DANTULURI NARAYANA RAJU COLLEGE (AUTONOMOUS)
Bhimavaram, W.G.DIST. A.P.

II.B.Sc

Paper 3 -ABSTRACT ALGEBRA

Department of Mathematics,

D.N.R College(A), Bhimavaram

DANTULURI NARAYANA RAJU COLLEGE (AUTONOMOUS)
(A College with Potential for Excellence)
Bhimavaram, W.G.DIST. A.P.
II B.Sc
Paper: 2B- <u>ABSTRACT ALGEBRA</u>

Unit - 1: Groups

Unit - 2: Sub Groups

Unit - 3: Normal Sub Groups

Unit - 4: Homomorphism

Unit - 5: Permutations and Cyclic Groups

Unit -1: Groups

INTRODUCTION :

Set :
Collection of well – defined objects.

Empty Set :
Having No Elements in the Set.

Non – Empty Set :
Having at least one Element in the Set.

Binary Operation / Closure Law

Let S be a non – empty set . If * : S X S → S is a mapping then * is called binary operation on S . If for all a , b ∈ S → a*b ∈ S

Examples:

1. +,-, · are binary operations on Z

For 1,2 ∈ Z →1+2=3 ∈ Z
→ 1-2=-1 ∈ Z
→ 1·2=2 ∈ Z

2. / is not binary operation on Z

For 1,2 ∈ Z →1/2 ∉ Z

Algebraic Structure :

A non – empty set equipped with one (or) more binary operations is called an Algebraic Structure

Examples :

(Z,+), (Z,-), (Z,·), (Z,+,·) are all algebraic structures and (Z, /) is not an algebraic structure.

NOTE:

If + is a binary operation on S then the algebraic structure can be written as (S, +)

Associative Law :

A binary operation * on S is said to be associative if (a*b)*c = a*(b*c), for all a,b,c ЄS.

Examples :

+, * *satisfies associative property in* Z.

/, - does not *satisfies associative property in* Z

Semi Group :

An Algebraic structure (G,*) is called a Semi Group if it satisfies the Associative Law with * in G.

Identity Element :

Let S be a non – empty set and * be a binary operation on S . If there exist e_1 Є S such that e_1*a=a ,for all a Є S ,then e_1 is called the ***left Identity***of S with respect to the binary operation *.

Let S be a non – empty set and * be a binary operation on S . If there exist e_2 Є S such that a* e_2 =a ,for all a Є S ,then e_2 is called the ***Right Identity***of S with respect to the binary operation *.

Let S be a non – empty set and * be a binary operation on S . If there exist e Є S such that e*a = a*e = a ,for all a Є S ,then e is called the ***Identity Element***of S with respect to the binary operation *.

Additive Identity is zero.

Multiplicative Identity is One.

Examples :

1. In (z,+) the identity is zero.
2. In (R, ·) the identity is one.

Monoid :

A semi Group (G,*) with identity **e** with respect to the binary operation * is called Monoid. **Example :**

1. (Z,+) is a monoid with identity Zero.
2. (N,+) is not a monoid because it has no identity element.

Invertible Element :

Let (S,*)be a semi Group with identity e. An element a **Є S** is said to be invertible .If there exists b Є S such that a*b = b*a = e

Here b is called inverse of a in S.

Examples:

1. $a+(-a) = 0 \rightarrow$ identity
   Here, $-a$ is the Inverse of a.
2. $a\cdot(1/a) = 1 \rightarrow$ identity
   Here, a^{-1} is the Inverse of a.

GROUP :

An Algebraic structure(G,*) is said to be a group , if the following conditions are hold.

(i) **Associative** :

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

(ii) **Existence of Identity** :

$\exists e \in G \ni a*e = e*a = a$ **,** $\forall$ a $\in$G.

(iii) Existence of Inverse :

for each a $\in$G $\exists$ b $\in$G $\ni$ $a*b = b*a = e$.

Examples : (Z ,+) is a Group.

Solution : Given that (Z,+)

Claim : (Z ,+) is a Group.

Clearly , (Z, +) is an Algebraic Structure

so , + is binary operation

(i) Associative :

Let a = 1, b = 2, c = 3

$(a + b) + c = a + (b + c)$

$(1 + 2) + 3 = 1+ (2 + 3)$

$6 = 6$

$\therefore$ Associative Laws holds.

(ii) Existence of Identity :

Let **e** $\in$Z ,**a** $\in$Z

$a*e = e*a = a$

$a + e = a$ …….(i)

$e = a - a$

$e = 0$

substitute, e = 0 in (i)

$a + 0 = a$

$a = a$

$\therefore$ 0 is the identity

(iii) Existence of Inverse :

Let a , b $\in$ Z , e $\in$ Z.

$a + b = e$

$a + b = 0$

$b = -a$

Here, “b” is the inverse of “a”

Let $a = -1$, $b = -(-1) = 1$
Take , $a + b = b + a = e$
then $-1 + 1 = 1-1 = e$
$0 = 0 = e$
∴ Every Element in Z has Inverse .
∴ (Z , +) forms a Group.
(N ,+) is not a Group.
Here Additive Identity is Zero ,
but we know that the set of all Natural numbers are N = {1, 2, 3, …}
Here, the Identity element ‘0’ does not exist .
So, (N ,+) is not a Group.
(N ,·) is not a Group.
Here , Inverse condition fails because N does not contains negative numbers.
So, (N ,·) is not a Group.

AbelianGroup :
A Group (G, *) is said to be Abelian if * is commutative.
i.e., $a*b = b*a \quad \forall\, a, b \in G$.

Finite and Infinite Groups :
If the set G contains a finite number of elements then the group G is called finite Group.
Otherwise, it is known as an Infinite Group.
Problems:
If the set G of all even integers forms an abelian group under addition as the operation.
(or)
If $G =\{2x/ x\in Z\}$, then Show that (G,+) forms an Abelian group.
Solution:
Given that $G = \{2x/ x\in Z\}$
$= \{\ldots,-4,-2,0,2,4,\ldots\}$
Let $a,b,c \in G$
Here, $a = 2\alpha$, $b = 2\beta$, $c = 2\gamma$, where $\alpha, \beta, \gamma \in Z$
Claim :
(G,*) forms an abelian group
(i) Binary Operation / Closure law:
Let $a , b \in G$
Now , $a + b = 2\alpha + 2\beta$
$= 2(\alpha +\beta) \in G$
$= a +b \in G$
Therefore, + is binary operation on G.
(ii) Associative law:
Let $a , b , c \in G$
$(a + b) + c = (2\alpha + 2\beta) + 2\gamma$

$= 2(\alpha + \beta) + 2\gamma$

$= 2[(\alpha + \beta) + \gamma]$

$= 2[\alpha + (\beta + \gamma)]$

$= 2\alpha +[(2\beta+ 2\gamma)]$

$= a +(b + c)$

$(a + b) + c = a +(b + c)$

Therefore, Associative law holds.

(iii) Existence of Identity:

Let a Є G

We know that 0ЄG

Now $a + 0 = 2\alpha + 0$

$= 2\alpha +2(0)$

$= 2(\alpha + 0)$

$= 2\alpha$

$= a$

Therefore, '0' is the identity in 'G'

(iv) Existence of Inverse:

Let a ЄG

$a = 2\alpha$, for some α ЄZ

$- a = -2\alpha$, for some -α ЄZ

→ -a ЄG

Now $a + (-a) = 2\alpha +(-2\alpha)$

$= 2\alpha - 2\alpha$

$= 2(\alpha - \alpha)$

$= 2(0)$

$= 0$

$= e$

∴ '-a' is the inverse element of 'a' in G

∴ Every Element in G has Inverse.

∴ (G, +) is a Group.

AbelianGroup (Commutative Law):

Let a , b Є G

Now , $a + b = 2\alpha + 2\beta$

$= 2(\alpha +\beta)$

$= 2(\beta +\alpha)$

$= 2\beta + 2\alpha$

$= b + a$

∴ (G, +) is an abelian group.

2. Show that the set Q^+ of all positive rational numbers forms an abelian group under the composition defined by o (circle) such that aob **=** $\frac{ab}{3}$∀ **a, b** Є$\mathbf{Q^+}$

Solution: Given that Q^+**=** The set of all positive rational numbers forms an abelian group under the composition defined by **o(circle)**, such that aob = $\frac{ab}{3}$∀ a, b Є Q^+

Claims : (**Q^+, o**) forms an abelian group.

(i) Binary Operation / Closure Law :

Let a, b Є Q^+

aob = $\frac{ab}{3}$ Є Q^+

aob Є Q^+

∴o is binary in Q^+

(ii) Associative law:

Let a , b , c Є Q^+

(ao b) o c = $(\frac{ab}{3})$ o c

= $(\frac{ab}{3})$c/3

= $(\frac{abc}{9})$

ao (b o c) = a o $(\frac{bc}{3})$

= a$(\frac{bc}{3})$/3

= $(\frac{abc}{9})$

(ao b) o c = a o(b o c)

Therefore, Associative law holds.

(iii) Existence of Identity:

Let a Є Q^+

Suppose that a o e = a for some e Є Q^+

$$\frac{ae}{3} = a$$

→ ae – 3e = 0

→ a(e - 3) = 0

→ a ≠ 0 (or) e – 3 = 0

→ e – 3 = 0

→ e = 3 Є Q^+

Now, ao e = a o 3 = $\frac{a3}{3} = a$

ao e = a

∴ e = 3 is the identity in Q^+

(iv) Existence of Inverse:

Let a Є Q^+ , b Є Q^+

Suppose that, a o b = e

$$\frac{ab}{3} = a$$

$$\frac{ab}{3} = 3$$

$$ab = 9$$

$b = \frac{9}{a}$Є Q^+

ao b = a o($\frac{9}{a}$)

= a($\frac{9}{a}$) / 3

= 9/3

= 3

= e

∴ao b = e

∴ Every element in Q^+ has Inverse

Commutative:

Let a, b Є Q^+

Now a o b = $\frac{ab}{3}$

= $\frac{ba}{3}$

= b o a

ao b = b o a

∴ (Q^+, o) forms an abelian group.

Problem:

Show that the set Z forms an abelian group w.r.to the operation * defined by a*b = a+b+2 ∀ a, b Є Z.

Solution : Given that Z = {0, ±1, ±2, ±3, ±4,….}

and a*b = a+b+2

Claim: (Z, *) forms an abelian group.

(i) Binary Operation / Closure Law :

Let a, b ЄZ

a*b = a+b+2 ЄZ

a*b ЄZ

∴ * is binary in

(ii) Associative law:

Let a , b , c Є Z

(a*b)*c = (a+b+2)*c

= a+b+2+c+2

a*(b*c) = a*(b+2+c)

= a+b+2+c+2

∴ (a*b)*c = a*(b*c)

(iii) Existence of Identity:

Let a Є Z

Suppose that a*e = a, for some e Є Z

→ a+e+2 =a

→ a+e+2-a =0

→ e+2 =0

→ e = - 2 Є Z

Now a*e = a*(-2)

= a-2+2

= a

∴a*e = a

∴ e = -2 is the identity in Z.

