SUB: MATHEMATICS (GE/RC)

B. Sc. 2nd Semester

Group

§ Binary operation on a set:

Let A be a non-empty set. Then $A \times A = \{(a,b) : a, b \in A\}$. If $f: A \times A \longrightarrow A$, then f is said to be a binary operation on the set A. The image of the ordered pair (a,b) under the function f is denoted by afb. Often we use symbols $+, \times, -, \div, \circ, *$ etc to denote binary operation on a set. Thus '$*$' will be a binary operation on A iff $a*b \in A \; \forall \; a, b \in A$ and $a*b$ is unique.

A binary operation on a set A is sometimes also called a binary composition in the set A. If '$*$' is a binary composition in A, then $a*b \in A \; \forall \; a, b \in A$. Therefore A is closed w.r.t. the composition denoted by '$*$'.

Examples:-

1. '$+$' (addition) and '$\times$' (multiplication) are binary operation on the set $\mathbb{N}$ of natural numbers.

e.g. $\quad 1, 2 \in \mathbb{N} \Rightarrow 1+2 = 3 \in \mathbb{N}$

and $1, 2 \in \mathbb{N} \Rightarrow 1.2 = 2 \in \mathbb{N}$

Therefore $\mathbb{N}$ is closed w.r.to addition and multiplication.

But '$-$' (subtraction) and '$\div$' (division) are not binary operation on $\mathbb{N}$.

e.g. $\quad 1, 2 \in \mathbb{N} \Rightarrow 1-2 = -1 \notin \mathbb{N}$

and $1, 2 \in \mathbb{N} \Rightarrow 1 \div 2 = 1/2 \notin \mathbb{N}$

Thus $\mathbb{N}$ is not closed w.r.to subtraction and division.

2. '$+$', '$-$', '$\times$' are binary operation on the set of integers I but '$\div$' is not binary operation on I.

§ Group :

Definition : Let G be a non-empty set and '$*$' be a binary operation on G. Then $(G, *)$ is said to be a group if it satisfies the following postulates.

(i) Closure property : $a * b \in G \ \forall \ a, b \in G$

(ii) Associativity : $(a*b)*c = a*(b*c) \ \forall \ a, b, c \in G$

(iii) Existence of identity; There exists an element $e \in G$ such that $a * e = a = e * a \ \forall \ a \in G$. The element e is called the identity.

(iv) Existence of inverse : For each $a \in G$, there exists an element $b \in G$ such that $a * b = e = b * a$. Then the element b is called the inverse of a and we write $b = a^{-1}$. Thus a^{-1} is an element of G such that $a * a^{-1} = e = a^{-1} * a$.

Abelian or Commutative group :

Definition :- A group $(G, *)$ is said to be an abelian or commutative if in addition to the above four postulates the following postulate is also satisfied.

(v) Commutativity :- $a * b = b * a \ \forall \ a, b \in G$.

§ Finite and infinite groups :-

A group G is called a finite group if G has a finite number of distinct elements and if the number of elements is infinite then it is called an infinite group.

§ Order of a group :-

The number of elements of a finite group is called the order of the group and is denoted by $O(G)$ or $|G|$. An infinite group is said to be of infinite order.

e.g. 1. $G = \{1, -1, i, -i\}$ is group under multiplication
G is finite and $O(G) = 4$

2. $(\mathbb{Z}, +)$ is group
$\mathbb{Z}$ is infinite group & $|\mathbb{Z}|$ is infinite.

§ Order of an element of a group.

Definition:- Let (G, o) be a multiplicative group whose identity element is e. Let $a \in G$ be any element. If there exists a least positive integer n such that $a^n = e$ but $a^{n-1} \neq e$, then n is called the order of a and is denoted by $o(a)$ or $|a|$.

If there exists no positive integer n such that $a^n = e$, then we say that a is of infinite order or of zero order.

If G is in additive group then order of a is n if n is the least positive integer such that $na = e$

Example: 1. Consider the multiplicative group $G = \{1, \omega, \omega^2\}$
Since 1 is the identity element, therefore $o(1) = 1$ ($\because 1^1 = 1$)

$\because \omega^3 = 1 \quad \therefore o(\omega) = 3$
$\because (\omega^2)^3 = 1 \quad \therefore o(\omega^2) = 3$

§ Integral powers of an element of a group:-

Let G be a group and $a \in G$. If n is a positive integer we define $a^n = a.a.a \cdots a$ to n factors. In particular $a^1 = a$, $a^2 = a.a$, $a^3 = aaa$, ... and so on.

