Unit - 4

Group Theory

1. **Binary Operations** :- Let G be a non-empty set and $a, b \in G$. Then an operation $*$ on G is said to be binary if $a*b \in G$ $\forall a, b \in G$
i.e. if $*: G \times G \to G$ then $*$ is binary. The propert is said to be the closure property.
For example, addition $(+)$ and multiplication $(\times)$ are binary operations on the set of natural no. $\mathbb{N}$.

2. **Algebric Structure** :- A non-empty set together with one or more than one binary operation and some properties is called an algebric structure.

Some of the Properties are as follows

1. **Associative law** :- A binary operation $*$ on a set S is said be associative iff $\forall a, b, c \in S$

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

2) **Commutative law** :- A binary operation $*$ on the set S is said to be commutative iff $\forall a, b \in S$

$$a*b = b*a$$

3) **Identity element** :- An element e in a set S is called an identity element with respect to the binary operatio $*$ if for any element $a \in S$ $\quad a*e = e*a = a$

Unit-4

Group Theory

1. **Binary Operations** :- Let G be a non-empty set and $a, b \in G$. Then an operation $*$ on G is said to be binary if $a*b \in G$ $\forall a, b \in G$
i.e. if $* : G \times G \to G$ then $*$ is binary. The property is said to be the closure property.
For example, addition (+) and multiplication (x) are binary operations on the set of natural no. $\mathbb{N}$.

2. **Algebric Structure** :- A non-empty set together with one or more than one binary operation and some properties is called an algebric structure.

Some of the Properties are as follows

1. **Associative law**:- A binary operation $*$ on a set S is said be associative iff $\forall a, b, c \in S$

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

2) **Commutative law**:- A binary operation $*$ on the set S is said to be commutative iff $\forall a, b \in S$

$$a*b = b*a$$

3) **Identity element** :- An element e in a set S is called an identity element with respect to the binary operation $*$ if for any element $a \in S$ $a*e = e*a = a$

4) Inverse element :- An element b is said to be the inverse of an element a if

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

Q.1 What is the identity element $e \in \mathbb{Z}$ with respect to the binary operation $*$ given by

$$a * b = a + b - 2, \text{ for all } a, b \in \mathbb{Z}$$

Soln :- The identity element is the element e for which $a * e = e \quad \forall a \in \mathbb{Z}$

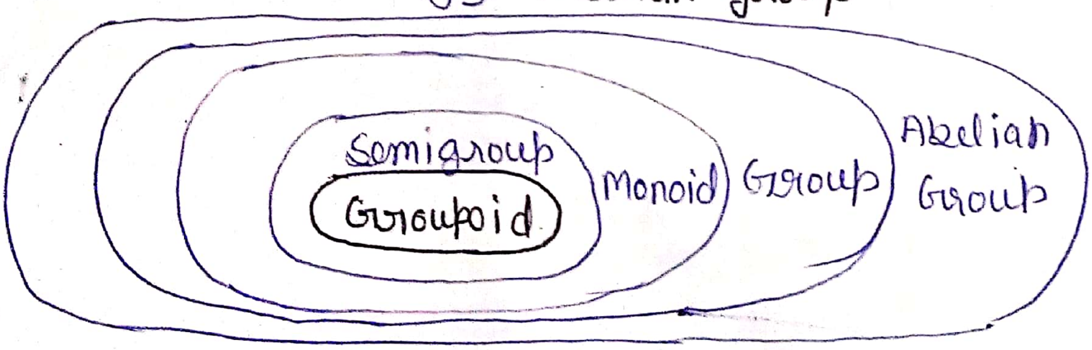
Here $a * e = a + e - 2$

$\Rightarrow a + e - 2 = a \Rightarrow e = 2.$

Hence the identity element is 2.

Algebric Structures

1) Closure Property } Groupoid
2) Associative property } Semigroup
3) Identity element } Monoid
4) Inverse element } Group
5) Commutative property } Abelian group



Q.2 Let Q denotes the set of rational no. Consider the operation $*$ given by $a*b = a+b+ab$, for $a, b \in Q$. Show that $(Q,*)$ is an abelian Monoid. Also find all invertible elements of Q with respect to $*$.

Solu^n:-

1) Closure property :- Since for every $a, b \in Q$, $a+b+ab \in Q$ therefore Q is closed with respect to $*$.