(iv) Existence of Inverse:

Let a Є Z , b Є Z

Suppose that, a * b = e

a +b+2 = -2

a +b = -2-2

a +b = -4

a* b = a+b+2

= -4+2

= -2

= e

∴ a * b = e

Commutative:

Let a,b Є Z

a* b = a+b+2

= b+a+2

= b * a

∴ a * b = b * a

(Z, *) forms an abelian group.

Problem:

If G = Q – {1} and * is defined as a*b = a + b - ab then show that (G , *) is an abelian group.

Solution:

Given that G = Q – {1} and a*b = a + b – ab.

Let a, b Є Q → ab Є Q , a≠1, b≠1

Claim: (G,*) forms an abelian group.

(i) Binary Operation / Closure Law :

Let a, b ЄG

a*b = a+b-ab ЄQ

a*b ЄQ

Now we have to prove that a*b ≠1

Suppose that a*b = 1

a+b-ab = 1

a+b(1-a) = 1

1(a-1)+b(1-a) = 0

(a-1)(1-b) = 0

a-1 = 0 (or) 1-b = 0

$a = 1$ (or) $b = 1$

which is a contradiction to $a \neq 1$, $b \neq 1$

$\therefore a*b \neq 1 \in G$

$\therefore$ * is binary in G

(ii) Associative law:

Let a , b , c Є G

$(a*b)*c = (a+b-ab)*c$

$= (a+b-ab)+c-(a+b-ab)c$

$= a+ b-ab+c- ac-bc+abc$

$=a+b+c-ab-bc-ca+abc$

$a*(b*c) =a*(b+c-bc)$

$= a+(b+c-bc) - a (b+c-bc)$

$= a+ b +c-ab - ac-bc+abc$

$=a+b+c-ab-bc-ca+abc$

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

(iii) Existence of Identity:

Let a Є G

Suppose that $a*e = a$

$a + e - ae = a$

$e - ae = 0$

$e(1 - a) = 0$

$e = 0$ (or) $1-a = 0$

$\therefore e = 0 \in G$

Now $a*e = a * 0$

$= a+0-a(0)$

$= a$

$\therefore a*e = a$

$\therefore$ $e = 0$ is the identity in G.

(iv) Existence of Inverse:

Let a Є G

Suppose that $a*b = 0$

$\rightarrow$ $a+b-ab = 0$

$\rightarrow$ $a+b(1-a) = 0$

$\rightarrow$ $b(1-a) = -a$

$\rightarrow$ $b = \frac{-a}{1-a}$

$\rightarrow$ $b = \frac{a}{-(a-1)}$

$\rightarrow$ $b = \frac{a}{(a-1)}$

Now, $a*b = a*\left(\frac{a}{(a-1)}\right)$

$= a + \frac{a}{(a-1)} - a(\frac{a}{(a-1)})$

$= \frac{a(a-1)+a-a2}{a-1}$

$= \frac{0}{a-1}$

$= 0$

∴a*b = e

∴ Every Element in G has Inverse.

Commutative:

Let a,b Є G

a* b = a+b-ab

= b+a-ba

= b * a

∴ a * b = b * a

(G, *) forms an abelian group.

Problem: Show that the set G of rational numbers other than one under the composition defined by ⊕ , such thata⊕b = a + b –ab for a,bЄ G. forms an abelian group and hence show that x = 3/2, is a solution of 4⊕5⊕x = 7

Solution: Given that G = Q – {1} and a⊕b = a + b – ab, for a, b, Є G .

Let a, b, c Є G

→ a, b, c Є Q ,

but a ≠ 1, b ≠ 1, c ≠ 1

Claim: (G, ⊕) forms an abelian group.

(i) Binary Operation / Closure Law :

Let a, b ЄG

a⊕b = a+b-ab ЄQ

a⊕b ЄQ

Now we have to prove that a⊕b ≠1

Suppose that a⊕b = 1

a+b-ab = 1

a+b(1-a) = 1

1(a-1)+b(1-a) = 0

(a-1)(1-b) = 0

a-1 = 0 (or) 1-b = 0

a = 1 (or) b = 1

which is a contradiction to a≠1, b≠1

∴a⊕b ≠1 ЄG

∴ ⊕ is binary in G

(ii) Associative law:

Let a , b , c Є G

(a⊕b) ⊕c = (a+b-ab) ⊕c

= (a+b-ab)+c-(a+b-ab)c

= a+ b-ab+c- ac-bc+abc

$=a+b+c-ab-bc-ca+abc$

$a\oplus(b\oplus c) = a\oplus(b+c-bc)$

$= a+(b+c-bc) - a(b+c-bc)$

$= a+b+c-ab-ac-bc+abc$

$=a+b+c-ab-bc-ca+abc$

$\therefore \quad (a\oplus b)\oplus c = a\oplus(b\oplus c)$

(iii) Existence of Identity:

Let $a \in G$

$\rightarrow a \neq 1$

Suppose that $a\oplus e = a$

$a + e - ae = a$

$e - ae = 0$

$e(1 - a) = 0$

$e = 0$ (or) $1-a = 0$

$\therefore e = 0 \in G$

Now $a\oplus e = a \oplus 0$

$= a+0-a(0)$

$= a$

$\therefore a*e = a$

$\therefore \quad e = 0$ is the identity in G.

(iv) Existence of Inverse:

Let $a \in G$

Suppose that $a\oplus b = 0$, for some $b \in G$

$\rightarrow \quad a+b-ab = 0$

$\rightarrow \quad a+b(1-a) = 0$

$\rightarrow \quad b(1-a) = -a$

$\rightarrow \quad b = \frac{-a}{1-a}$

$\rightarrow \quad b = \frac{a}{-(a-1)}$

$\rightarrow \quad b = \frac{a}{(a-1)}$

Now, $a\oplus b = a\oplus\left(\frac{a}{(a-1)}\right)$

$= a + \frac{a}{(a-1)} - a\left(\frac{a}{(a-1)}\right)$

$= \frac{a(a-1)+a-a2}{a-1}$

$= \frac{0}{a-1}$

$= 0$

$\therefore a\oplus b = e$

$\therefore$ Every Element in G has Inverse.

Commutative:

Let $a,b \in G$

$a \oplus b = a+b-ab$

$= b+a-ba$

$= b \oplus a$

$\therefore \quad a \oplus b = b \oplus a$

$(G, \oplus)$ forms an abelian group.

Now, $(4 \oplus 5) \oplus x = 7$

$(4 \oplus 5-4(5)) \oplus x=7$

$(9-20) \oplus x=7$

$-11 \oplus x = 7$

$-11 + x - (-11x) = 7$

$x + 11x = 7+11$

$12x = 18$

$x = 18/12$

$x = 3/2$

THEOREM : In a group the identity element is unique .

PROOF: Let e_1, e_2 be two identities ina group $(G,\cdot)$

CLAIM : $e_1=e_2$

Since e_1 be the identity and $e_2 \in G$

$e_1.e_2 = e_2.e_1 = e_2$---(1)

since e_2 be the identity and $e_1 \in G$

$e_2.e_1 = e_1.e_2 = e_1$ -------(2)

from 1&2

$e_1=e_2$

hence in a group , the identity element is unique .

THEOREM: In a group the inverse of any element is unique.

PROOF : Let $(G,\cdot)$ be a group and `e" be the identity in G , $a \in G$

Let b,c are two inverses of `a"

$a.b=b.a=e$ --- (1)

since c is the inverse of `a"

$a.c=c.a=e$----(2)

now $b=b.e$

$=b(a.c)$

$=(ba)c$

$= e.c$

$= c$

Therefore b=c

Therefore In a group ,the inverse of each element is unique

CANCELLATION LAWS :

Let a,b ,c∈G and a≠0 then left cancellation law (LCL):

Ab=bc=> b=c
RIGHT CANCELLATION LAW (RCL):
ba=ca=> b=c

THEOREM :
Cancellation laws hold in a group in a group G .
PROOF : Let a,b,c∈G and a≠0
Let `e" be the identity in G
L.C.L: Now ab=ac
$a^{-1}(ab)= a^{-1}(ac)$
$(a^{-1} a)b=(a^{-1}a)c$
Eb=ec
b=c
R.C.L: Now consider ba =ca
$(ba) a^{-1}=((a))a^{-1}$
$B(a a^{-1})=c(a a^{-1})$
b=c
therefore hence cancelation laws in group G

THEOREM : IN a group G and a,b∈G then $(ab)^{-1}=b^{-1} a^{-1}$
PROOF : Let a,b∈G and `e" be the identity in G
CLAIM : $(ab)^{-1}=b^{-1} a^{-1}$
$(1/ab) =b^{-1} a^{-1}$
$1=(a.b) (b^{-1} a^{-1})$
Now consider $(ab) =(b^{-1} a^{-1})$
$=(ab b^{-1}).a^{-1}$
$= a.e.a^{-1}$ (therefore e=1)
$= a.a^{-1}$
=1
Now consider $(b^{-1} a^{-1}) (a.b) =(b^{-1} a^{-1} a).b$
$=b^{-1} .e.b$ (e=1)
$= b^{-1}.b$
=1
Therefore $(ab)^{-1} =b^{-1} a^{-1}$

Problem
Show that a group G is an abelian (if and only if) $(ab)^2 = a^2b^2 \forall$ a,b∈G
Soln: given that G be a group
Suppose that $(ab)^2=a^2b^2 \forall$ a,b∈G
Claim: G Isabelian
That is ab=ba
$(ab)^2= a^2.b^2$
Consider (ab) (ab)=(a.a) (b.b) a(bc)=(ab)c

$(ab)a)b=(a.a)b)b$
$A(ba)b=a(ab)b$
$Ba=ab$
Therefore G is abelian
Conversely suppose that G is abelian ,that is ab=ba

CLAIM: $(ab)^2= a^2.b^2 \forall$ a,b∈G
Consider $(ab)^2=(a b) (ab)$
$= a(ba)b$
$= a(ab)b$
$= (a.a) (b.b)$
$= a^2.b^2$
$(ab)^2= a^2.b^2 \forall$ a,b∈G
Therefore a group G is an abelian $\Leftrightarrow$ $(ab)^2= a^2.b^2 \forall$ a,b∈G

THEOREM : In a group G , for a∈G $a^{-1}=a$ then show that G is abelian
PROOF : given that G be a group , for a∈G $a^{-1}=a$

CLAIM : G is abelian
Let a,b∈G
$a^{-1}=a$, $b^{-1}=b$
sincea,b∈G=> a,b∈G
$(a b)^{-1}= ab$
$b^{-1}.a^{-1}=ab$
b.a =ab
therefore G is abelian

NOTE : A semigroup (G,·) is a group $\Leftrightarrow$ for an a.b∈G the eq ax=b and ya=b have solutions in
G.

