© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 04 , Issue : 13 | October – December 2017

GROUP THEORY

Priya, Department of Mathematics, KUK

Abstract:

Group theory is the study of algebraic structures called groups. It is an important part in present day mathematics, was established early in the nineteenth century in connection with the solutions for algebraic equations. Originally, a group was the set of all permutations of the roots of an algebraic equation which has the property that the combination of any two of these permutations again belongs to the set. Later the idea was generalized to the concept of an abstract group. An abstract group is essentially the study of a set with an operation defined on it. Group theory has many useful applications both within and outside mathematics. Groups arise in a number of apparently unconnected subjects. In fact, they appear in crystallography and quantum mechanics, in geometry and topology, in analysis and algebra, and even in biology. Before we start talking about a group it is beneficial to discuss the binary operation on a set, because these are sets on whose elements algebraic operations can be made. We can obtain a third element of the set by combining two elements of a set. It is not always true, which is why this concept needs attention.

Keywords:

C is set of complex numbers.
R is set of real numbers.
Q is set of rational numbers.
Z is set of integers.
N is set of natural numbers.

Set:

Set is well defined collection of distinct objects. For example

{tiger, lion, puma, cheetah, leopard, cougar, ocelot}

is a set of large species of cats.

Semigroup:

If S is a non empty and * be a binary operation on S, then the algebraic system {S,*} is called a semigroup, if the operation * is associative i.e. if for any a, b, c €S then

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

For example, if S is the set of positive even numbers, then {E, +} is a semigroup.

Monoid:

If a semigroup {M,*} has an identity element with respect to the operation *, then {M,*} is called a monoid i.e. if

- for any a, b, c € M, (a*b)*c=a*(b*c)
- if there exists an element e€M such that for any a€M, a*e=e*a

then the algebraic system {M,*} is called a monoid.

For example, if N is the set of natural numbers, then {N, X} is monoid with the identity 1.

Group:

A group is a monoid with an inverse element. The inverse element denoted by I of a set is an element such that (a*I)=(I*a)=a, for each element a€G.

So,a group holds four properties,

- Closure,

- Associative,
- Identity element,
- Inverse element.

For example, if R is the set of real numbers, then {R,+} is a group with identity 0.

Order of a Group:

The number of elements in a group is called order of the group. It is denoted by o(G).

For example

a) order of group of real numbers is infinite i.e. o(R)=∞
b) order of group of complex numbers is infinite i.e. o(C)=∞
c) order of group of multiplication modulo n is n.
d) order of Klein's 4-group is 4.

Order of an Element:

Let G be a group, the order of an element a€G is the least positive integer n such that a^n=e. If such n does not exist than order of element a is infinite. It is denoted by o(a).

For example

a) If Z is the group of integers i.e.
   Z={0,±1,±2,±3,…} then
   o(0)=1
   o(1)=∞
b) If Z*={1,-1} is a group with respect to multiplication then
   o(1)=1 and
   o(-1)=2

Abelian Group:

A group G is said to be abelian group if every element of G commute with each other i.e.

x*y=y*x for all x,y €G

For example

a) The group of integers with respect to addition is an abelian group i.e. (Z,+) is an abelian group.
b) The group of multiplication modulo is an abelian group.
c) K_4= {e,a,b,ab|a^2=e,b^2=e, ab=ba} is an abelian group.

Theorem: If every element of a group G has self inverse then G is abelian.

Proof: Let G be a group and every element of G has a self inverse.

Now let a € G then a^{-1}=a …(1)

And b € G then b^{-1}=b …(2)

a € G and b € G and G is a group then

a*b € G

⇨ $(ab)^{-1}$=ab

⇨ $b^{-1}a^{-1}$=ab

⇨ ba=ab (using 1 and 2)

⇨ G is an abelian group.

Cyclic Group:

A group G is said to be cyclic group if there exist an element a€G such that every element of G is generated by a. The element a is called generator of G. It is denoted by <a> i.e.

G=<a>={a^n|n€Z} and

G=<a>={na| n€Z} in case of additive group.

For example:

a) Z*={1,-1} is a cyclic group generated by -1.
b) Z_2={0,1} a group over addition modulo 2 is cyclic group generated by 1.
c) Group of integers is a cyclic group generated by 1 and -1.

Theorem: If G is a cyclic group then G is abelian but converse need not be true.

Proof: If G is a cyclic group then there exist a €G such that

G=<a>

Let x, y € G then $x=a^r$

$y=a^s$, where r, s are integers

such that $xy = (a^r)(a^s)$

$xy = a^{r+s}$

$xy = a^{s+r}$

$xy = a^s a^r$

xy = yx

⇨ G is abelian.

Converse: Let G = K_4= {e,a,b,ab|a^2=e,b^2=e, ab=ba} which is an abelian group but not cyclic because order of every element of K_4 is not greater than 2 but o(K_4)=4.

NOTE: If G is non abelian then G is not cyclic.

Subgroup:

Let H be a non empty subset of a group G then H is said to be subgroup of G if H is itself a group under the same binary operation of G.

For example:

a) (Z,+) is subgroup of (Q,+).
b) (R,+) is subgroup of (C,+).

Theorem: H is subgroup of G if and only if ab^{-1} € H for all a,b € H.

Proof: Let H be a subgroup of G

then a € H and b € H => b^{-1}€H

Now a € H b^{-1}€H and H is a subgroup of G

=> ab^{-1}€H

Conversly suppose ab^{-1}€H for all a,b € H.

Put a=b then bb^{-1}€H => e € H

then H has identity element e.

Put a=e then eb^{-1}€H for all b € H.

=> b^{-1} € H for all b € H

Hence inverse of all elements of H exists.

Let a € H and b € H => b^{-1}€H

Such that $a(b^{-1})^{-1}$€H for all a,b € H

=> ab € H for all a, b € H

=> H is a group.

Hence H is a subgroup of G.

Reference:

1. Joseph A. Gallian: Contemporary Abstract Algebra

2. Surjit Singh and Quazi Zameeruddin : Modern Algebra
3. P.B. Bhattacharya S.R. Jain and S.R. Nagpal : Basic Abstract Algebra
4. I.D. Macdonald: Theory of groups
5. I.N. Herstein: Topics in Algebra
6. W.R. Scott:Group Theory