2) Associative property :- For $a, b, c \in Q$

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

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

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

3) Commutative :- for $a, b \in Q$.

$$a+b+ab = b+a+ba \Rightarrow a*b = b*a$$

4) Identity element; for identity element e

$$a*e = a. \quad \forall a \in Q$$

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

$$\Rightarrow e = 0$$

Therefor '0' is the identity element of $(Q,*)$

5) Inverse element :- Let b is the inverse of a

$\Rightarrow$ $a*b = e \Rightarrow a+b+ab = 0 \Rightarrow a+b(1+a) = 0$

$\Rightarrow$ $b = \left(\frac{-a}{1+a}\right)$ which exist iff $a \neq -1$.

Q3 On the set $M = Q \times Q$ consider the operation $*$ given by $(a,b)*(x,y) = (ax, ay+b)$, for $a,b,x,y \in Q$, Show that $(M,*)$ is a non-Abelian monoid. Also find all its invertable elements.

Soln:-

1) Closure property :- If (a,b) & $(x,y) \in M \Rightarrow (ax, ay+b) \in M$

Hence M is closed

2) Associative property :- Let $(a,b), (c,d), (p,q) \in M$

$$\Rightarrow (a,b)*((c,d)*(p,q)) = (a,b)*(cp, cq+d)$$
$$= (acp, a(cq+d)+b)$$
$$= (acp, acq+ad+b)$$

& $$((a,b)*(c,d))*(p,q) = (ac, ad+b)*(p,q)$$
$$= (acp, acq+ad+b)$$

$$\Rightarrow (a,b)*((c,d)*(p,q)) = ((a,b)*(c,d))*(p,q)$$

3) Identity property :- Let (e_1, e_2) be an identity of M s.t. $(a,b)*(e_1,e_2) = (a,b)$ $\forall$ $(a,b) \in M$

$$\Rightarrow (ae_1, ae_2+b) = (a,b) \Rightarrow e_1 = 1 \text{ \& } e_2 = 0$$

$\Rightarrow$ $(1,0)$ is the identity

4) Inverse element :- let (a^{-1}, b^{-1}) is the inverse of $(a,b) \in M$ $\Rightarrow$ $(a,b)*(a^{-1},b^{-1}) = (aa^{-1}, ab^{-1}+b)$
$$= (1, 0)$$

$$\Rightarrow aa^{-1} = 1 \Rightarrow a^{-1} = \frac{1}{a} \quad \& \quad ab^{-1}+b = 0 \Rightarrow b^{-1} = \frac{-b}{a}$$

Thus $\left(\frac{1}{a}, \frac{-b}{a}\right)$ is the inverse of (a,b) if $a \neq 0$

Q.4 Define Group

Q.5 Let $G = \{0,1,2,3,4,5\}$, and $+_6$ denotes the addition modulo 6. Show that $(G, +_6)$ is a group.

Soln:- The composition table as follows.

$+_6$	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) Closure property :- Here all the entries in the table are element of G, thus $(G, +_6)$ is closed.

2) Associative :- The composition is associative

ex: $1 +_6 (2 +_6 3) = (1 +_6 2) +_6 3$

3) Identity element :- Here the row headed by the element '0' coincides with the top row. Thus '0' is the identity element.

4) Inverse :- The identity element occured in every row and column only once hence inverse of every element exists. ~~The~~

The inverse of 0, 1, 2, 3, 4, 5 are 0, 5, 4, 3, 2, 1 respectiv

Q.6 Show that the set $\{1,2,3,4,5\}$ is not a group with respect to $+_6$ & $\times_6$.

Q.7. Show that the set $(Q^+, *)$ is an abelian group where $a * b = \frac{ab}{3} \quad \forall a, b \in Q^+$

Q.8. Show that $\{G, *\}$ is an abelian group where $G = \{1, -1, i, -i\}$ and $*$ is the usual multiplication.

Q9 Verify that $(\mathbb{Z}, *)$ is an abelian group s.t. $x*y = x+y+1$, for $x, y \in \mathbb{Z}$

Q10 Prove that the set $A = \{1, \omega, \omega^2\}$ is an abelian group with respect to usual multiplication

Q11. <u>Cyclic group</u> :-

A group is called a cyclic group if, for some $a \in G$, every element of G is of the form a^n, where n is an integer i.e. $G = \{a^n : n \in \mathbb{Z}\}$.
The element a is the generator of G. If G is a cyclic group generated by a, it is denoted by $G = \langle a \rangle$. The elements of G are in the form

$$\ldots a^{-2}, a^{-1}, a^0, 0, a, a^2, a^3 \ldots$$

Note :- There may be more than one generator. Every cyclic group has at least two generators, generator and its inverse.