THEOREM : A finite semi group (G,·) satisfying cancellation laws is a group
PROOF: Let G ={a_1 , a_2,…a_n} be a finite semigroup with `n" distinct elements and cancellation laws hold in G
CLAIM : (G,·) is a group
Let a ∈G
⇨ a. a_1 , $a.a_2$,…$a.a_n$∈G
⇨ a. a_1 , $a.a_2$,…$a.a_n$ are all distinct elements in G
let b∈G
⇨ b= $a.a_k$ for some unique a_k in G
⇨ $a.a_k$=b
ax=b has unique solution in G similarly , we get ya=b has a unique solution in G
therefore (G,·) is a group

THEOREM : If G is a group such that $(ab)^n=a^nb^n$ for three consecutive positive integers ∀ a,b∈G then show that (G,·) is an abelian group .
Proof : Given that G is a group let a,b∈G
Let m,m+1,m+2 be three consecutive positive integers .
Such that $(ab)^m=a^m.b^m$ ----- (1)
$(ab)^{m+1}=a^{m+1}.b^{m+1}$ ---(2)
$(ab)^{m+2}=a^{m+2}.b^{m+2}$-------(3)
Now consider equation (3)
$(ab)^{m+2}=a^{m+2}.b^{m+2}$
$(ab)^{m+1}.(ab)^1=a^{m+1}.a.b^{m+1}.b$
$a^{m+1}.b^{m+}1.ab=a^m.a.a.b^{m+1}.b$
$a^m. b^{m+1}.a= a^m.a.b^{m+1}$
⇨ $a^m.b^m.b.a =a^m.a.b^m.b$
⇨ $(ab)^m,ba=(ab)^m.a.b$
⇨ ba=ab (by L.C.L)
therefore (G,·) is abelian

Order of an elements of a group :

- Let (G, .) be a group and a∈G then the order of the element a in G is defined as the least positive integer n such that $a^n = e$
- In case such a positive integer does not exist say that the order of `a' is infinite (or) zero
- The order of `a" is defined as o(a) or | a |

NOTE:
$a^{m=e}$, m is a positive integer in G O(a) ≤ M

EXAMPLE: Consider the group G={ 1,-1} under usual multiplication . Find the order of each element in G .
Solution: Given that G={1,-1}
Clearly e=1 is the identify

Let a=1
$(a)^1 =(1)^1=1$
$(a)^2=(1)^2=1$
$(a)^3=(1)^3=1$
.
.
.
Therefore O(1)=1

$a=-1$

$(a)^1=(-1)^1 \neq e$

$(a)^2=(-1)^2=1$

$(a)^3=(-1)^3=-1 \neq e$

$(a)^4= (-1)^2=1$

O (-1)=2

PROBLEM : Find the order of each element in the multiplication group G={ 1,-1,i,-i}.

SOL: Given that G ={ 1,-1,i,-i}

Clearly e=1 is the identity

Let a=1

$(a)^1 =(1)^1=1$

$(a)^2=(1)^2=1$

$(a)^3=(1)^3=1$

.

.

.

Therefore O (1)=1

Let a=-1

$(a)^1 =(-1)^1=-1 \neq e$

$(a)^2=(-1)^2=1$

$(a)^3=(-1)^3=-1 \neq e$

$(a)^4= (-1)^4=1$

.

.

.

O (-1)=2

Let a=i

$(a)^1=(i)^1=i$

$(a)^2 = (i)^2=-1$

$(a)^3 = (i)^3= (i)^2.i=(-1)i=-i$

$(a)^4= (i)^4=(i)^2.(i)^2=(-1) (-1) =1=e$

Therefore O(i)=4

Let a=-i

$(a)^1=(-i)^1=-i$

$(a)^2 = (-1)^2 = (-i) (-i) =i^2=-1$

$(a)^3 = (i)^3= (-i).(-i) (-i)=(-1)-i=i$

$(a)^4= (i)^4=(i)^2.(i)^2=(-1) (-1) =1=e$

Therefore O (-i)=4

PROBLEM: Find the order of each element of the group G { 1, ω, ω ^{2}} under usual multiplications

Solution: Given that G is ({ 1, ω, ω^2} , ·) is a group clearly e =1 is the identity
Let a=1
$(a)^1 = (1)^1 = 1 = e$
$(a)^2 = (1)^2 = 1 = e$
$(a)^3 = (1)^3 = 1 = e$
.
.
.
Therefore 0(1)=1
Let a= ω
$(a)^1 = (\omega)^1 = \omega^1$
$(a)^2 = (\omega)^2 = \omega^2$
$(a)^3 = (\omega)^3 = \omega^3 = 1 = e$
.
.
.
Therefore 0(ω) =3
Let a= ω^2
$(a)^1 = (\omega^2\omega)^1 = \omega^2$
$(a)^2 = (\omega^2)^2 = (\omega^4 = \omega^3.\ \omega = 1.\ \omega = \omega$
$(a)^3 = (\omega^2)^3 = (\omega^3)^2 = (1)^2 = 1 = e$
Therefore $0(\omega^2) = 3$

NOTE :

(1) $+_n$ = addition modulo " n" , n $\in z^+$
$a +_n b$= reminder when a+b is divisible by `n"
example : $2 +_2 3 = 1$, $9 +_3 1 = 1$, $3 +_3 3 = 0$, $8 +_2 6 = 0$, $2 +_4 5 = 3$

(2) X_n= multiplication modulo `n", n $\in z^+$

aX_nb= reminder when a $\times$ b is divisible by `n'

example: $5x_26=0$, $3x_33=0$, $5x_3 3=0$.

(3) In additive notation ,na=c→ O(a) =n .

PROBLEM : Find the order of each element of the group Z_6={0,1,2,3,4,5} under the composition being addition modulo 6(or) $+_6$
Sol: Given that (Z_6, $+_6$) is a group clearly
e=0 is the identity

$1 +_6 1 \ +_6 1 \ +_6 1 \ +_6 1 \ +_6 1 = 0$

⇨ 6(1)=0=>0(1) =6

$2 +_6 2 +_6 2 = 0$

⇨ 3(2)=0 => 0(2) =3

$3 \ +_6 3 = 0$

⇨ 2(3)=0 => 0(3) =2

$4 \ +_6 4 \ +_6 4 = 0$

⇨ 3(4) =0=> 0(4)=3

$5 \ +_6 5 \ +_6 5 \ +_6 5 \ +_6 5 \ +_6 5 = 0$

⇨ 6(5)=0 =>0(5)=6

DEFINITION :

Let a,b, $\in$ z , we say that a/b (a divides b) , if b = a.q for some q $\in$ z

Example : (1) 2|6

Here a=2,b=6

a|b if b=a.q

6=2(3)

(2) 2|7

Here a=2 , b=6

a|b if b=a.q

$7 \neq 2(q)$, q $\in$ z

Division algorithm :

If a,b , $\in$ z and a≠0 then there exist ($\ni$) a unique integer `q" and `r" such that b=a.q +r.

Example : 2|7 =7=2.(3) +1 .

THEOREM : If in a group G ,a $\in$ G such that 0(a) ,then $a^m = e$ ⟺ n/m

PROOF: Given that G is a group and a $\in$ G

Since O(a) =n

Aleast a positive integer such that $a^n = e$……....(1)

Assume that $a^m = e$

Claim :n|m

By division algorithm M=n.q+r…........ (2)

$a^m = a^{n.q} + r$

$= a^{n.q} + a^r => a^{n.q+r}$

$=(a^n)^{q} \cdot a^r$

$^{=}1 \cdot a^r$

$a^m = \cdot a^r$

$a^m = e$, $0 \leq r < n$

if r>0 then O(a) =r

which is a contradiction to O(a) n
r>0
r=0
from (2) ,m =n=>n|m
conversely suppose that n|m
m=n·q for some q ∈
CLAIM: $a^m=e$
$a^n=a^{nq}$
$=(a^n)^q$
$=e^q=e$

WELL ORDERING PRINCIPLE:
Every non empty set of positive integer has a least element (number)

THEOREM : Show that the order of each element in a finite group is finite and is less than are equal to the order of a group

PROOF: Let G be a finite group and a ∈ G
CLAIM : O(a) is finite
Since a, a ∈ G, · is a binary in G
$a^2 \in G$
$a^3 \in G$
.
.
.
By induction , $a^n \in G \ \forall\ n$
$a^1, a^2, \ldots. a^n \in G$
since G is finite
let $a^s=a^r$ for some $r,s \in z^+$, r>s
$a^s.a^{-s}=a^r.a^{-s}$

- ⇨ $a^{s-s}=a^{r-s}$
- ⇨ $a^0= a^{r-s}$
- ⇨ $a^{r-s}=e$, where $r-s \in z^+$
  let s= { $a^m=e/m \in z^+$ }where r-s=m
- ⇨ $s \neq \phi$.
  from Well ordering prinicipe ,s has a least number say `n”
  Therefore n is the least positive integer ∃ $a^n=e$
  0(a) is finite
  0(a) ≤0(G) :
  Suppose that 0(a) ≤ 0(G)
- ⇨ 0(a) . 0(G)
- ⇨ Let O(a)=n then n >O(G)

- ⇨ Since $a^1, a^2 \ldots a^n$ are an distinct
- ⇨ O(G) =n
- ⇨ n>n
- ⇨ which is contradiction $O(a) \leq O(G)$

COMPOSITION TABLE :

(1) Let G ={1,-1,i,-i} the G is a group

·	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	1
I	I	-i	-1	1
-i	-i	i	1	-1

BINARY / CLOSURE LAW:

Since all that entries (elements) of the table are the elements of G

ASSOCIATIVE LAW :

$(a.b).c = a(bc) \ \forall \ a,b,c \in G$

EXISTENCE OF IDENTITY:

Since the top row is indentical with the row corresponding to 1

EXISTENCE OF INVERSE :

Inverse of 1=1

Inverse of -1=-1

Inverse of i=-1

Inverse of –i =i

Therefore G is a group .

(2) Let G ={ $1, \omega, \omega^2$} then G is a group

·	1	Ω	ω^2
1	1	Ω	ω^2
ω	ω	ω^2	1
Ω	ω^2	1	ω

(1) BINARY /CLOSURE LAW:

Since all the existence (elements) of the table are the elements of G

(2) **Associative law** :

$(a,b).c = a.(b.c) \ \forall \ a,b,c \in G$

(3) **EXISTENCE OF IDENTITY :**

Since the top row is identical with the row corresponding to 1

(4)**EXISTENCE OF INVERSE :**

Inverse of 1=1

Inverse of $\omega=\omega^2$

Inverse of $\omega^2=\omega$

Therefore G is a group

1.) Write down the binary operation table for which addition modulo 6($+_6$) of the set z_6 = { 0,1,2,3,4,5}

Given that z_6={ 0,1,2,3,4,5}

(z_6 , $+_6$)

$+_6$	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

2.) Write down the binary operation table for which x_4 (multiplication modulo 4) of the set z_4 ={ 0,1,2,3}.

Given that z_4={ 0,1,2,3}.

(z_4, x_4)

X_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

3.) Write down the binary operation table for which user multiplication table for which user multiplication of the Set a={1,-1}

·	1	-1
1	1	-1
-1	-1	1

UNIT II

Sub Groups

COMPLEX :

Any subset of a group G is called a complex of G .

Example : 2z is of complex of z

NOTE:

(1) If M , N are complex's of a group G then $(M.N)^{-1} = N^{-1}. M^{-1}$
(2) If H is a complex of G then $H^{-1} = \{ h^{-1}/h \in H \}$

SUB GROUP:

Let G be a Group . A non empty Complex H of a Group G is said to be a Subgroup of G if H is a group with respect to the operation `·'(dot) in G .