If e is the identity element of the group G, then we define $a^0 = e$.

If n is a positive integer then $-n$ is a negative integer. Now we define $a^{-n} = (a^n)^{-1}$ where $(a^n)^{-1}$ is the inverse of a^n of G. $\therefore a^{-n} \in G$.

Thus we have defined a^n for all integral values of n positive, zero or negative.

If n is a positive integer, then according to our definition

$$a^{-n} = (a^n)^{-1} = (a\,a\,a \;\cdots\; a \text{ upto } n \text{ factors})^{-1}$$
$$= (a^{-1})(a^{-1})(a^{-1}) \cdots (a^{-1}) \text{ upto } n \text{ factors}$$
$$= (a^{-1})^n$$

$\therefore$ we write $a^{-n} = (a^n)^{-1} = (a^{-1})^n$

Note: Suppose our group consists of a non empty set G equipped with binary operation denoted multiplicatively. (i.e we omit $*$)

§ Some General properties of a group:-

Property 1: The identity element in a group is unique.

Proof:- Let G be any group. If possible, let e and e' be two identity elements of G. We have

$ee' = e = e'e$ when e' is identity and $e \in G \rightarrow (1)$

and $e'e = e' = ee'$ when e is identity and $e' \in G \rightarrow (2)$

From (1) and (2) we get $e = e'$.

Hence the identity element is unique.//

Property 2: The inverse of each element of a group is unique

Proof: Let a be any element of a group G and let e be the identity element of G. If possible, let b and c be two inverses of a.

$\therefore ab = e = ba$ and $ac = e = ca$

Now $b = be = b(ac) = (ba)c$ [by associative property]
$= ec = c$

Hence the inverse of a is unique.//

Property 3:- If $a \in G$ then $(a^{-1})^{-1} = a$
i.e the inverse of a^{-1} is a

Proof:- Let e be the identity element of G, we have

$$aa^{-1} = a^{-1}a = e$$

Now $a^{-1}a = e$

$\Rightarrow (a^{-1})^{-1}(a^{-1}a) = (a^{-1})^{-1}e$ [Multiplying by $(a^{-1})^{-1}$ on both sides from left, $\because a^{-1} \in G \Rightarrow (a^{-1})^{-1} \in G$]

$\Rightarrow [(a^{-1})^{-1}a^{-1}]a = (a^{-1})^{-1}$ [$\because$ G is associative]

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

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

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

Property 4:- If a and b are two elements in a group G, then
$(ab)^{-1} = b^{-1}a^{-1}$

Proof: We have $a \in G$ and $b \in G$, therefore $a^{-1} \in G$, $b^{-1} \in G$

Then $aa^{-1} = e = a^{-1}a$

and $bb^{-1} = e = b^{-1}b$

Now $(ab)(b^{-1}a^{-1}) = [a(bb^{-1})]a^{-1}$ [by associativity]

$= (ae)a^{-1}$

$= aa^{-1}$

$= e$

Again $(b^{-1}a^{-1})(ab) = b^{-1}[(a^{-1}a)b]$ [by associativity]

$= b^{-1}(eb)$

$= b^{-1}b$

$= e$

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

$\Rightarrow b^{-1}a^{-1}$ is the inverse of ab

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

Property 5: Cancellation laws hold in a group i.e., if a, b, c be any three elements of a group G, then

(i) $ab = ac \Rightarrow b = c$ (left cancellation law)

(ii) $ba = ca \Rightarrow b = c$ (right cancellation law)

Proof: We have $a \in G \Rightarrow a^{-1} \in G$ such that $aa^{-1} = e = a^{-1}a$ where e is the identity element.

(i) Now $ab = ac$

$\Rightarrow a^{-1}(ab) = a^{-1}(ac)$ [multiplying both sides on the left by a^{-1}]

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$ [by associativity]

$\Rightarrow eb = ec$

$\Rightarrow b = c$

(ii) Again $ba = ca$

$\Rightarrow (ba)a^{-1} = (ca)a^{-1}$ [multiplying both sides by a^{-1} on right]

$\Rightarrow b(aa^{-1}) = c(aa^{-1})$ [by associativity]

$\Rightarrow be = ce$

$\Rightarrow b = c$

Property 6: If a, b are any two elements of a group G, then the equations $ax = b$ and $ya = b$ have unique solutions in G.