Permutation Group :- Let A be a finite set. Then ~~the~~ a func^n. $f : A \to A$ is said to be a permutation of A if f is one-one and onto. The no. of distinct elements in the finite set A is called the degree of the permutation.

A permutation can be written as $\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ f(a_1) & f(a_2) & & f(a_n) \end{pmatrix}$.

There are $n!$ permutations can be formed from n no. of elements and the set of all these permutations is denoted by S_n and called as Symmetric group or permutation group.

For example, if $A = \{1,2,3\}$, Then

$$S_3 = \{p_0, p_1, p_2, p_3, p_4, p_5\}$$

where $p_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ & $p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

The multiplication table for the compositions of permutations in S_3 is as given below:

	p_0	p_1	p_2	p_3	p_4	p_5
p_0	p_0	p_1	p_2	p_3	p_4	p_5
p_1	p_1	p_2	p_0	p_5	p_3	p_4
p_2	p_2	p_0	p_1	p_4	p_5	p_3
p_3	p_3	p_4	p_5	p_0	p_1	p_2
p_4	p_4	p_5	p_3	p_2	p_0	p_1
p_5	p_5	p_3	p_4	p_1	p_2	p_0

1) The table shows that S_3 is closed and associative.

2). p_0 is the identity element

3) Inverse of $p_0, p_1, p_2, p_3, p_4, p_5$ are $p_0, p_2, p_1, p_3, p_4, p_5$ respectively

4) Here the rows are not same as its respective column hence not commutative.

Scanned with OKEN Scanner

Order of an element

The order of an element g in a group G is the smallest positive integer n s.t. $g^n = e$. denoted by $o(g)$. If no such integer exist then g has infinite order.

Ex:- For $G = \{1, -1, i, -i\}$

order of $1, -1, i, -i$ are $1, 2, 4, 4$ respectively.

Q.11. In a group (G, o), a is an element of order 30. Find the order of a^5

Soln:-

$o(a) = 30 \Rightarrow a^{30} = e \Rightarrow (a^5)^6 = e$.

$\Rightarrow o(a^5) = 6$

Q.12 In a group G for $a, b \in G$, $o(a) = 5$, $b \neq e$ and $aba^{-1} = b^2$ show that $o(b) = 31$

Soln:-

$$(aba^{-1})^2 = (aba^{-1})(aba^{-1}) = (ab)(a^{-1}a)(ba^{-1})$$
$$= (ab)(ba^{-1})$$
$$= ab^2a^{-1}$$
$$= a(aba^{-1})a^{-1}$$
$$= a^2ba^{-2}$$

$$\Rightarrow (aba^{-1})^4 = (aba^{-1})^2(aba^{-1})^2 = (a^2ba^{-2})(a^2ba^{-2})$$
$$= a^2(aba^{-1})a^{-2}$$
$$= a^3ba^{-3}$$

$$\Rightarrow (aba^{-1})^8 = a^4ba^{-4}$$

$$\& \ (aba^{-1})^{16} = a^5ba^{-5} = ebe^{-1} = b$$

$$\Rightarrow (b^2)^{16} = b \Rightarrow b^{32} = b \Rightarrow b^{31} = e \Rightarrow o(b) = 31$$

Q.13 Let $(G,*)$ be a group, and $a,b \in G$. Prove that (i) $(a^{-1})^{-1} = a$ and (ii) $(a*b)^{-1} = b^{-1}*a^{-1}$

Proof :-

(i) Let e be the identity element for $*$ in G

$\Rightarrow \quad a*a^{-1} = e$, where $a^{-1} \in G$

also $(a^{-1})*(a^{-1})^{-1} = e = a*a^{-1}$

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

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

(ii) Let $a,b \in G \Rightarrow a*b \in G$

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

$\because \; a,b \in G \Rightarrow a^{-1}$ & $b^{-1} \in G$

$\Rightarrow \; (b^{-1}*a^{-1})*(a*b) = b^{-1}*(a^{-1}*a)*b$ (associative)

$= b^{-1}*e*b = e.$ —(2)

from (1) & (2)

$\Rightarrow$

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

$\Rightarrow \; (a*b)^{-1} = b^{-1}*a^{-1}.$ (Right Cancellation)

Q.14 Let G be a group. Justify that $(ab)^2 = a^2b^2$, ~~for~~ $\forall \; a,b \in G$ iff G is an abelian group

Solu^n:- Let $a, b \in G$, Suppose $(ab)^2 = a^2b^2$
To prove that G is abelian, we have to show that $ab = ba$

$\Rightarrow (ab)^2 = a^2b^2 \Rightarrow (ab)(ab) = (aa)(bb)$

$\Rightarrow a(ba)b = a(ab)b$

$\Rightarrow ba = ab$ (Right and left cancellation)

Again, Suppose G is abelian $\Rightarrow ab = ba$.
We have to prove that $(ab)^2 = a^2b^2$

here. $(ab)^2 = (ab)(ab) = a(ba)b$
$= a(ab)b$
$= (aa)(bb)$
$= a^2b^2$

Hence proved

Q.15 Consider the element $\alpha = (13562)$ and $\beta = (1523)(46)$ of the permutation group S_6. Compute the elements $\alpha^{-1}\beta\alpha$ and $\beta^{-1}\alpha\beta$.

