An Introduction to Group

(For B.A/B.Sc, Part –I, Hons. And Subsidiary Coursesof Mathematics)

Dr. Binay Kumar

Department of mathematics, Magadh Mahila College

Patna University

Introduction to Group theory

Defination1.1: A non empty set *G* is said to be group if in *G* there defined a operation '*' such that:

(1) For all *a, b* in *G*, the result of the operation, $a * b$, is also in *G*. **[Closure law]**

(2) For all *a, b* and *c* in *G*, then $(a * b) * c = a * (b * c)$. **[Associative Law]**

(3)There exists an element *e* in *G* such that, for every element *a* in *G*, the equation $e * a = a * e = a$ holds. **[Existence of Identity element]**

(4) For each *a* in *G*, there exists an element *b* in *G*, commonly denoted a^{-1} (or $-a$, if the operation is denoted "+"), such that $a * b = b * a = e$, where e is the identity element. Here b is called inverse of *a* and denoted as $a^{-1}=b$. **[Existence of Inverse element]**

Remarks: (i) **A** group <G,*> is called **Abelian** group or **Commutative** if it satisfy the condition a*b=b*a for all element in *G*.

(ii) Generally, the binary composition is denoted by '.'(dot). This binary composition '.' is also called product or multiplication (although it may have nothing to do with the usual multiplication).

(iii) If the set G is finite element, then <G,*> is called finite group other wise, it is called infinite group.

(iv) The closure property need not to be state separately if we used 'non empty set *G* together with binary operation' instead of only 'operation'.

(v) Since $a^{-1} * a = e = a * a^{-1}$, which means $(a^{-1})^{-1} = a$.

Defination1.2: If in a group <G,*> the underlying set *G* consists of finite numbers of distinct element, then the group is called a finite group otherwise infinite group.

The number of distinct element in the group is defined as **order** of the group. It is denoted by o(G) or |G|.

Eample.1 Show that the set of all integers …**-4, -3, -2, -1, 0, 1, 2, 3, 4,** … is an infinite Abelian group with respect to the operation of addition of integers.

Solution: Let us test all the group axioms for an Abelian group.

(1) Closure Axiom: We know that the sum of any two integers is also an integer, i.e., for all a,b∈Z, a+b∈ Z. Thus Z is closed with respect to addition.

(2) Associative Axiom: Since the addition of integers is associative, the associative axiom is satisfied, i.e., for $a,b,c \in Z$ such that $a+(b+c)=(a+b)+c$

(3) Existence of Identity: We know that 0 is the additive identity and $0 \in Z$,

i.e., $0+a=a=0+a \ \forall a \in Z$

Hence, additive identity exists.

(4) Existence of Inverse: If $a \in Z$ then $-a \in Z$. Also, $(-a)+a=0=a+(-a)$

Thus, every integer possesses additive inverse. Therefore Z is a group with respect to addition.

Since the addition of integers is a commutative operation, therefore $a+b=b+a \ \forall a,b \in Z$

Hence (Z,+) is an Abelian group. Also, Z contains an infinite number of elements.

Therefore (Z,+) is an Abelian group of infinite order.

Example 2: The set integer I, w.r.t. multiplication does not form group, although it satisfy the condition of closure, associativity and identity conditions.

Example 3: The set of natural number N, does not form group w.r.t addition as it does not possesses identity and inverse of element. although it satisfy the conditions of closure and associativity.

Example 4: Show that set of rational number Q-{0} form group w.r.t. operation usual multiplication.

Solution: Let the given set be denoted by Qo. Then by group axioms, we have

(1) We know that the product of two non-zero rational numbers is also a non-zero rational number. Therefore Qo is closed with respect to multiplication. Hence, the closure axiom is satisfied.

(2) We know for rational numbers:

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a,b,c \in Qo$. Hence, the associative axiom is satisfied.

(3) Since 1 the multiplicative identity is a rational number, hence the identity axiom is satisfied.

(4) If $a \in Qo$, then obviously, $1/a \in Qo$. Also $(1/a) \cdot a = 1 = a \cdot (1/a)$

so that 1/a is the multiplicative inverse of a. Thus the inverse axiom is also satisfied. Hence Qo is a group with respect to multiplication.

Example 5: Show that C, the set of all non-zero complex numbers is a multiplicative group.

Solution: Let $C=\{z:z=x+iy, x,y \in R\}$. Here R is the set of all real numbers and $i = \sqrt{-1}$.

(1) Closure Axiom: If $a+ib \in C$ and $c+id \in C$, then by the definition of multiplication of complex numbers

$$(a+ib)(c+id)=(ac-bd)+i(ad+bc) \in C$$

Since $ac-bd, ad+bc \in R$ for $a,b,c,d \in R$. Therefore,C is closed under multiplication.

(2) Associative Axiom:

$$(a+ib)\{(c+id)(e+if)\}=(ace-adf-bcf-bde)+i(acf+ade+bce-bdf)$$

$$=\{(a+ib)(c+id)\}(e+if) \text{ for } a,b,c,d \in R.$$

(3) Identity Axiom: $e=1(=1+i0)$ is the identity in C.

(4) Inverse Axiom: Let $(a+ib)(\neq 0) \in C$, then

$$(a+ib)^{-1}=1/(a+ib)=a-ib/(a^2+b^2)$$

$$(a+ib)^{-1}=a/(a^2+b^2)+i(b/(a^2+b^2)$$

$$=m+in \in C$$

where $m= a/(a^2+b^2)$ and $n= b/(a^2+b^2)$. Hence C is a multiplicative group.

