Chapter 1

GROUPS AND RINGS

Binary Operation :-

Let S be a non-empty set. A Binary Operation $*$ on S is a function $*: S * S \rightarrow S$. The image of any ordered pair (a,b) of elements of S under $*$ is denoted by $a*b$.

The Number sets are

N = the set of positive integers $= \{1, 2, 3, \}$

Z = the set of integers $= \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$

Q = the set of rational numbers

$= \left\{\frac{p}{q} \mid p, q, \in Z, q \neq 0\right\}$

R = the set of real numbers

C = the set of complex numbers

$= \{a + ib \mid a, b \in R\}$.

Thus $(N, +)$, $(Z, +)$, $(Q, +)$, $(R, +)$ and $(C, +)$ are algebraic Systems.

Let $S = \{0, 1, 2\}$. A Binary Operation $*$ on S is defined by $0*0 = 0$, $0*1 = 1*0 = 1$, $0*2 = 2*0 = 0$.

$1*1 = 2$, $1*2 = 2*1 = 1$, $2*2 = 1$.

The result of the operation can be displayed as a two way table.

The table is

$*$	0	1	2
0	0	1	0
1	1	2	0
2	0	1	1

This table is called the multiplication table or Operation table or cayley table.

Properties of Binary Operations.

(1) Associative property:

A Binary operation $*$ on S is said to be associative if $a*(b*c) = (a*b)*c \quad \forall\ a, b, c \in S$.

(2) Commutative property.

A Binary Operation $*$ on S is said to be Commutative if $a*b = b*a \ \forall\ a, b \in S$

(3) Existence of Identity.

A Binary Operation $*$ on S is said to have an identity element $e \in S$ if $e*a = a*e = a \ \forall\ a \in S$.

(4) Existence of inverse.

Let $*$ be a binary operation on S with an identity element e in S. An element $a \in S$ is said to have an inverse $a' \in S$ if $a*a' = a'*a = e$.

(5) Closure property.

Let $*$ be a binary operation On S and A be a subset of S. A is said to be closed under $*$ if $a*b \in A$ $\forall\ a, b \in A$

(6) Group:

A non-empty set G with a binary Operation $*$ defined on it is called a group if the following axioms are satisfied. Let $*$ be a binary Operation on S and A be a subset of S. A, is said to be closed under $*$ if $a*b \in A \ \forall\ a, b \in A$.

1. Associativity:

For all $a, b, c \in G$, we have $a*(b*c) = (a*b)*c$.

2. Identity:

There exists an element $e \in G$ such that $a * e = e * a = a \quad \forall a \in G$.

3. Inverse:

For each $a \in G$, there exists an element a' such that $a * a' = a' * a = e$.

The group is denoted by $(G, *)$ the set and the binary operation.

Order of a Group.

Let G be a group under the operation $*$. The number of elements in G is called the order of Group G and is denoted by $o(G)$.

If G has n elements, then $o(G) = n$.

If the $o(G)$ is finite, then G is called a finite group, otherwise it is an infinite group.

Abelian group:

A group $(G, *)$ is said to be abelian or commutative if $a * b = b * a \quad \forall a, b \in G$.

THEOREM 1: Let $(G, *)$ be a group, then (i) identity element is unique (ii) For each $a \in G$, inverse is unique.

Proof:- Given $(G, *)$ is a group.

(i) Let e and e' be two identity elements of G. Then by identity axiom (2) of a group we get.

$e * e' = e$ [Treating e' as identity]

and $e * e' = e'$ [Treating e as "]

$e = e'$

Hence identity element is unique.

(ii) Let e be the identity element of G. Let $a \in G$ be any element. Suppose a' and a'' are two inverses of a, then by inverse axiom,

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

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

Now, $a' = a' * e$ [$\because$ e is identity]

$= a' * (a * a'')$ [$\because a * a'' = e$]

$= (a' * a) * a''$ [by associative axiom]

$= e * a''$ [$\because a' * a = e$]

$= a''$.

THEOREM 2

In a group $(G, *)$ the cancellation laws hold. For all $a, b, c \in G$.

(i) $a * b = a * c \Rightarrow b = c$ [Left cancellation law]

(ii) $b * a = c * a \Rightarrow b = c$ [Right cancellation law].

Proof: Given $(G, *)$ is a group. Let e be the identity element of G.

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

Let a^{-1} be the inverse of a.

premultiplying by a^{-1}, we get

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

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

$\Rightarrow e * b = e * c$ [by inverse]

$\Rightarrow b = c$ [by identity]

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

$\Rightarrow (b * a) * a^{-1} = (c * a) * a^{-1}$ [post multiplying by a^{-1}.

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

$\Rightarrow b * e = c * e$ [by inverse]

$\Rightarrow b = c$ [by identity]

THEOREM 3 In a group $(G, *)$ the equation $a * x = b$ and $y * a = b$ have unique solutions for the unknowns x and y as $x = a^{-1} * b$, $y = b * a^{-1}$, where $a, b \in G$.

Proof: Given $(G, *)$ is a group and let e be the identity element of G and a^{-1} be the inverse of a.

Given $a * x = b$

$\Rightarrow a^{-1} * (a * x) = a^{-1} * b$. [premultiplying by a^{-1}]

$\Rightarrow (a^{-1} * a) * x = a^{-1} * b$ [by associative

$\Rightarrow e * x = a^{-1} * b$ [by inverse

$\Rightarrow x = a^{-1} * b$ [by identity

Thus $x = a^{-1} * b \in G$ is a solution.

We shall now prove the uniqueness.

Suppose, $x_1, x_2 \in G$ be two solutions of $a * x = b$ then

$a * x_1 = b$ and $a * x_2 = b$

$a * x_1 = a * x_2$

$\Rightarrow x_1 = x_2$ [by left cancellation laws.

Hence the solution is unique and the unique solution is $x = a^{-1} * b$.

Similarly we can prove that $y * a = b$ has unique solution $y = b * a^{-1}$.

Now $y * a = b$.

$\Rightarrow (y * a) * a^{-1} = b * a^{-1}$ [post-multiplying by a^{-1}]

$\Rightarrow (y * (a * a^{-1})) = b * a^{-1}$ [by associative.