Solu^n:-
Here $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix} \Rightarrow \alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 3 & 5 \end{pmatrix}$

& $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix} \Rightarrow \beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 6 & 1 & 4 \end{pmatrix}$

$\Rightarrow \alpha^{-1}\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 3 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 2 & 3 & 1 \end{pmatrix}$

$= (1536)(24)$

& $B^{-1}QB = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 6 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}$ (ii)

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 3 & 1 & 6 \end{pmatrix} = (12435)$ Ans

Q.16 Let S_3 denote the set of permutations of the set $\{1, 2, 3\}$. Show that S_3 is a group with respect to the binary operation composition of funcⁿ.

Q.17 ~~Write~~ Construct ~~multiplication~~ Composite table for the set Z_4 with respect to $+_4$ & $\times_4$. Is $(Z_4, +_4)$ is a group? Show that $(Z/\{0\}, \cdot)$ is not a group.

Soluⁿ:- $Z_4 = \{0, 1, 2, 3\}$ & $Z/\{0\} = \{1, 2, 3\}$

Table 1

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Table 2

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

From table 1 it is noticed that $(Z_4, +_4)$ is closed and associative, Its identity element is '0' and inverse element of 0, 1, 2, 3 are 0, 3, 2, 1 respectively hence $(Z_4, +_4)$ is a group.

$\Rightarrow$ From table 2 it is noticed that $\{Z/\{0\}, \times_4\}$ is not closed as $2, 2 \in Z/\{0\}$

but $2 \times_4 2 = 0 \notin Z_4/\{0\}$

hence it is not a group.

Q. 18 Give an example of a cyclic group of order 4.

Ans. $(Z_4, +_4)$ is a cyclic group of order 4 as every element of Z_4 can be written as the power of 1

$\Rightarrow$

$$1 = 1^1$$
$$2 = 1^2 = 1 +_4 1$$
$$3 = 1^3 = 1 +_4 1 +_4 1$$
$$0 = 1^4 = 1 +_4 1 +_4 1 +_4 1$$

Thus $Z_4 = \{1^4, 1, 1^2, 1^3\}$, 1 is the generator

also $Z_4 = \{3^4, 3^3, 3^2, 3\}$, 3 is the generator

Q 19 Show that every cyclic group is abelian.

Proof:- Let G be a cyclic group and let a be a generator of G so that $G = \langle a \rangle = \{a^n : n \in Z\}$

$\Rightarrow$ if g_1 & g_2 are two elements of G s.t.

$g_1 = a^r$ and $g_2 = a^s$ $(r \,\&\, s \in Z)$

$\Rightarrow g_1 \cdot g_2 = a^r \cdot a^s = a^{r+s} = a^{s+r} = a^s \cdot a^r = g_2 \cdot g_1$

proved

Subgroup

Def^n:- Let $(G, *)$ be a group and H is a subset of G then $(H, *)$ is said to be the subgroup of $(G, *)$ if $(H, *)$ is itself a group.

Ex:- i) The multiplicative group $\{1, -1\}$ is a subgroup of group $\{1, -1, i, -i\}$

ii) The additive group of even integers is a subgroup of the additive group of all integers.

Theorems

Th-1 The identity element of a subgroup is the same as that of the group

Proof:- Let H be the subgroup of the group G and e & e' be the identity element of G & H respectively.

Now if $a \in H \Rightarrow a \in G$ ($\because H \subset G$) $\Rightarrow ae = a$ ($\because e$ is the identity of G)

Again as $a \in H$ & e' is the identity of H $ae' = a$

$\Rightarrow ae = ae' \Rightarrow e = e'$ Hence proved

Th-2:- The inverse of any element of a subgroup is the same as the inverse of the same element of the group.

Proof:- Let $a \in H$ & e is the common identity of H & G

let b is the inverse of a in H $\Rightarrow ab = e$

& c " " " " G $\Rightarrow ac = e$

$\Rightarrow ab = ac \Rightarrow b = c$ Hence proved

Imp.