Proof: We have $a \in G \Rightarrow a^{-1} \in G$ such that $aa^{-1} = e = a^{-1}a$, where e is the identity element of G.

$\therefore a \in G, b \in G \Rightarrow a^{-1} \in G, b \in G$

$\Rightarrow a^{-1}b \in G$ [by closure preoperty]

Now putting $x = a^{-1}b$ in the equation $ax = b$, we get

$$a(a^{-1}b) = (aa^{-1})b = eb = b$$

Thus $x = a^{-1}b$ is a solution in G of the equation $ax = b$.

Next we show that the solution of the equation is unique, If possible, let x_1 and x_2 be two solutions of the equation $ax = b$.

Then $ax_1 = b$ and $ax_2 = b$

$\therefore ax_1 = ax_2$

$\Rightarrow x_1 = x_2$ [by left cancellation law]

Hence the solution is unique.

Now we are to prove that the equation $ya = b$ has a unique solution in G. We have $a \in G, b \in G \Rightarrow ba^{-1} \in G$

Now $(ba^{-1})a = b(a^{-1}a) = be = b$

$\therefore y = ba^{-1}$ is a solution in G of the equation $ya = b$.

If possible, let y_1 and y_2 be two solutions of the equation.

Then $y_1 a = b$ and $y_2 a = b$

$\therefore y_1 a = y_2 a$

$\Rightarrow y_1 = y_2$ [by right cancellation law]

Hence the equation $ya = b$ has unique solution.

Example 1: Show that the set of integers $\mathbb{Z}$ forms an abelian group with respect to addition.

Solution: (i) closure property: We know that the sum of any two integers is also an integer. i.e $a+b \in \mathbb{Z}$ $\forall a, b \in \mathbb{Z}$

(ii) Associativity: We know that addition is associative in $\mathbb{Z}$.

$\therefore (a+b)+c = a+(b+c)$ $\forall a, b, c \in \mathbb{Z}$

(iii) Existence of identity: We have $0 \in \mathbb{Z}$ and $a+0 = a = 0+a$ $\forall a \in \mathbb{Z}$. Therefore 0 is the additive identity of $\mathbb{Z}$.

(iv) Existence of inverse: Let $a \in \mathbb{Z}$ be any element. Then $-a \in \mathbb{Z}$ and $a+(-a) = 0 = (-a)+a$. 0 is the identity of $\mathbb{Z}$.

$\therefore -a$ is the additive inverse of a

$\therefore (\mathbb{Z}, +)$ is a group w.r.to addition

(v) Commutativity : We know that addition is commutative in $\mathbb{Z}$

$\therefore \quad a+b = b+a \quad \forall\, a,b \in \mathbb{Z}$

Hence $(\mathbb{Z},+)$ is an abelian group.

Note: Also $\mathbb{Z}$ is an infinite set. Therefore $(\mathbb{Z},+)$ is an infinite abelian group.

Example 2: In the set $\mathbb{Z}$ of integers the binary operation '$+$' defined as follows : $a+b = a+b+1$. Prove that $\mathbb{Z}$ is a group with respect to '$+$'.

Proof : (i) Closure property : Let $a,b \in \mathbb{Z}$

$\therefore\ a+b \in \mathbb{Z}$

$\Rightarrow a+b+1 \in \mathbb{Z} \quad (\because 1 \in \mathbb{Z})$

$\Rightarrow a+b \in \mathbb{Z}$

$\therefore\ \mathbb{Z}$ is closed under '$+$'

(ii) Associativity : Let $a,b,c \in \mathbb{Z}$

$$\begin{aligned}\therefore\ (a+b)+c &= (a+b+1)+c \\ &= a+b+1+c+1 \\ &= a+b+c+2\end{aligned}$$

And

$$\begin{aligned}a+(b+c) &= a+(b+c+1) \\ &= a+b+c+1+1 \\ &= a+b+c+2\end{aligned}$$

$\therefore\ (a+b)+c = a+(b+c) \quad \forall\, a,b,c \in \mathbb{Z}$

(iii) Existence of identity : Let $a \in \mathbb{Z}$ and e be the identity of $\mathbb{Z}$ w.r.to '$+$'

$\therefore\ a+e = a = e+a$

Now $a+e = a$

$\Rightarrow a+e+1 = a$

$\Rightarrow e = -1 \in \mathbb{Z}$

Also $e+a=a$

$\Rightarrow e+a+1=a$

$\Rightarrow e=-1\in\mathbb{Z}$

Since $-1\in\mathbb{Z}$, $a\in\mathbb{Z}$

$\therefore (-1)+a=-1+a+1=a$

$\therefore -1$ is the identity element of $\mathbb{Z}$ w.r.t. '+'

(iv) Existence of inverse: Let $a\in\mathbb{Z}$. Then b will be the inverse of a if $a+b=-1=b+a$ where -1 is the identity.