Ex:

(1) (2z , +) is a sub group of (z, +)

(2)(z ,+) is a sub group of (Q,+)

(3) (Q ,+) is a sub group of (R,+)

NOTE :

(1) If H is a Subgroup of G then the identity element in H and G are same .
Ex:
`0' is the identity in z with respect to the SubGroup of 2Z of Z ,0 is the identity element in 2z.
(2) If H is a SubGroup of a group G and a∈G then the inverse of a in G is same as the inverse of a in H

Ex:

-z is the common inverse of z in both z and 2z

NOTE:

(1) If H is any sub group G then $H^{-1}=H$
(2) H is a sub group of a group G $\Leftrightarrow$ $HH^{-1}=H$
(3) If H is any subgroup of a group G then H.H =H

THEROEM:

If H and K are two subgroups of a group G, then HK is a subgroup of G $\Leftrightarrow$ HK =KH

PROOF:

Given that H and K are two subgroups of a group G

NECESSARY CONDITION:

$\Rightarrow$Suppose that H.K is a subgroups of G

CLAIM: HK=KH

By known theorem $(HK)^{-1}= HK$

$\Rightarrow K^{-1} H^{-1}=HK$

=> KH =HK

=> HK =KH

SUFFICIENT CONDITION:

Suppose that HK=KH

CLAIM: HK is a subgroup of G

Consider $(HK)(HK)^{-1} = (H K)(K^{-1}.H^{-1})$

$= H\,(K\,K^{-1}H^{-1})$

$= H(K\,K^{-1})H^{-1}$

$= (HK)\,H^{-1}$

$= (\,KH\,)\,H^{-1}$

$= K(H\,H^{-1})$

$= KH$

$=HK$

Therefore HK is a subgroup of group G.

THEROEM :

A non empty set complex H is a SubGroup of G

⇔ (1) $a,b \in H \Rightarrow a.b \in H$

(2) $a \in H \Rightarrow a^{-1} \in H$.

PROOF:

NECESSARY CONDITION:

Suppose that H is a SubGroup of G

CLAIM: (1) and (2) holds

Since (H ·) its self a group

(1) For $a,b \in H$

$a.b \in H$

for $a \in H$,H is a group

$\Rightarrow a^{-1} \in H$.

SUFFICIENT CONDITION:

Suppose that (1) $a,b \in H \Rightarrow a.b \in H$

(2) $a \in H \Rightarrow a^{-1} \in H$

CLAIM : H is a SubGroup of a group G i.e, to prove that (H,·) itself a group

ASSOCIATIVE ; Let $a,b,c \in H$

$\Rightarrow a,b,c \in G$
$\Rightarrow (a.b).c = a.(b.c)$

IDENTITY: Since $a \in H \Rightarrow a^{-1} \in H$

By (1) $a,a^{-1} \in H$
$e \in H$

Therefore (H,·) itself is a group

Therefore H is a subgroup of G .

THEROEM :

A NON Empty Complex H is a SubGroup of a group G⇔ a,b ∈H then $a,b^{-1} \in H$.

PROOF :

NECESSARY CONDITION:

Suppose that H is a SubGroup of a group (G .)

CLAIM :

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

Since (H ·) itself is a group
Let $a,b \in H$

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

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

SUFFICIENT CONDITION:

suppose that

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

CLAIM:

H is SubGroup of G (i.e) we have to prove that (H .) itself a Group

(1) ASSOCIATIVE : Let $a,b,c \in H$

$\Rightarrow a,b,c \in G$
$\Rightarrow (a.b).c = a.(b.c)$

(2) **IDENTITY** : by (1) ,a, $a \in H \Rightarrow a.a^{-1} \in H$

$\Rightarrow e \in H$

(3) **INVERSE** : By (1) $e,a \in H \Rightarrow e.a^{-1} \in H$

$\Rightarrow a^{-1} \in H$

(4) **BINARY OPERATION** :

Let $a,b \in H$

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

by (1) ,$a.(b^{-1})^{-1} \in H$

$\Rightarrow a.b \in H$

Therefore (H,·) itself is a group

Therefore H is a subgroup of G .

THEROEM :

IF H_1,H_2 are two SubGroup G then $H_1 \cap H_2$ is also a SubGroup of G .

PROOF :

Given that H_1 and H_2 are two SubGroups of a group G

CLAIM: $H_1 \cap H_2$ is a SubGroup of G clearly e $\in H_1 \cap H_2$

$\Rightarrow H_1 \cap H_2$ is a non empty subset

Let a,b $\in H_1 \cap H_2$

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

$\Rightarrow$ $a.b^{-1} \in H_1$ and $a.b^{-1} \in H_2$

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

By known theorem ,

$H_1 \cap H_2$ is a subgroup of G

PROBLEM :

By an Example to show that the union of two Subgroup's of a group need not be a subgroup .

Solution:

consider 2z & 3z are two Subgroups' of a group (z,+)

Now 2z.$\cup$ 3z ={0,± 2, ±3, ±4, ±6…}

Let 3,2 $\in$ 2z $\cup$3z

$\Rightarrow$ 3+2=5 not belongs to 2z $\cup$ 3z

Therefore 2z$\cup$ 3z need not be a subgroup

THEROEM :

If H_1 and H_2 are two subgroups of a group G, then $H_1 \cup H_2$ is a subgroup of G $\Leftrightarrow$ $H_1 \subseteq H_2$ (or) $H_2 \subseteq H_1$

PROOF:

Given $H_1 and$ H_2 are two subgroups of G

SUFFICIENT CONDITION:

Suppose $H_1 \subseteq H_2$ (or) $H_2 \subseteq H_1$

CLAIM:

$H_1 \cup H_2$ is a subgroup of G

If $H_1 \subseteq H_2 \Rightarrow H_1 \cup H_2 = H_2$ is a SubGroup of G
If $H_2 \subseteq H_1 \Rightarrow H_1 \cup H_2 = H_1$ is a SubGroup of G

Therefore $H_1 \cup H_2$ is a SubGroup of G

NECESSARY CONDITION:

Suppose $H_1 \cup H_2$ is a SubGroup of G

CLAIM : $H_1 \subseteq H_2$ (or) $H_2 \subseteq H_1$

If possible suppose that $H_1 \subsetneq H_2$ (or) $H_2 \subsetneq H_1$

Since $H_1 \subsetneq H_2 \Rightarrow \exists$ a $\in H_1 \ni$ a not belngs to H_2

$H_2 \subsetneq H_1 \Rightarrow \exists$ b $\in H_2 \ni$ b not belngs to H_1

Since a $\in H_1$, b $\in H_2 \Rightarrow$ a,b $\in H_1 \cup H_2$

$\Rightarrow ab \in H_1 \cup H_2$
$\Rightarrow ab \in H_1$ (or) $ab \in H_2$

Since $a^{-1} \in H_1$, ab $\in H_1$
$\Rightarrow a^{-1}(ab) \in H_1$

$\Rightarrow a^{-1} a.b \in H_1$

$\Rightarrow e.b \in H_1$

$\Rightarrow b \in H_1$

which is a contradiction to b does not belongs to H_1 similarly , we array a contradiction to a does not belongs to H_2.

Therefore $H_1 \subseteq H_2$ (or) $H_2 \subseteq H_1$.

THEROEM:

A finite non empty complex H is a SubGroup of a Group G ⇔ a,b $\in H$ for ab$\in H$

PROOF:

NECESSARY CONDITION:

Suppose that H is a SubGroup of a Group (G,·)

i.e ,(H .) itself is a group

CLAIM: a,b $\in H \Rightarrow$ ab $\in H$

Let a,b $\in H$

$\Rightarrow$a.b $\in H$

SUFFICIENT CONDITION:

Let a,b $\in H$-----(1) for a,b $\in H$

CLAIM: H is a subgroup of G

(1) from (1) , **.** is a Binary operation on H

(2) ASSOCIATIVE LAW:

Let a,b,c $\in H$

$\Rightarrow$a,b,c $\in G$

$\Rightarrow$a.(bc)=(ab).c

(3) IDENTITY : Let a $\in H$

Since a,a $\in H$ => $a^2 \in H$

$a^3 \in H$

.

.

.

$a^n \in H$ for $n \in z^+$

Let $a^r = a^s$ for some $r, s \in z^+$, $r > s$

$\Rightarrow a^r . a^{-s} = a^s . a^{-s}$

$\Rightarrow a^{r-s} = a^{s-s}$

$\Rightarrow a^{r-s} = a^{\circ} = e$

$\Rightarrow a^{r-s} = e$

$\Rightarrow e \in H$

(4) INVERSE : Let $a \in H$

Clearly $r-s-1 \in z^+ \Rightarrow a^{r-s-1} \in H$

Also $a^1.(a^{r-s-1}) = a^{r-s} = e$

Therefore $a^{r-s-1} \in H$ is the inverse of `a'

Therefore H itself a group

Therefore H is a subgroup of G

NORMALIZER OF AN ELEMENT IN A GROUP :

If G is a group and $a \in G$ then the set N (a) $= \{x \in G \,/\, ax = x\,a\}$ is called the NORMALIZER of `a' in G.

CENTRAIZER (OR) CENTRE OF A GROUP:

If G is a Group then the set Z (G) (or) $Z = \{ a \in G / ax = xa \in G\}$ is called Centre of a Group .

THEROEM:

Show that N (a) of `a' is a sub group of G .

PROOF:

CLAIM: N (a) is a subgroup of G

Let $a \in G$

Since a .e=e .a

$\Rightarrow e \in N$(a)

Therefore N (a) $\neq \emptyset \subseteq$ G

(1) Let x ,y $\in N$ (a)

$\Rightarrow$a x= xa, ay=y a

Now (x y) a=x (y a)

= x (ay)

= (x a) y

= (ax) y

(x y) a =a(x y)

$\Rightarrow x\, y \in N(a)$

(2) Let $x \in N$(a)

$\Rightarrow$x a=ax

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

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

$\Rightarrow e.\, a.\, x^{-1}= x^{-1}.a.e$

$\Rightarrow .a.\, x^{-1}= x^{-1}.a$

$\Rightarrow x^{-1} \in N$ (a)

Therefore N(a) is a SubGroup of G .

THEROEM:

Show that the centre Z(G) is a subgroup of G

PROOF :

Let $Z = \{a \in G \,/ ax=xa \ \forall\, x \in G\}$

CLAIM: Z is a SubGroup of G

Let $x \in G$

Since $x.\, e = e\, .x$

$\Rightarrow e \in Z$

Therefore $Z \neq \emptyset \subseteq G$

(1) Let $a,b \in Z$

$\Rightarrow a\, x=xa;\ bx=x\, b$

Now $(a\, b)\, x=a\, (b\, x)$

$= a(x\, b)$

$= (ax)\, b$

$(a\, b)x =(x\, a)b$

$(a\, b)x = x(a\, b)$

$\Rightarrow ab \in Z$

(2) Let $a \in Z$

$\Rightarrow x\, a=a\, x$

$\Rightarrow a\, x=x\, a$

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

$\Rightarrow (a^{-1}a)\, (xa^{-1}) = a^{-1}x\, (aa^{-1})$

$\Rightarrow e.xa^{-1}=a^{-1}x.e$

$\Rightarrow xa^{-1}=a^{-1}x$

$\Rightarrow a^{-1} \in Z$

Therefore Z is a subgroup of G.