Th-3 :- The necessary and sufficient condition for a non-empty sub-set H of a group $(G, *)$ to be a subgroup is

$$a * b^{-1} \in H \quad \forall\, a, b \in H$$

where b^{-1} is the inverse of b in G.

Proof:- let H be a sub-group and $a, b \in H$, Since $b \in H \Rightarrow b^{-1} \in H$

Now $a \in H$ & $b^{-1} \in H$ $\Rightarrow ab^{-1} \in H$ (by closure property)

Thus the condition is necessary.

Sufficient condition:- Now assume that $ab^{-1} \in H \;\forall\, a, b \in H$ and

we have to show that H is a subgroup of G.

We have $a, a \in H$ by the condition $a * a^{-1} \in H \Rightarrow e \in H$ where e is the identity element. Hence H contains the identity element.

Again, we have

e & $a \in H$ $\Rightarrow$ $e * a^{-1} \in H$ $\Rightarrow$ $a^{-1} \in H$ $\forall a \in H$

hence the inverse of each element exists in H

Now, If $b \in H \Rightarrow b^{-1} \in H$ (Previous condition)

also if a & $b^{-1} \in H$ $\Rightarrow a * (b^{-1})^{-1} \in H$

$\Rightarrow a * b \in H$ (: Closure property)

Thus H satisfies closure property, contains identity elements and inverse of each element of H also exists in H. H also satisfies associative law as every element of H is the element of group G, which satisfies associative law.

Therefore $(H, *)$ is the subgroup of $(G, *)$

Th-4. The intersection of any two subgroups of a group is the subgroup of the group.

Proof: Let H_1 & H_2 form any two subgroups of $(G, *)$. since identity element $e \in H_1$ & $e \in H_2$

$\Rightarrow$ $H_1 \cap H_2 \neq \phi$

now let $a \in H_1 \cap H_2$ and $b \in H_1 \cap H_2$

$\Rightarrow$ $a, b \in H_1$ & $a, b \in H_2$

$\Rightarrow$ $a * b^{-1} \in H_1$ & $a * b^{-1} \in H_2$ $\Rightarrow$ $a * b^{-1} \in H_1 \cap H_2$

$\Rightarrow$ $H_1 \cap H_2$ is a subgroup

Note :- However the union of two subgroups is not necessarily a subgroup

Q.20. Give an example of a group G, with two subgroups H & K, such that $H \cup K$ is not a subgroup.

Solnⁿ;- Let G be the additive group of Integers

Then $H_1 = \{ \ldots -6, -4, -2, 0, 2, 4, 6 \ldots \}$

and $H_2 = \{ \ldots -12, -9, -6, -3, 0, 3, 6, 9, 12 \ldots \}$

are both subgroup of G.

Now $H_1 \cup H_2 = \{ \ldots -9, -6, -4, -3, -2, 0, 2, 3, 4, 6, 9 \ldots \}$

Here $2 \,\&\, 3 \in H_1 \cup H_2$

but $2+3 = 5 \notin H_1 \cup H_2$

$\Rightarrow H_1 \cup H_2$ is not closed $\Rightarrow H_1 \cup H_2$ is not a subgroup of G.

Cosets

Let H be a subgroup of a group G and let $a \in G$. Then the set $\{a * h : h \in H\}$ is called the left coset generated by a and H, denoted by aH.

similarly $Ha = \{h * a : h \in H\}$ is called the right coset. Both Ha & aH are the subsets of G.

Note: 1) If e is the identity of G, then $e \in H$ and $He = H = He$. Therefore, H itself is a right as well as left coset of H.

2) If a group is ablian then $aH = Ha$
$\Rightarrow$ right coset is equal to the left coset

3) If the operation is addition, then right coset of H generated by a will be
$H+a = \{h+a : h \in H\}$ &

left coset will be $a+H = \{a+h : h \in H\}$

<u>Properties of Cosets</u> : If H is a subgroup of G & $a, b \in G$, Then

1) $a \in aH$
2) $aH = H$ iff $a \in H$
3) $aH = bH$ or $aH \cap bH = \phi$
4) $aH = bH$ iff $a^{-1}b \in H$

Proof :-

1) $aH = \{a*h : h \in H\}$

and $a = a*e$ where $e \in H \Rightarrow a \in aH$
(identity element)

2) Let $aH = H \Rightarrow ae \in H$ {e is the identity in H}
$\Rightarrow a \in H$ (prove)

Conversely, let $a \in H \Rightarrow a^{-1} \in H$ {$\because$ H is a subgroup of G}

$\Rightarrow a^{-1}h \in H \ \forall \ h \in H$ (closure property)

$\Rightarrow a(a^{-1}h) \in aH \ \forall \ h \in H$ " " "

$\Rightarrow h \in aH \ \forall \ h \in H$

$\Rightarrow H \subset aH$

Again if $a \in H$ and $h \in H$ then $ah \in H \ \forall \ h \in H$
$\Rightarrow H \subset aH$

Since $aH \subset H$ & $H \subset aH \Rightarrow aH = H$.

hence proved

(3) Let H be a sub-group of a group G and let aH and bH be two left cosets of H.

