : A \rightarrow B$



One to one



Not one to one.

#### Example:

If  $f(x) = 3x - 2$ , then show that  $f$  is one-one

$$\text{Solve } f(x_1) = 3x_1 - 2, \quad f(x_2) = 3x_2 - 2$$

$$f(x_1) = f(x_2) \Rightarrow 3x_1 - 2 = 3x_2 - 2$$

$$(x_1 = x_2)$$

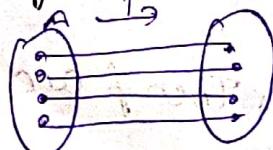
### (ii) Many-one function:

A function  $f$  from A to B is said to be many-one if and only if two or more elements of A have some image in B.

e.g. let  $f(x) = x^2$ ,  $x$  is any real number and  $f : R \rightarrow R$ ,  
then  $f$  is many one function.

onto function:  
A function  $f$  from A to B is called onto (surjective) if every element of B is the image of some element in A,

that is, Range of  $B = \text{codomain of } B$ .



In order to check whether  $y = f(x)$  from a set A to B is onto or not, write it in terms of y and set  
if for every  $y \in B$ ,  $\exists x \in A$  such that  $y = f(x)$ .

$f: A \rightarrow B$

range  $f \subseteq B$

Preimage  $\rightarrow f^{-1}(B) \subseteq A$   $f: N \rightarrow N$

$$\{ \text{preim. } (d, 0) \} = \{ d \in D \}$$

$$D = D \times D$$

$$= D \times D$$

forward image of  $D \times D$  under  $f$  is  $B \times B$

forward image of  $b \in B$  under  $f$  is  $f^{-1}(b)$

$$(x, y) \in D \times D$$

forward image of  $(x, y) \in D \times D$  under  $f$  is  $f(x, y)$

$$(x, y) \in D \times D$$

forward image of  $x \in D$  under  $f$  is  $f(x)$

$$f(x) = y \in D$$

forward image of  $y \in D$  under  $f$  is  $f^{-1}(y)$

forward image of  $(x, y) \in D \times D$  under  $f$  is  $f(x, y)$

$$f(x, y) = z \in D$$

## Group Theory

If  $f: A \times A \rightarrow A$   
 $A \times A = \{ (a, b) , a \in A, b \in A \}$

### Binary operations:

If  $f: A \times A \rightarrow A$ , then  $f$  is said to be binary operation on  $A$ . The symbols  $+$ ,  $\circ$ ,  $\circlearrowleft$ ,  $\circlearrowright$  are used to denote binary operations on a set.

Thus,  $+$  will be a binary operation on  $A$  iff  $(a+b) \in A$  if  $a, b \in A$ .

Algebraic Structure:  
 $(A, *)$ ,  $(R, *, \circ)$

### Laws of binary operations:

1) Associative law  $\rightarrow$  Let  $A$  be a non-empty set then

$$a * (b * c) = (a * b) * c \text{ if } a, b, c \in A$$

2) Commutative law  $\rightarrow$   
 $a * b = b * a \text{ if } a, b \in A \text{ e.g. } (N, +)$

3) Identity element  $\rightarrow$

Let  $e \in A$  Then

$$a * e = e * a = a \quad \forall a \in A$$

4) Inverse element  $\rightarrow$

consider  $A$  & let  $a$  having identity element  $e$  w.r.t. B.O.  $*$

Then for each element  $a \in A \exists b \in A$

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

# Group: Let  $(A, *)$  be an algebraic structure, where  $*$  is a binary operator, then  $(A, *)$  is called a group under this operation if the following conditions are satisfied-

1) Closure law  $\rightarrow$   $a * b \in A \quad \forall a, b \in A$

(ii) Associative law  $\rightarrow a * (b * c) = (a * b) * c \forall a, b, c \in G$

(iii) Identity element  $\rightarrow$  for some  $e \in G$ , ex  $a = a * e = e * a \forall a \in G$

(iv) Inverse element  $\rightarrow$  for each  $a \in G$  there exists  $a' \in G$  such that

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

Note: A group  $G$  is said to be Abelian if  $a * b = b * a \forall a, b \in G$  (In addition to above prop. it also holds commutative property)

Ques. Show the set  $\{1, -1, i, -i\}$  is an abelian group w.r.t. multiplication.

Solu.  $1 * 1 = 1$

$$1 * i = i * 1 = i \quad \text{I. Inverse}$$

Theorem: If  $(G, *)$  is a group and  $a, b, c \in G$  then

(cancellation law)  $\rightarrow$  If  $(G, *)$  is a group and  $a, b, c \in G$  then

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

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

Proof:

(i) "  $a \in G$  so from  $a * b = a * c$  we can write

$$a^{-1} * (a * b) = a^{-1} * (a * c) \quad a^{-1} * a = e$$

$$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c \quad a^{-1} * a = e$$

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

$$\Rightarrow b = c \quad b = a$$

Thm: In a group  $(G, *)$   $(ab)^{-1} = b^{-1}a^{-1}$

\* Show that if  $a, b$  are arbitrary elements of a group  $G$  then  $(ab)^{-1} = a^{-1}b^{-1}$  iff  $G$  is abelian.

then let  $a, b \in G$  suppose  $(ab)^{-1} = a^{-1}b^{-1}$  — (1)

$$(ab)^{-1} = a^{-1}b^{-1} \quad \text{Left cancell. of } ab \in G$$

we have to show that  $ab = ba \quad ab \in G$

$$(ab)^{-1} = a^{-1}b^{-1} \quad \text{Left cancell. of } ab \in G$$

$$(ab)(ab)^{-1} = (aa)(bb) \quad \text{So by left cancell. of Right cancell. we have}$$

$$\Rightarrow a(ba)b = a(lab)b \quad [ba = ab]$$

Hence,  $G$  is abelian.

Conversely, suppose  $G$  is an abelian group so that  $ab = ba$  iff  $a \in b^{-1}G$ .

To prove that  $(ab)^2 = a^2b^2$  (from ①)

$$\because (ab)^2 = (ab)(ab) = a(ba)b \quad (\text{from ①})$$

$$= (aa)(bb) = \underline{\underline{a^2b^2}}$$

Hence, Proved.

Subgroup:

If the following conditions are satisfied -

i)  $a * b \in S \forall a, b \in S$

ii)  $a * (b * c) = (a * b) * c \forall a, b, c \in S$

iii) for some  $e \in S$ ,  $e * a = a * e = a \forall a \in S$ .

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

Note: Since set is a subset of itself. Therefore, if  $G$  is a group of  $G$  then  $G$  itself is a subgroup of  $G$ . The set  $\{e\}$  is also a subgroup of  $G$ . These two subgroups  $\{e\}$  and  $(G, *)$  of  $G$  is called improper or trivial subgroups. Others are proper or non-trivial.

E.g. The multiplicative group  $\{-1, 1\}$  is a subgroup of the multiplicative group  $\{1, -1, i, -i\}$ .

Theorem:

A non-empty subset of  $H$  of a group  $G$  is a subgroup of  $G$  iff

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

ii)  $a \in H \Rightarrow a^{-1} \in H$

iii)  $a \in H \Rightarrow a + d \in H$

iv)  $a \in H \Rightarrow a * d \in H$

v)  $a \in H \Rightarrow a / d \in H$

vi)  $a \in H \Rightarrow a \cdot d \in H$

vii)  $a \in H \Rightarrow a \cdot d^{-1} \in H$