COSETS AND LAGRANGE'S THEOREM:

DEFINITION:

Let H be a subgroup of a group G and $a \in G$ then this set $a.H = \{ a.h / h \in H\}$ is called left coset of H in G & the set $H.a = \{ h.a / h \in H \}$ is called Right coset of H in G .

NOTE:

If H is a subgroup of an abelian group G then $a.H = H.a$.

i.e , every left coset is a right coset .

RESULT:

Let H be a subgroup of G and $a,b \in G$

Then

(1) $a \in H \Leftrightarrow a.H = H$

$a \in H \Leftrightarrow H.a = H$

(2) $a \in Hb \Leftrightarrow H.a = H.b$

$a \in bH \Leftrightarrow a.H = b.H$

(3) $H.a = H.b \Leftrightarrow a.b^{-1} \in H$

$a.H = b.H \Leftrightarrow a^{-1}.b \in H$

THEROEM:

Any two left cosets of a subgroup of a group are either disjoint (or) identical .

PROOF:

Let H be a subgroup of a group G and $a,b \in G$.

Let aH,bH be two left cosets of H in G

CLAIM :

$aH \cap bH = \emptyset$ (or) $aH=bH$

Suppose that $aH \cap bH \neq \emptyset$

To prove that $aH = bH$

Let $c \in aH \cap bH$

$\Rightarrow c \in aH$ and $c \in bH$

$\Rightarrow cH = aH$ and $cH = bH$

$\Rightarrow aH=cH=bH$

$\Rightarrow aH=bH$

Therefore aH and bH are identical .

THEROEM :

Any two right cosets of a subgroup of a group either disjoint (or) identical .

PROOF :

Let H be a subgroup of a group G and $a,b \in G$

Let Ha,Hb be two Right cosets of H in G

CLAIM: $\boldsymbol{Ha \cap Hb = \emptyset}$

Suppose that $Ha \cap Hb \neq \emptyset$

To prove that $Ha = Hb$

Let $c \in Ha \cap Hb$

$\Rightarrow c \in Ha$ and $c \in Hb$

$\Rightarrow Hc=Ha$ and $Hc=Hb$

$\Rightarrow Ha=Hc=Hb$

$\Rightarrow Ha=Hb$

Therefore Ha and Hb are identical .

THEROEM :

If H is any subgroup of a group G then there exists a bijection between any two left cosets of H in G .

PROOF :

Given that H is a subgroup of a G and $a,b \in G$.

Let aH,bH be two left cosets of H in G

Define $f: aH \rightarrow bH$ by $(ah) = bh$, for $ah \in aH$

f is one –one:

Let $ah_1, ah_2 \in aH$ for $h_1, h_2 \in H$

Consider $f(ah_1) = f(ah_2)$

$\Rightarrow bh_1 = bh_2$

$\Rightarrow h_1 = h_2$

$\Rightarrow ah_1 = ah_2$

f is on –to:

Let $bH \in bH$

$\Rightarrow h \in H$

$\Rightarrow a \cdot h \in aH$

by (1) , $f(ah) = bh$

Therefore, f is onto

Therefore, $f:aH \to bH$ is a bijection .

NOTE:

By above theorem , concludes that any two left (right) cosets have the same no.of elements

THEROEM :

If H is a subgroup of a group G then there is a one to one correspondece between the set of all distinct left cosets of H inG and the set of all disrinct Right cosets of H inG .

PROOF:

Let G_1=set of all distinct left cosets of H in G .

G_2 = Set of all distinct Right cosets of H in G

Define $f:G_1 \to G_2$ by $f(aH) = H.a^{-1}$, for $aH \in G$

f is well defined and one-one :

Let $aH, bH \in G_1$

Let aH =bH

$\Leftrightarrow a^{-1}.b \in H$

$\Leftrightarrow a^{-1}[(b^{-1})]^{-1} \in H$

$\Leftrightarrow Ha^{-1} = Hb^{-1}$

$\Leftrightarrow f(aH) = f(bH)$.

f is onto :

Let $Ha \in G_2$

$\Rightarrow a \in G$

$\Rightarrow a^{-1} \in G$

$\Rightarrow a^{-1} \cdot H \in G,$

Therefore $f(a^{-1}H) = H(a^{-1})^{-1}$ [by (1)]

$= Ha$

Therefore f is onto

Therefore $f: G_1 \rightarrow G_2$ is a bijection

THEROEM :

State and Prove Lagrange's Theorem.

STATEMENT :

If H is a subgroup of a finite group G then $O(H) \mid O(G)$

PROOF :

Given that H is a subgroup of a finite group G

$\Rightarrow$H is finite & the no.of right cosets of H in G is finite

Let $Ha_1, Ha_2, \ldots, Ha_k$ be the distinct right cosets of H in G .

We know that every Right cosets of

$O(Ha_1) = O(Ha_2) = \ldots = O(Ha_k) = o(H)$

Since G is finte , the right cosets partitions into equivalence classes .

Therefore $G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_k$

$\Rightarrow$ $O(G) = O[Ha_1 \cup Ha_2 \cup_{\dots} \cup Ha_k]$

$= O(Ha_1) + O(Ha_2) + \dots + O(Ha_k)$

$\Rightarrow$ $O(G) = O(H) + O(H) + \dots$ [K times]

$\Rightarrow$ $O(G) = O(H).k$

$\Rightarrow$ $O(H) \mid O(G)$.

UNIT : III

Normal Subgroups

Definition:

A Subgroup H of a Group G is said to be Normal in G if $x\ h\ x^{-1} \in H, \forall\ h \in H$, $x \in G$

(or)

$X\ H\ x^{-1} \subseteq H\ \forall\ x \in G$ and it is denoted by H **α** G

Theorem :

Show that Every Subgroup of an abelian group is Normal

Proof : let H be a Subgroup of an abelian group G

Claim : H **α**G

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

$x\ h\ x^{-1} =(hx)x^{-1}$

$=h(xx^{-1})$

$=he$

$\therefore\ x\ h\ x^{-1}$

$\therefore\ x\ h\ x^{-1} \in H$

There fore H **α**G

Theorem :

A Subgroup H of a Group G is Normal in G $\Leftrightarrow$ **$xHx^{-1}=H$,** $\forall x \in G$

(or)

$H \,\alpha\, G \Leftrightarrow x H x^{1} = H, \forall x \in G$

Proof :

Necessary condition : let $H \,\alpha G$

By definition $x Hx^{-1} \subseteq H$------(i) $\forall x \in G$

Claim : $x H x^{-1}=H \ \forall x \in G$

From (i) $x^{-1}H (x^{-1})^{-1} \subseteq H \ \forall$

$X (x^{-1} H x) x^{-1} \subseteq x H x^{-1}$

$(x x^{-1}) H(x x^{-1}) \subseteq x H x^{-1}$

$e (H x) x^{-1} \subseteq x H x^{-1}$

$H (x x^{-1}) \subseteq x H x^{-1}$

$H e \subseteq x H x^{-1}$

$H \subseteq x H x^{-1} \forall x \in G$------(ii)

From (i) and (ii)

$x H x^{-1}=H , \forall x \in G$

Sufficiant Condition :

Suppose that $x H x^{-1}=H$------(iii) $\forall x \in G$

Claim : $H \,\alpha G$

From (iii) it is clear

$x H x^{-1} \subseteq H \forall x \in G$

There fore $H \,\alpha\, G$

Theorem :

A Subgroup H of a group G is Normal in G $\Leftrightarrow$ Each left coset of H in G is a right coset of H in G

Proof :

Necessary condition :

Let H α G

Claim : Each left coset is a right coset of H in G

By known theorem $x H x^{-1}=H \; \forall \; x \in G$

$\Rightarrow \; x H x^{-1} x = H x$

$\Rightarrow \; x H e=H x$

$\Rightarrow \; x H = H x \, , \; \forall \; x \in G$

Therefore Each left coset is a right coset of H in G

Sufficiant condition :

Suppose that Each left coset is right coset of H in G

That is X H = H X ....(i)

Claim : H α G

From (i) ,XH=HX

$\Rightarrow \; X H X^{-1} =H X X^{-1}$

$\Rightarrow X H X^{-1} = He$

$\Rightarrow X H X^{-1} = H \, , \; \forall \; x \in G$

There fore H α G

Theorem :

A Subgroup H of a group G is a Normal Subgroup of G $\Leftrightarrow$ The product of two right cosets of H in G is again a right coset of H in G

Proof :

Neccessary Condition :

Let H α G

Claim : Let a,b,ab ϵ G

$\Rightarrow$Ha ,Hb,Hab ϵ G are right cosets of H in G

Consider (Ha) (Hb) =H (aH) b

=H (Ha) b

=(HH) ab

=Hab is a right coset

$\therefore$ The product of two right cosets of H in G is again a right coset of H in G

Sufficiant condition :

Let (Ha) (Hb) =Hab……. (i)

Claim : H α G

Let xϵG ,hϵH

Consider xhx^{-1} = $(ex)\,h\,x^{-1}$ ϵ Hx H x^{-1}

$=H\,x\,x^{-1}$

= He

=H

$\Rightarrow$ $x\,h\,x^{-1}$ ϵ H

$\therefore$ By definition , H is a Normal Subgroup of G

Similarly , we can prove the theorem for left cosets also

Theorem:

Show that the intersection of two Normal Subgroups of a group G is again a Normal Subgroup of G

proof :

Let H and K be two Normal Subgroups of group G

Claim : H ∩ K **α** G

Clearly H ∩ K is a subgroup

Let x ϵ G ,h ϵ H ∩ K

⇒ x ϵ G , h ϵ H

⇒ $x \; h \; x^{-1}$ ϵ H........ (i)

x ϵ G , h ϵ K

⇒ $x \; h \; x^{-1}$ ϵ K........ (ii)

From (i) and

∴ $x \; h \; x^{-1}$ ϵ H ∩ K

∴ H ∩ K **α** G

Simple group :

A Group G is said to be Simple if it has no proper Normal Subgroups

Note :

G is Simple if and only if G has no Normal Subgroups other than G and {e}

Theorem:

Prove that Every group of prime order is simple

Proof :

0

Let G be a Group of Prime order P

Let N be a Normal Subgroup of G

By Lagrange's theorem

$$O(N) / O(G)$$

$$\Rightarrow O(N) / P$$

$$\Rightarrow O(N) = 1 \text{ (or) } O(N) = P$$

If $O(N) = 1$, then $N = \{e\}$

If $O(N) = P$, then $N = G$

$\therefore$ G has no Proper Normal Subgroups and hence, G is Simple

Hence, Every Group of Prime Order is Simple

UNIT -4

HOMOMORPHISMS

DEFINITIONS:-

HOMOMORPHISM: - Let G,G' be two groups. A mapping f: G →G' is called a "**Homomorphism**" if f(ab)=f(a) · f(b) ∀ a,b∈G.

HOMOMORPHIC IMAGE :- If f:G→G'is a homomorphism then the set f(G)={f(a)/a∈G} is called a "**Homomorphic Image Of G**".

_**MONOMORPHISM: -** A mapping f:G→G' is called a "**Monomorphism**"

if (I) f is homomorphism (II)f is 1-1.

EPIMORPHISM: - A mapping f:G→G' is called a "**Epimorphism**" if

(i)f is homomorphism and (ii)f is onto.