Suppose $aH \cap bH \neq \phi$ and $c \in aH \cap bH$

then c can be written as

$c = ah$ and $c = bh'$ s.t $h, h' \in H$

$\Rightarrow ah = bh' \Rightarrow a = (bh')h^{-1} = b(h'h^{-1})$

let $h'' = h'h^{-1} \Rightarrow h'' \in H$ $(\because h', h^{-1} \in H)$

$\Rightarrow$ $a = bh''$ or $aH = bh''H = b(h''H) = bH$

$(\because aH = H$ if $a \in H$, here $h'' \in H \Rightarrow h''H = H)$

Thus either $aH \cap bH = \phi$ or $aH = bH$.

Hence proved

(4) We have

$aH = bH \Rightarrow a^{-1}aH = a^{-1}bH$

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

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

$\Rightarrow a^{-1}b \in H$ (if $aH = bH$)

Conversely, if $a^{-1}b \in H$

then $bH = e(bH) = (aa^{-1})(bH) = a(a^{-1}b)H$

$= a(a^{-1}bH) = aH$

$\Rightarrow bH = aH$

Thus $aH = bH \overset{\text{Hence}}{\Leftrightarrow} a^{-1}b \in H$

Hence proved

Index of a subgroup in a group :-

If H is a subgroup of a group G, the no. of distinct right (left) cosets of H in G is called the index of H in G and is denoted by $[G;H]$ or $i_G(H)$

Q.21 Consider the group $G = (\mathbb{Z},+)$, and subgroup $H = 6\mathbb{Z} = \{\ldots -12,-6,0,6,12\ldots\}$. Find

i) Cosets of H in G

ii) The index $[G:H]$

or

Q.22 Compute the cosets of the subgroup $H = 6\mathbb{Z}$ in the group $G = (\mathbb{Z},+)$. What is the index of H in G.

<u>Solu</u>: (Both questions are same)

$G = \{\ldots -3,-2,-1,0,1,2,3,\ldots\}$

$H = 6\mathbb{Z} = \{\ldots -12,-6,0,6,12,\ldots\}$

Since G is abelian left and right cosets will be same

Here $0 \in G$

$\Rightarrow$

$H+0 = \{\ldots -12,-6,0,6,12\ldots\}$

$H+1 = \{\ldots -11,-5,1,7,13,\ldots\}$

$H+2 = \{\ldots -10,-4,2,8,14,\ldots\}$

$H+3 = \{ \cdots -9, -3, 3, 9, 15, \cdots \}$

$H+4 = \{ \cdots -8, -2, 4, 10, 16, \cdots \}$

$H+5 = \{ \cdots -7, -1, 5, 11, 17, \cdots \}$

$H+6 = \{ \cdots -6, 0, 6, 12, 18, \cdots \}$

Here we observe that $H+0 = H = H+6$

Similarly $H+1 = H+7 = H+13 \cdots$

$H+2 = H+8 \cdots$

Thus $\exists$ six disjoint right Cosets namely $H, H+1, H+2, H+3, H+4, H+5$

$\Rightarrow$ the index $[G:H] = 5$

and $G = H \cup H+1 \cup H+2 \cup H+3 \cup H+4 \cup H+5$

Q.23. Compute all cosets of the subgroup $H = 5\mathbb{Z}$ in the group $(\mathbb{Z}, +)$. What is the index $[G:H]$?

Solⁿ:- Same as above

V. imp.

Lagrange's theorem :-

The order of each sub-group of a finite group G is a divisor of the order of the group G.

Proof :- Let H be any subgroup of order m of a finite group of order n. We consider the left coset $aH = \{ah : h \in H\}$ let $H = \{h_1, h_2 \cdots h_m\}$

$\Rightarrow aH = \{ah_1, ah_2 \cdots ah_m\}$

here all m elements of aH will be distinct

($\because$ if $ah_i = ah_j \Rightarrow h_i = h_j$)

$\Rightarrow$ each ~~all~~ left cosets of H consist of m different elements

Since G is a finite group, no. of distinct left cosets will be finite say K, Hence the total no. of elements in all cosets is km which is equal to the total no. of elements of G

$\Rightarrow \quad n = mk$

$\Rightarrow$ m the order of H is the divisor of n, the order of G.