Now $a+b=-1$

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

$\Rightarrow a+b=-2$

$\therefore b=-2-a\in\mathbb{Z}$

Also $b+a=-1$

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

$\Rightarrow b=-2-a\in\mathbb{Z}$

$\therefore -2-a$ is the inverse of a w.r.t. '+'

Since $a*(-2-a)=a+(-2-a)+1$

$=-1$

$\therefore$ Every element of $\mathbb{Z}$ has an inverse.

$\therefore (\mathbb{Z},+)$ is a group.

Example 3: Let $G=\mathbb{R}\setminus\{-1\}$ and it is defined $a*b=a+b+ab$ for every $a,b\in G$. Show that $\langle G,*\rangle$ is an abelian group.

Solution: Here, the operation '$*$' on G is defined as follows

$a*b=a+b+ab$ (where $G=\mathbb{R}\setminus\{-1\}$)

(i) Closure Property: Let $a,b\in G$. Then a and b are real numbers such that $a\neq-1$, $b\neq1$

Now $a*b=a+b+ab$ which is also a real number and it cannot be equal to -1.

Since $a+b+ab=-1 \Rightarrow a+b+ab+1=0$

$\Rightarrow (a+1)(b+1)=0$

$\therefore$ $a=-1$ or $b=-1$ which is not so.

$\therefore$ $a*b \in G$ $\forall$ $a,b \in G$. Hence G is closed w.r.t. the operation '$*$'.

(ii) Associativity :- If $a,b,c \in G$

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

Also $a*(b*c) = a*(b+c+bc)$
$$= a+(b+c+bc)+a(b+c+bc)$$
$$= a+b+c+ab+ac+bc+abc$$

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

(iii) Existence of identity : Let $e \in G$ i.e let e be a real number and $e \neq -1$. Then e will be the identity if $a*e = a = e*a$

Now, $a*e = a$

$\Rightarrow a+e+ae = a$

$\Rightarrow e+ae=0$

$\Rightarrow e(1+a)=0$

$\Rightarrow e=0$ or $1+a=0$

$\therefore$ $e=0 \in G$ $\therefore$ $a=-1$ is not possible $\because a \neq -1$

Also $e*a = a$

$\Rightarrow e+a+ea = a$

$\Rightarrow e(1+a)=0$

$\therefore$ $e=0 \in G$ $\because a \neq -1$

Since $0 \in G$ and we have for any $a \in G$ $(a \neq -1)$

$$\therefore 0*a = 0+a+0$$
$$= a$$

$\therefore$ 0 is the identity of G.

(iv) Existence of inverse: Let $a \in G$ and $a \neq -1$. Then the element $b \in G$ will be the inverse of a if

$$a * b = 0 = b * a$$

Now $a * b = 0$

$\Rightarrow a + b + ab = 0$

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

$\therefore b = -\frac{a}{a+1} \quad (\because a \neq -1)$

Also $b * a = 0$

$\Rightarrow b + a + ba = 0$

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

$\therefore b = \frac{-a}{a+1} \quad (\because a \neq -1)$

Now $b = -\frac{a}{a+1} \in G$. Also $-\frac{a}{a+1} \neq -1$

Again $a * \left(-\frac{a}{a+1}\right) = a + \left(\frac{-a}{a+1}\right) + \left(-\frac{a^2}{a+1}\right)$

$$= \frac{a^2 + a - a - a^2}{a+1} = \frac{0}{a+1}$$

$= 0$, which is the identity of G.

$\therefore -\frac{a}{a+1}$ is the inverse of a

Also $a * b = a + b + ab$

$= b + a + ba$

$= b * a$, therefore operation is also commutative.

Hence $(G, *)$ is an abelian group.

§ Semi-group: An algebraic structure $(G, *)$ is called a semigroup if '$*$' satisfies the (i) closure property and (ii) Associativity.

For example - the set $\mathbb{N}$ of natural numbers is a semigroup w.r.t. addition.

Note: Every group is a semi-group but every semi-group may not be a group.

---x---