Isomorphism: - A mapping f: G→G' is called an **"Isomorphism"** if (i) f is homomorphism and (ii) f is both 1-1 and onto.

Endomorphism: - A homomorphism f: G→G is called an **"Endomorphism".**

Automorphism :- A mapping f: G→G is called an **"Automorphism"** if (i) f is homomorphism (ii) f is both 1-1 and onto.

Isomorphic: - Two graphs G and G' are said to be **"isomorphic"** if there exists an isomorphism of G and G' we write G≈G'.

Theorem:-_Let (G, ·) and (G', ·) be two groups Let f be a homomorphism from G onto G' Then (i)f(e)=e' where e be the identity in G and e' be the identity in G' (ii)$f(a^{-1})=\{f(a)\}^{-1}$.

Proof:- Given that (G, ·) and (G', ·) be two groups and f:G →G' is a homomorphism.

i.e., f(ab)=f(a).f(b) ∀ a∈G

(i)To prove f(e)=e'

$$f(e \cdot e)=f(e)$$

$$\Rightarrow f(e).f(e)=f(e).e'$$

$$\Rightarrow f(e)=e'$$

ii) To prove $f(a^{-1}) = (f(a))^{-1}$

$$= f(e). \quad \text{By(i) } f(e)=e'$$

$$= e'$$

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

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

i.e The inverse of $f(a^{-1})$ is f(a).

Theorem :- If f is a homomorphism from a group (G, ·) into (G', ·) Then

(f(G), ·) Is a subgroup of G' (or) the homomorphic Image of a group is a group.

Proof:- Given that f: G→G' is a homomorphism

The homomorphic Image of G is f(G)={f(a)/a∈G}

To Prove that f(G) is a subgroup of G'

Clearly $f(G) \subseteq G'$

Let $a', b' \in f(G)$

Then there exists $a, b \in G$ such that $f(a) = a'$ and $f(b) = b'$

Now $a'(b')^{-1} = f(a) \cdot (f(b))^{-1}$

$= f(a) \cdot f(b^{-1})$

$= f(ab^{-1})$

$\in f(G)$

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

Therefore $a', b' \in f(G)'$

Then $a'(b')^{-1} \in f(G)$

$\therefore f(G)$ is a subgroup of G'

Theorem:- Every Homomorphic Image of an abelian group is abelian.

Proof:- Let $(G, \cdot)$ be an abelian group and $(G', \cdot)$ be a group

Let $f: G \rightarrow G'$ be a homomorphism

Let G' be the homomorphic Image of G i.e $G' = f(G)$

To prove that G' is abelian

Since G is abelian $\Rightarrow ab = ba$ for $a, b \in G$

Let $a' b' \in G'$

Then there exists $a, b \in G \ni f(a) = a'$ and $f(b) = b'$

$a'b' = f(a)f(b)$

$= f(ab)$

$= f(ba)$

$= f(b) \cdot f(a)$

$= b'a'$

$\Rightarrow a'b' = b'a'$

Therefore G' is abelian

Kernel of a homomorphism:-

If f is a homomorphism of a group G into a group G' then the kernel of f is defined by Ker $f=\{x\in G/f(x)=e'\}$ where e' is the identity in G' .

Theorem: - If f is a homomorphism of a group G into a group G' then the kernel of f is a normal subgroup of G.

Proof:- Given that G and G' are two groups

Also $f:G\rightarrow G'$ be a homomorphism

To prove that ker f is a normal subgroup of G we know that

Ker $f=\{x\in G/f(x)=e'\}$ where $e'$is the identity in G'

Since $e\in G \Rightarrow f(e)=e'$, $e\in$ker f

$\Rightarrow$ker $f\neq\emptyset\subseteq G$

First we Prove ker f is a subgroup of G

Let $a,b\in$ ker f

$\Rightarrow f(a)=e'$ and $f(b)=e'$

Now $f(ab^{-1})= f(a) \cdot f(b^{-1})$

$= f(a) \cdot (f(b))^{-1}$

$= e'.(e')^{-1}$

$= e'.e'$

$= e'$

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

$\Rightarrow ab^{-1} \in \ker f$

Therefore ker f is a subgroup of G.

Now we Prove ker f is normal

Let $x \in G$ and $a \in \ker f \Rightarrow f(a)=e'$

Now $f(xax^{-1})= f(x)f(a)f(x^{-1})$

$= f(x).e'.f(x^{-1})$

$= f(x).f(x^{-1})$

$= f(xx^{-1})$

$= f(e)=e'$

$\Rightarrow \quad f(xax^{-1})=e'$

$\Rightarrow xax^{-1} \in \ker f$

$\therefore$ ker f is a normal subgroup of G.

Theorem: - The necessary and sufficient condition for a homomorphism f of a group G onto group G' with kernel K to be an isomorphism of G into G' is that k={e}.

Proof: - Let f be a homomorphism of a group G onto a group G'.

Let e,e' be the identities in G,G' respectively.

Let k be the kernel of f.

i.e., K = **Ker f = {x∈G/f(x)=e'}**

Suppose f:G→G' is an isomorphism

To prove that k = {e}.

Let a∈k

⇒f(a)=e'.

⇒f(a)=f(e)

⇒a=e for a∈G

Therefore e is the only element of k

⇒K = {e}

Conversely, suppose K = {e}

To Prove that f is an isomorphism.

Since f is onto homomorphism.

To prove f is one-one

Let a,b∈G

f(a) = f(b)

⇒ $f(a)(f(b))^{-1} = f(b)\,(f(b))^{-1}$

⇒ $f(ab^{-1}) = e$

⇒ $ab^{-1} \in K = \{e\}$

⇒ $ab^{-1} = e$

⇒ $ab^{-1}b = eb$

⇒ ae = b

$\Rightarrow a = b$

$\therefore$ f is one-one

Therefore f is an Isomorphism of G onto G'.

Theorem:- Let f be a homomorphism of a group G into G' then f is Monomorphism ⇔ ker f ={e} where e is the identity in G.

Proof :- Let f be a homomorphism of a group G into G'

We Know that **Ker f={x∈G/f(x)=e'}**

Suppose f: G→G' is Monomorphism

To Prove that ker f={e}

Let a∈ker f

$\Rightarrow f(a) = e'$.

$\Rightarrow f(a) = f(e)$

$\Rightarrow a = e$ for $a \in G$

$\therefore$ e is the only element of ker f

$\Rightarrow$ ker f={e}

Conversely, suppose ker f={e}

To prove that f is Monomorphism

Since f is homomorphism.

To prove f is one-one .

Let a,b∈G

f(a)=f(b)

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

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

$\Rightarrow f(ab^{-1}) = e$

$\Rightarrow ab^{-1} \in k = \{e\}$

$\Rightarrow ab^{-1} = e$

$\Rightarrow ab^{-1}b = eb$

$\Rightarrow ae = b$

$\Rightarrow a = b$

∴f is one-one

∴ f is an monomorphism of G into G'.

Theorem:- Let G be a group and N be a normal subgroup of G. Let f be a mapping from G to G/N defined by f(x)=Nx for x∈G . Then f is a homomorphism of G onto G/N and ker f = N

Proof:- Given that G is a group and N is a normal subgroup of G.

Let f be a mapping from G to G/N defined by $f(x)=Nx \rightarrow (1)$ for $x \in G$.

(i) f is a homomorphism :-

Let $a,b \in G$

$f(ab)= Nab$ ∴by(1)

$= Na\cdot Nb$ ($\because Ha\cdot Hb=Hab$)

$= f(a).f(b)$

$\Rightarrow f(ab) = f(a).f(b)$

Therefore f is a homomorphism.

(ii) f is onto :-

Let $Nx \in G/N$ for $x \in G$

Since $x \in G$

Now $f(x)=Nx$ $\therefore$by (1)

$\therefore$ f is onto

(iii) ker f=N :-

The identity of the quotient group G/N is N

$\Rightarrow \ker f=\{x \in G/f(x)=N\}$

Let $k \in \ker f$

$\Rightarrow f(k)=N$

By (1) $f(k)=Nk$

$\Rightarrow N = Nk$

$\Rightarrow k \in N$

$\Rightarrow \ker f \subseteq N \rightarrow (1)$ $(H = hH, h \in H)$

Let $n \in N$

We have $f(n) = Nn = N$

$\Rightarrow f(n)=N$

$\Rightarrow n \in \ker f$

$\Rightarrow N \subseteq \ker f \rightarrow (2)$

From (1) and (2) we get $\ker f = N$

Definition: - The mapping $f:G \rightarrow G/N$ such that $f(x)=Nx$ for all $x \in G$ is called Natural (or) "canonical homomorphism".

PROBLEM:

1. **If for a group G, $f:G \rightarrow G$ is given by $f(x)=x^2$ $\forall$ $x \in G$ is a homomorphism then prove that G is abelian.**

Proof : Given that $f:G \rightarrow G$ is a homomorphism and is defined by

$$f(x)=x^2 \ \forall \ x \in G$$

To Prove G is a abelian

Let $x,y \in G \Rightarrow f(x)=x^2, f(y)=y^2$

$xy \in G \Rightarrow f(xy)=(xy)^2$

$\Rightarrow f(x) \cdot f(y)=(xy)(xy)$

$\Rightarrow x^2 \cdot y^2=(xy)(xy)$

$\Rightarrow (x \cdot x)(y \cdot y)=(xy)(xy)$

$\Rightarrow x\,(xy)y=x(yx)y$

$\Rightarrow xy=yx$

$\therefore$ G is abelian.

Theorem: - Let G be a multiplicative group and $f:G \rightarrow G$ be a mapping such that for $a \in G, f(a)=a^{-1}$ then prove that f is one-one onto. Also prove that f is a homomorphism iff G is commutative

Proof:- Given that $f:G \rightarrow G$ is a mapping defined by $f(a)=a^{-1}$ for all $a \in G$

(i) **f is one –one :-** Let $a,b \in G$

$f(a) = f(b)$

$a^{-1} = b^{-1}$

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

$a = b$

$\therefore$ f is one - one

(ii) <u>f is onto</u> :- Let $x \in G$

Then $x^{-1} \in G$ such that $f(x^{-1}) = (x^{-1})^{-1}$

$= x$

$\Rightarrow f(x^{-1}) = x$

$\therefore \exists\, x^{-1} \in G \ni f(x^{-1}) = x$

$\Rightarrow$ f is onto

(iii) Suppose f is a homomorphism :-

To prove G is commutative

Let $a,b \in G \Rightarrow f(a) = a^{-1}$, $f(b) = b^{-1}$

Since $f(ab) = f(a) \cdot f(b)$

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

$\Rightarrow b^{-1}a^{-1} = a^{-1} \cdot b^{-1}$

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

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

$\Rightarrow ba = ab$

$\Rightarrow ab = ba$

Conversely, suppose G is commutative

i.e. $a, b \in G \Rightarrow ab = ba$

To prove f is a homomorphism

Now $f(ab) = (ab)^{-1}$

$= b^{-1}a^{-1}$

$= a^{-1}b^{-1}$

$= f(a) \cdot f(b)$

$\Rightarrow f(ab) = f(a) \cdot f(b)$

Fundamental theorem of homomorphism of groups:-

Statement:-If $f: G \to G'$ is a homomorphism and onto with kernel K, then Prove that $G/K \approx G'$.