Proved.

Note: Converse is not true

Q.24 Prove that every group of Prime order is cyclic.

Proof:- let G be a group of order p, where p is a prime

$|G| = p \quad \Rightarrow |G| > 1$

let $g \in G$, $g \neq e$

$\Rightarrow \quad \langle g \rangle \leq G$

$\Rightarrow \quad |\langle g \rangle| > 1$

$\Rightarrow \quad |\langle g \rangle| = p$

$\Rightarrow \quad \langle g \rangle = G$

Hence G is cyclic

Hence proved.

prime
(2, 3, 5, 7 --)

Lagranges th.

G

H

$o(H) \mid o(G)$

if $o(G) = p$

$\Rightarrow o(H) = 1$ or p

Normal Subgroup :-

A Subgroup H of a group G is said to be the normal subgroup of G if $Ha = aH$ $\forall a \in G$.

Note: Every subgroup of an abelian group G is normal

Theorem 1:- A Subgroup H of a group G is normal iff $g^{-1}hg \in H$ for every $h \in H, g \in G$

Proof:- Let H be a normal subgroup of G.

Let $h \in H, g \in G$

Then $Hg = gH$

$\Rightarrow$ $hg \in Hg = gH$

So $hg = gh_1$ for some $h_1 \in H$

$\Rightarrow$ $g^{-1}hg = h_1$ where $h_1 \in H$

$\Rightarrow$ $g^{-1}hg \in H$

Conversely, Let H be such that $g^{-1}hg \in H$ $\forall h \in H$ & $g \in G$
we have to show that $Ha = aH$ $\forall a \in H$

Consider. $a \in G$ & $h \in H$ $\Rightarrow$ $a^{-1}ha \in H$

$\Rightarrow$ $a(a^{-1}ha) \in aH$ $\Rightarrow$ $(aa^{-1})(ha) \in aH$

$\Rightarrow$ $ha \in aH$ $\forall h \in H$

$\Rightarrow$ $Ha \subseteq aH$

let $b = a^{-1}$ $\Rightarrow$ $b^{-1}hb \in H$

but $b^{-1}hb = (a^{-1})^{-1}ha^{-1} = aha^{-1}$ $\Rightarrow$ $aha^{-1} \in H$

so that $(aha^{-1})a \in Ha$ $\Rightarrow$ $ah \in Ha$ $\forall h \in H$

$\Rightarrow$ $aH \subseteq Ha$ $\Rightarrow$ $Ha = aH$ Proved

Q. 25 Prove that the intersection of two normal subgroups of a group G is again a normal subgroup of G

Proof:- ~~Since e/∈H∩K~~ Let H and K are two normal subgroups of group G

let $g \in G \Rightarrow g^{-1} h_1 g \in H \quad \forall\ h_1 \in H$

$\& \quad g^{-1} h_2 g \in K \quad \forall\ h_2 \in K$.

let $h \in H \cap K \Rightarrow g^{-1} h g \in H \ \&$

$g^{-1} h g \in K$

$\Rightarrow g^{-1} h g \in H \cap K \quad \forall\ h \in H \cap K$

Hence. $H \cap K$ is a normal subgroup of G.

Hence Proved

Homomorphism of Groups:-

Def^n:- Let (G, o) and $(G', *)$ be two groups. ~~are called~~ A mapping $f : G \to G'$ is said to be a homomorphism if

$$f(a o b) = f(a) * f(b) \quad \forall\ a, b \in G$$

Isomorphism:- Let (G, o) & $(G', *)$ are two groups and $f : G \to G'$ is a homomorphism. f is said to be an isomorphism if f is 1-1 and onto.

Notes:- 1) Two groups are called isomorphic to each other denoted by $G \cong G'$

2) An isomorphism of a group onto itself called automorphism

3) A homomorphism is called called monomorphism if only 1-1 not onto

4) A homomorphism is called epimorphism if only onto not 1-1.