Example 6: Let the set $G=\{\pm 1, \pm i, \pm j, \pm k\}$. Define product on G by usual multiplication together with $i^2=j^2=k^2=-1$, $ij=-ji=k$, $jk=-kj=i$, $ki=-ik=j$. This define a non-Abelian group of order 8. It is denoted by Q_8, called **Quaternion Group.**

Defination 1.3: Addition (Multiplication) Modulo

Now here we are going to discuss a new type of addition(multiplication), which is known as "addition(multiplication) modulo m" and written in the form $a +_m b (a \times_m b)$ where a and b belong to an integer and m is any fixed positive integer. By definition we have

$$a +_m b=r, \text{ for } 0 \leqslant r<m \quad (a \times_m b=r),$$

Here r is the least non-negative remainder when a+b (a.b), i.e., the ordinary addition (multiplication) of a and b is divided by m.

For example, $5+_6 3=2$, since $5+3=8=1(6)+2$, i.e., it is the least non-negative reminder when 5+3 is divisible by 6 and $5\times_6 3=3$, since $5\times3=15=2(6)+3$

Thus to find $a+_m b (a\times_m b)$, we add(multiply) a and b in the ordinary way and then from the sum(multiplication), we remove integral multiples of m in such a way that the remainder r is either 0 or a positive integer less than m.

Ex: Let $G=\{0,1,2,3,4,5)$ be a set. Show that under addition modulo 6 G form agroup

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

1. From table it is clear that *G* is closed under closure property as resulting element again element of set *G.*
2. Clearly associative law hold in *G*
3. From second row and second column it is clear that 0 is the identity element of the group.
4. From table it is clear that inverse of every element of *G* exist in *G.* That is $1^{-1}=5$, $2^{-1}=4$, i $3^{-1}=3, 4^{-1}=2$, $5^{-1}=1$.
5. Since all the elements are symmetrical about principle diagonal, *G* is abelian.
   Hence *G* is abelian group .

Ex: Let $G=\{1,2,3,4,5,6\}$ be a set. Show that under multiplication modulo 7 *G* form a group.

$\times_7$	**1**	**2**	**3**	**4**	**5**	**6**
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

1. From table it is clear that *G* is closed under closure property as resulting element again element of set *G.*
2. Clearly associative law hold in *G*
3. From second row and second column it is clear that 1 is the identity element of the group.
4. From table it is clear that inverse of every element of *G* exist in *G.* Since all the elements are symmetrical about principle diagonal, *G* is abelian.
   Hence *G* is abelian group .

Example 8: Prove that the set G of all *n*th roots of unity, where n is fixed positive integer form an abelian group under usual multiplication of complex numbers.

Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ and G be the set of all n-th roots of unity. Mathematically,

$$G = \left\{ w_k = \exp\left(i\frac{2k\pi}{n}\right) \middle| \, k \in \mathbb{Z}_n \right\}.$$

Closure: Take $k,\ l \in \mathbb{Z}_n$.

$$\begin{aligned} w_k w_l &= \exp\left(i\frac{2k\pi}{n}\right)\exp\left(i\frac{2l\pi}{n}\right) \\ &= \exp\left(i\frac{2(k+l)\pi}{n}\right) \end{aligned}$$

By division algorithm, $k + l = qn + r$ with $q \in \mathbb{Z}$ and $0 \leq r < n$.

$$\begin{aligned} w_k w_l &= \exp\left(i\frac{2(qn+r)\pi}{n}\right) \\ &= \exp(2q\pi i)\exp\left(i\frac{2r\pi}{n}\right) \\ &= w_r \\ &= w_{(k+l) \bmod n} \end{aligned}$$

Associativity: Associativity follows from $\mathbb{C}$ since $G \subset \mathbb{C}$. Or take $k,\ l,\ m \in \mathbb{Z}_n$.

$$\begin{aligned} w_k(w_l w_m) &= w_k w_{(l+m) \bmod n} \\ &= w_{(k+(l+m) \bmod n) \bmod n} \\ &= w_{((k+l)+m) \bmod n} \\ &= w_{((k+l) \bmod n + m) \bmod n} \\ &= w_{(k+l) \bmod n} w_m \\ &= (w_k w_l) w_m \end{aligned}$$

Identity: Take $k \in \mathbb{Z}_n$.

$$\begin{aligned} w_k w_0 &= w_{(k+0) \bmod n} \\ &= w_{k \bmod n} \\ &= w_k \end{aligned}$$

Similarly, for all $k \in \mathbb{Z}_n$, $w_0 w_k = w_k$. Therefore, $w_0 = 1$ is the identity element.

Inverse: If $k = 0$, then

$$w_0 w_0 = 1.$$

Now consider $k \in \mathbb{Z}_n$ with $k \neq 0$. Since $1 \leq k < n$, then $n - k \in \mathbb{Z}_n$, and

$$\begin{aligned} w_k w_{n-k} &= w_{n \bmod n} \\ &= w_0 \\ &= 1 \end{aligned}$$

Therefore, the inverse of w_k is w_{n-k}.

Moreover, since for all $k, l \in \mathbb{Z}_n$,

$$w_k w_l = w_l w_k$$

this group is commutative or, abelian.

Further, since for all $k \in \mathbb{Z}_n$, $w_k = w_1^k$,

$$G = \langle w_1 \rangle,$$

in other words, G is cyclic.