OR

Every homomorphism Image of a group G is "Isomorphic" to some "quotient group" of G.

Proof:- Let f be a homomorphism of a group G onto group G'.

Then $f(G) = G'$

$\Rightarrow$ K is a normal subgroup of G.

$\Rightarrow$ G/K is a quotient group.

for $a \in G$, $Ka \in G/K$ and $f(a) \in G'$

Now Define a mapping $\varnothing : G/K \to G'$ by $\varnothing(Ka) = f(a)$ for $a \in G$

$\varnothing$ is well defined:-

Let $Ka, Kb \in G/K$

Now $Ka = Kb$

$ab^{-1} \in K$

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

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

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

$\Rightarrow f(a)\, e' = e'\, f(b)$

$\Rightarrow f(a) = f(b)$

$\Rightarrow \varnothing(Ka) = \varnothing(Kb)$

$\therefore \varnothing$ is well defined

$\varnothing$ **is one-one** :-

Let $Ka, Kb \in G/K$

$\varnothing(Ka)=\varnothing(Kb)$

$\Rightarrow f(a) = f(b)$

$\Rightarrow f(a)\, e' = e' f(b)$

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

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

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

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

$\Rightarrow ab^{-1} \in K$

$\Rightarrow Ka = Kb$

$\therefore \varnothing$ is one-one.

$\varnothing$ **is onto :-**

Let $x \in G'$

Since $f:G \to G'$ is onto

$\Rightarrow \exists\ a \in G \ni f(a)=x$

Since $a \in G$ then $ka \in G/K$

Now $\varnothing(Ka) = f(a) = x$

$\Rightarrow \varnothing(Ka) = x$

$\therefore \varnothing$ is onto

$\varnothing$ is a homomorphism:-

Let $Ka, Kb \in G/K$

$\varnothing(Ka \cdot Kb) = \varnothing(Kab)$

$= f(ab)$

$= f(a) \cdot f(b)$

$= \varnothing(Ka) \cdot \varnothing(Kb)$

$\Rightarrow \varnothing(Ka \cdot Kb) = \varnothing(Ka) \cdot \varnothing(Kb)$

$\therefore \varnothing$ is a homomorphism

Hence $\varnothing: G/K \to G'$ is an isomorphism.

$\Rightarrow G/K \approx G'$

Theorem: - show that the mapping $f:G \to G$ Is defined by $f(a)=a^{-1}$ for $a \in G$ is an automorphism iff G is abelian.

Proof: - Given that $f:G \to G$ is a mapping defined by $f(a)=a^{-1}$ for $a \in G$.

First Assume f is an automorphism.

To prove G is abelian

Let $x, y \in G \Rightarrow f(x) = x^{-1}, f(y) = y^{-1}$

$\Rightarrow f(xy) = (xy)^{-1}$

$\Rightarrow f(xy) = y^{-1}x^{-1}$

$\Rightarrow f(xy) = f(y)f(x)$

$\Rightarrow f(xy) = f(yx)$

$\Rightarrow \quad xy = yx$

$\therefore$ G is abelian

Conversely suppose G is abelian

To prove f is an Automorphism

f is one-one :-

Let $x, y \in G$

$f(x) = f(y)$

$x^{-1} = y^{-1}$

$(x^{-1})^{-1} = (y^{-1})^{-1}$

$x = y$

$\therefore$ f is one-one

f is onto :-

Let $x \in G$ (co-domain)

Then $x^{-1} \in G$ (domain)

Now $f(x^{-1}) = (x^{-1})^{-1} = x$

$\therefore x \in G \ \exists \ x^{-1} \in G \ni f(x^{-1}) = x$

$\Rightarrow$ f is onto

f is homomorphism :-

Let $x,y \in G$

$f(xy) = (xy)^{-1}$

$= y^{-1}x^{-1}$

$= x^{-1}y^{-1}$

$= f(x) \cdot f(y)$

$\Rightarrow f(xy) = f(x) \cdot f(y)$

$\therefore$ f is a homomorphism

Hence f is an Automorphism.

Theorem: - Let a be a fixed element of a group G.Then the mapping $f_a : G \to G$ is defined by $f_a(x) = a^{-1}xa$ for $x \in G$ is an Automorphism of G.

Proof :- Let a be a fixed element of G.

$f_a : G \to G$ is defined by $f_a(x) = a^{-1}xa$ for $x \in G$

To prove fa is an Automorphism

f_a is one-one :-

Let $x,y \in G$

$f_a(x) = f_a(y)$

$\Rightarrow a^{-1}xa = a^{-1}ya$

$\Rightarrow x = y$

$\therefore$ fa is one-one

f_a is onto :-

Let $y \in G$ (Co-Domain)

Since $a \in G$

$\Rightarrow a^{-1} \in G$

$\Rightarrow aya^{-1} \in G$ (Domain)

Now $f_a(aya^{-1}) = a^{-1}(aya^{-1})a$

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

$= e\ y\ e$

$= y$

$\therefore y \in G \ \exists\ aya^{-1} \in G \ni f_a(aya^{-1}) = y$

$\Rightarrow f_a$ is onto

f_a is a homomorphism :-

Let $x, y \in G$

$f_a(xy) = a^{-1}xya$

$= a^{-1}xeya$

$= a^{-1}x(aa^{-1})ya$

$= a^{-1}xeya$

$= a^{-1}x(aa^{-1})ya$

$= (a^{-1}xa)\ (a^{-1}ya)$

$= fa(x) \cdot f(a)y$

$= fa(xy) = fa(x) \cdot fa(y)$

$\therefore f_a$ is a homomorphism

Hence f_a is an Automorphism.

Inner Automorphism :- Let G be a group and 'a' be a fixed element in G. Then the mapping $f_a:G \to G$ is defined by

$f_a(x)=a^{-1}xa$ for $x \in G$ is known as Inner Automorphism.

Outer Automorphism :- An Automorphism which is not inner is called outer Automorphism.

NOTE :- The Set of all Automorphism of a group G is denoted by A(G) and is defined as $A(G)=\{f/f:G \to G \text{ is an Automorphism}\}$.

Theorem:- The set of all Automorphism of a group G form a group with respect to composition of mappings.

Proof :- Let G be a group

Define $A(G)=\{f/f:G \to G \text{ is an Automorphism}\}$

To prove that (A(G),o) is a group.

Binary operation :-

Let $f,g \in A(G)$

Clearly fog is bijective (one-one,onto)

Now $(fog)(ab) = f(g(ab))$

$= f(g(a)\cdot g(b))$

$= f(g(a))\cdot(g(b))$

$= fog(a)\cdot fog(b)$

$\Rightarrow$ fog is a homomorphism

$\Rightarrow fog \in A(G)$

$\therefore f,g \in A(G)$

$\Rightarrow fog \in A(G)$

$\Rightarrow$ 'o' is a binary operation on A(G).

Associative :-

Let f,g,h $\in$A(G),x$\in$G

Now ((fog)oh)(x) = (fog)(h(x))

= f(g(h(x)))

= f((goh)(x))

= (fo(goh))(x)

$\therefore$ 'o' is associative.

Existence of Identity:-

Let f $\in$bA(G).

We know that I:G→G is an Automorphism

$\Rightarrow$ I$\in$A(G)

Now (foI)(x) = f(I(x))

= f(x)

$\Rightarrow$ foI = f

(Iof)(x) = I(f(x))

= f(x)

Iof = f

$\therefore$ I $\in$ A(G) is the identity.

Existance of Inverse :-

Let f $\in$ A(G), I $\in$ A(G)

Clearly f^{-1}:G→G is bijective

Let $a,b \in G$

Now $f[f^{-1}(a) \cdot f^{-1}(b)]$

$= (f o f^{-1})(a) \cdot (f o f^{-1})(b)$

$= I(a) \cdot I(b) = ab$

$\Rightarrow f[f^{-1}(a) \cdot f^{-1}(b)] = ab$

$\Rightarrow f^{-1}[f(f^{-1}(a) \cdot f^{-1}(b))] = f^{-1}(ab)$

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

$\Rightarrow f^{-1}$ is an homomorphism

$\Rightarrow f^{-1} \in A(G)$

$\therefore$ (A(G),o) is a group.

UNIT – 5

PERMUTATIONS GROUPS

DEFINITION:A Permutation is a one –one mapping of a empty set onto itself.Thus a permutation is a bijective mapping of a non-empty set onto itself.

Example: f: R → R defined by f(x) = x+1 is a permutation of R since f is an one-one mapping onto itself .

Note: If S = { a_1 , a_2 ,..... a_n } then a one – one mapping from S onto itself is called a permutation of degree n . The number of elements in S is called the degree of permutation.

Equal Permutation: Two permutations f and g defined over a non-empty set S are said to be equal if f(a) = g(a) for all a ∈S

Permutation multiplication (or) Product of permutations:

It is the composition of mappings defined over the non – empty set S. If g , f are two permutations (bijective mapping) defined over S, then the product or multiplications of f, g is defined as gof (or) gf where

(gf) (a) = g[f(a)] for all a ∈S.Further gf is also a bijective mapping over S .

Product of Permutations (or) Multiplication of permutations (or) Composition of permutations in S_n :

Let f = $\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$, g = $\begin{pmatrix} b_1 & b_2 & \dots & b_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix}$ be two elements (permutations) of S_n. Here b_1 , b_2, ... b_n (or)c_1 , c_2 , ... c_n are nothing but the elements a_1 , a_2 ,..... a_n of S_n is some order.

Therefore gf = $\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix}$

Permutation Group: The set A(S) of all permutations defined over a

non-empty set S forms a group under the operation permutation multi[placation.

The above group is called group of permutations .

Identity Permutation: If f is a permutation of S such that f(a) = a for all a $\in$S, then f is identity of S and we denote f as I .

Order of permutation: If f$\in S_n$ such that f^n = I, the identity permutation in S_n,where n is the least positive integer, then the order of the permutation f is S_n is n.

Note: Order of S_n is n!

If the number of elements in S is 1, then the order of S is 1! = 1

If the number of elements in S is 2, then the order of S is 2! = 2

If the number of elements in S is 3, then the order of S is 3! = 6 and so on

Problems:

1. **If A = $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and B = $\begin{pmatrix} 1 & 2 & 3 \\ & 1 & 2 \end{pmatrix}$, then find AB and BA.**

Solution: Given that A = $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and B = $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

AB= $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ = I

BA= $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ = I

Therefore AB = BA = I

2. **If f =$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}$, g = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$, then find fg and gf.**

Solution: Given that f =$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & \end{pmatrix}$, g = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & \end{pmatrix}$

fg = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$

gf = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & \end{pmatrix}$

3. **If f =$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$, g = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ & 3 & 4 & 5 & 2 \end{pmatrix}$, h = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$**
Then find (fg)h = f(gh).

Solution: Given that f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$, g= $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & \end{pmatrix}$, and h = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & \end{pmatrix}$

fg = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$

(fg)h = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$

(fg)h = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}$

Next to find f(gh)

gh = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & \end{pmatrix}$

f (gh) = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$

f (gh) = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}$

Therefore f(gh) = (fg)h

Multiplication is Associative.

Inverse of a permutation: It is also a permutation (bijection).