5) A homomorphism into itself is called endomorphism

Theorem: Let (G, o) and $(G, *)$ be two groups and $f: G \to G'$ be a homomorphism. Then

i) $f(e) = e'$ where e and e' are identity of G & G' respectively

(ii) $f(a^{-1}) = (f(a))^{-1}, \forall a \in G$

Proof: 1) Here $a \in G \Rightarrow f(a) \in G'$

$$\Rightarrow \quad f(a) * e' = f(a)$$
$$= f(aoe)$$
$$= f(a) * f(e)$$
$$= f(a) * f(e)$$
$$\Rightarrow \quad f(a) * e' = f(a) * f(e)$$
$$\Rightarrow \quad e' = f(e)$$ hence proved.

2) let $a \in G \Rightarrow a^{-1} \in G$

$\Rightarrow f(a) \in G'$ & $f(a^{-1}) \in G'$

$\Rightarrow e = a o a^{-1} \Rightarrow e' = f(e) = f(a o a^{-1})$

$= f(a) * f(a^{-1})$

and $e' = f(a) * (f(a))^{-1}$

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

Kernel of Homomorphism

Def^n:- Let $(G, \circ)$ and $(G', *)$ be two groups and $f: G \to G'$ is a homomorphism. Then, the kernel of f denoted by ker f, is a subset of G defined by

$$\ker f = \{a \in G : f(a) = e'\}$$

~~Thus~~ ~~ker~~ f ~~is~~

Rings & Fields

Ring:- An algebric structure $(R, +, \cdot)$ where R is a non-empty set with two binary operation with multiplication and addition defined on R is called a ring if the following conditions are satisfied.

1) $(R, +)$ is an abelian group
2) $(R, \cdot)$ is a semigroup (closed and associative)
3) The operation is distributive

$$a\cdot(b+c) = a\cdot b + a\cdot c \quad \forall\, a, b, c \in R$$

$$\& \quad (b+c)\cdot a = b\cdot a + c\cdot a \quad \forall \quad " \quad "$$

Commutative Ring:- A ring $(R, +, \cdot)$ is said to be commutative if $a\cdot b = b\cdot a \;\; \forall\, a, b \in R$

Ring with unity:- If the ring consist of the identity element w.r.t. multiplication

Ex:-

1) $(\mathbb{Z},+,\cdot)$ is a commutative ring with unity

2) $(2\mathbb{Z},+,\cdot)$ is a Commutative ring without unity

3) $(\mathbb{Z}_n,+,\cdot)$ is a commutative ring with unity

4) $(M_2(\mathbb{Z}),+,\cdot)$ is a non-commutative ring with unity where $M_2(\mathbb{Z})$ is the set of 2×2 matrices with integer elements.

Properties of Ring

1) $a\cdot 0 = 0\cdot a = 0 \quad \forall a\in R$, where 0 is the identity element w.r.t. addition

2) $a\cdot(-b) = (-a)\cdot b = -(a\cdot b) \quad \forall a,b\in R$

3) $(-a)\cdot(-b) = (a\cdot b) \quad \forall a,b\in R$

4) $a\cdot(b-c) = a\cdot b - a\cdot c$
& $(b-c)\cdot a = b\cdot a - c\cdot a \quad \forall a,b,c\in R.$

Ring with zero divisor :-

If a and b are two non-zero elements of a ring R s.t. $ab=0$, then a and b are the divisors of 0. Then the Ring R is said to be a ring with zero divisors.

Ex:-

Q.26 Find the zero divisors & unit element of $(\mathbb{Z}_6, +_6, \times_6)$

Ans :- $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$\times_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

1) Here the row headed by 1 is same as the top row hence 1 is the unit element of $\mathbb{Z}_6$ as every element of $\mathbb{Z}_6$ can be written as $a \times_6 1 = a$

2) Here the product of non-zero product is zero that is $2 \times_6 3 = 0$, $3 \times_6 2 = 0$, $3 \times_6 4 = 0$
$4 \times_6 3 = 0$

Therefor 2, 3 and 4 are the zero divisors of $\mathbb{Z}_6$.

Integral domain :- A ring containing at least two elements is called an integral domain if it is

1) Commutative
2) has unit element.
3) is without zero divisor

for example.

i) $(Z,+,\cdot)$, $(R,+,\cdot)$ are integral domain

ii) $(2Z,+,\cdot)$ is not an integral domain as it doesn't contain unit element

iii) $(M_2(Z),+,\cdot)$ is not an integral domain since it is not commutative

(iv) $(Z_{2n},+,\cdot)$ is not an integral domain as it has zero divisor.

V. Imp.

Field :- A ring containing at least two element is called field if

1) It is commutative
2) It has unity
3) every element of R has a multiplicative inverse.

Ex :- $(Q,+,\cdot)$, $(R,+,\cdot)$, $(C,+,\cdot)$, $(Z_5,+_5,\times_5)$ are fields.