If f = $\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$,then its inverse, denoted by f^{-1} is $\begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$

Problems:

1. **Find the inverse of the permutation f =** $\begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} & \mathbf{6} \\ \mathbf{3} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{1} & \mathbf{2} \end{pmatrix}$

Solution: Given that f = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & \end{pmatrix}$

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

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & \end{pmatrix}$

Example: Consider S = {1 , 2 , 3} and a permutation on S is f = $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Here f(1) = 2

$f^2(1) = f(f(1)) = f(2) = 1$

The orbits of 1 under f = { f(1) , f(2)} = {2 , 1}

f(2) = 1

$f^2(1) = f(f(2)) = f(1) = 2$

The orbits of 2 under f = { f(2) , $f^2(2)$} = { 1, 2}

f(3) = 3

The orbits of 3 under f = { f(3)} = {3}.

Problem : Find the orbits of σ = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 5 & 1 & 4 & 6 & 8 & 7 \end{pmatrix}$

Solution : Given that $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 5 & 1 & 4 & 6 & 8 & 7 \end{pmatrix}$

Now σ (1) = 2

$\sigma^2(1) = \sigma(\sigma(1)) = \sigma(2) = 3$

$\sigma^3(1) = \sigma(\sigma^2(1)) = \sigma(3) = 5$

$\sigma^4(1) = \sigma(\sigma^3(1)) = \sigma(5) = 4$

$\sigma^5(1) = \sigma(\sigma^4(1)) = \sigma(4) = 1$

The orbits of 1 under σ is {2,3,5,4,1}.

σ (2) = 3

$\sigma^2 (2) = \sigma (\sigma(2)) = \sigma (3) = 5$

$\sigma^3 (2) = \sigma (\sigma^2(2)) = \sigma (5) = 4$

$\sigma^4 (2) = \sigma (\sigma^3(2)) = \sigma (4) = 1$

$\sigma^5(2) = \sigma (\sigma^4(2)) = \sigma (1) = 2$

The orbits of 2 under σ is {3,5,4,1,2}.

$\sigma (3) = 5$

$\sigma^2 (3) = \sigma (\sigma(3)) = \sigma (5) = 4$

$\sigma^3 (3) = \sigma (\sigma^2(3)) = \sigma (4) = 1$

$\sigma^4 (3) = \sigma (\sigma^3(3)) = \sigma (1) = 2$

$\sigma^5(3) = \sigma (\sigma^4(3)) = \sigma (2) = 3$

The orbits of 3 under σ is {5,4,1,2,3}.

$\sigma (4) = 1$

$\sigma^2 (4) = \sigma (\sigma(4)) = \sigma (5) = 2$

$\sigma^3 (4) = \sigma (\sigma^2(4)) = \sigma (4) = 3$

$\sigma^4 (4) = \sigma (\sigma^3(4)) = \sigma (1) = 5$

$\sigma^5(4) = \sigma (\sigma^4(4)) = \sigma (2) = 4$

The orbits of 4 under σ is {1,2,3,5,4}.

$\sigma (5) = 4$

$\sigma^2 (5) = \sigma (\sigma(5)) = \sigma (5) = 1$

$\sigma^3 (5) = \sigma (\sigma^2(5)) = \sigma (4) = 2$

$\sigma^4 (5) = \sigma (\sigma^3(5)) = \sigma (1) = 3$

$\sigma^5(5) = \sigma (\sigma^4(5)) = \sigma (2) = 5$

The orbits of 5 under σ is {4,1,2,3,5}.

$\sigma (6) = 6$

The orbits of 6 under σ is {6}.

σ (7) = 8

$\sigma^2 (7) = \sigma (\sigma(7)) = \sigma (8) = 7$

The orbits of 7 under σ is {8,7}.

σ (8) = 7

$\sigma^2 (8) = \sigma (\sigma(8)) = \sigma (7) = 8$

The orbits of 8 under σ is {7,8}.

Problem : Find the order of the permutation σ = $\begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} & \mathbf{6} \\ \mathbf{2} & \mathbf{3} & \mathbf{5} & \mathbf{1} & \mathbf{4} & \mathbf{6} \end{pmatrix}$

Solution : Given that $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 1 & 4 & 6 \end{pmatrix}$

$$\sigma^2 = \sigma.\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 1 & 4 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 1 & 4 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 2 & 1 & 6 \end{pmatrix}$$

$$\sigma^3 = \sigma^2.\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 2 & 1 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 1 & 4 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 3 & 2 & 6 \end{pmatrix}$$

$$\sigma^4 = \sigma^3.\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 3 & 2 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 1 & 4 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 5 & 3 & 6 \end{pmatrix}$$

$$\sigma^5 = \sigma^4.\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 5 & 3 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 1 & 4 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

The order of the permutation σ is 5.

Cyclic permutation : Consider a set $S = \{ a_1, a_2, \ldots\ldots a_n\}$ and a permutation

$$f = \begin{pmatrix} a_1 & \square_2 & \square & \cdots & \square_{\square} & a_{k+1} & \cdots & a_n \\ a_2 & & {}_3 & & & a_{k+1} & \cdots & a_n \end{pmatrix} \quad \text{on } S$$

i.e., $f(a_1) = a_2$, $f(a_2) = a_3$, $f(a_3) = a_4 \ldots f(a_k) = a_1$, $f(a_{k+1}) = a_{k+1} \ldots f(a_n) = a_n$

This type of permutation f is called a cyclic permutation of length k and degree n. It is represented by $(a_1, a_2, \ldots a_k)$ (or) $(a_1, a_2, \ldots a_k)$ which is a cycle of length k (or) k-cycle. The number of elements permuted by a cycle is called it's length.

Example : If S = {1 , 2 , 3 , 4 , 5 , 6} then a permutation f on S is

$$\begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} \\ \mathbf{3} & \mathbf{1} & \mathbf{4} & \mathbf{6} & \mathbf{5} \end{pmatrix}$$

Solution: It can be written as (1 3 4 6 2)

f is a cycle of length 5

f can also be written as (3 4 6 2 1) (or) (4 6 2 1 3) etc

Example: Find the order of the cycle (1 4 5 7)

Solution : Let f = (1 4 5 7)

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 5 & 7 & 6 & 1 \end{pmatrix}$$

$$f^2 = f \cdot f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 5 & 7 & 6 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 5 & 7 & 6 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 3 & 7 & 1 & 6 & 4 \end{pmatrix}$$

$$f^3 = f^2 \cdot f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 3 & 7 & 1 & 6 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 5 & 7 & 6 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}$$

$$f^4 = f^3 \cdot f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 5 & 7 & 6 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$$

$f^4 = I$

The order of the cycle is 4.

Transposition: A cycle of length 2 is called is called a transposition.

Example : If S = {1 2 3 4 5 } and a permutation f on S is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$

then f = (2 , 3) is a cycle of length 2 and degree 5.

Disjoint cycle: Let S = { a_1 ,a_2 , ... a_n} . If f , g be two cycles on S such that they have no common elements then these are called disjoint cycles.

Example: Let S = {1 2 3 4 5 6 7}

- If f = (1 3 7) and g = (2 4 5) then f , g are disjoint cycles .
- If f = (1 3 7) and g = (2 3 4 5) then f , g are not disjoint cycles .

Inverse of a cyclic permutation:

Example : If f = (2 3 4 1) of degree 5 then find f^{-1}

Solution : Given that f = (2 3 4 1)

f^{-1} = (1 4 3 2)

Since $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$

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

Problem : If f = {1 2 3 4 5 8 7 6} , g = {4 1 5 6 7 3 2 8} are cyclicpermutations then show that $(fg)^{-1} = g^{-1} f^{-1}$.

Solution : Given that f = {1 2 3 4 5 8 7 6}

$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 8 & 1 & 6 & 7 \end{pmatrix}$

$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 2 & 3 & 4 & 7 & 8 & 5 \end{pmatrix}$

$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 2 & 1 & 6 & 7 & 3 & 4 \end{pmatrix}$

$g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 7 & 8 & 1 & 5 & & 6 \end{pmatrix}$

$$fg = \begin{pmatrix}1&2&3&4&5&6&7&8\\2&3&4&5&8&1&6&7\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8\\5&8&2&1&6&7&3&4\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3&4&5&6&7&8\\8&7&3&2&1&6&4&\end{pmatrix}$$

$$(fg)^{-1} = \begin{pmatrix}1&2&3&4&5&6&7&8\\5&4&3&7&8&6&2&1\end{pmatrix}$$

$$g^{-1} f^{-1} = \begin{pmatrix}1&2&3&4&5&6&7&8\\4&3&7&8&1&5&6&2\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8\\6&1&2&3&4&7&8&\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3&4&5&6&7&8\\5&4&3&7&8&6&2&1\end{pmatrix}$$

Therefore $(fg)^{-1} = g^{-1} f^{-1}$.

Order of a cyclic permutation:

Example : If $f = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ is a permutation group f_3.

Solution : The cyclic permutation of f is (1 2 3)

$$f^2 = f.f = \begin{pmatrix}1&2&3\\&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$$f^3 = f^2.f = \begin{pmatrix}1&2&3\\&3&2\;1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\&2&3\end{pmatrix}$$

$$f^3 = I$$

Therefore f is a cyclic permutation of length 3 and degree 3. Also the order of f is 3.

Problem: write down the following products are disjoint cycles.

i. **(1 3 2)(5 6 7)(2 6 1)(4 5)**
ii. **(1 3 6)(1 3 5 7)(6 7)(1 2 3 4)**

Solution : (i) (1 3 2)(5 6 7)

$$= \begin{pmatrix}1&2&3&4&5&6&7\\3&1&2&4&5&6&7\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7\\1&2&3&4&6&7&5\end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 4 & 6 & 7 & 5 \end{pmatrix}$$

(2 6 1)(4 5)

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 3 & 4 & 5 & 1 & 7 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 5 & 4 & 6 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 3 & 5 & 4 & 1 & \end{pmatrix}$$

Now $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 4 & 6 & 7 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 3 & 5 & 4 & 1 & 7 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 2 & 6 & 4 & 3 & 5 \end{pmatrix} = (2\ 7\ 5\ 4\ 6\ 3)\ (1)$$

(ii) (1 3 6)(1 3 5 7)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 6 & 4 & 5 & 1 & 7 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 7 & 6 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 5 & 4 & 7 & 1 & 3 \end{pmatrix}$$

(6 7)(1 2 3 4)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 7 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 5 & 6 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 5 & 7 & 6 \end{pmatrix}$$

Now $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 5 & 4 & 7 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 5 & 7 & 6 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 4 & 6 & 7 & 3 & 1 \end{pmatrix} = (1\ 2\ 5\ 7)(3\ 4\ 6)$$

Problem: Express the product (2 5 4)(1 4 3)(2 1) are the product of disjointcycles and find its inverse.

Solution : Given that (2 5 4)(1 4 3)(2 1)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$$

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

Let $f = (1\ 5\ 4\ 3)(2)$

$f^{-1} = (3\ 4\ 5\ 1)\ (2) = \begin{pmatrix}1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & \end{pmatrix}.$

Note :

- The multiplication of disjoint cycles is commutative.
- Every permutation can be expressed as a product of disjoint cycles which is unique(a part from the order of the factors).
- Every cycle can be expressed as a product of transpositions.
- Every permutation can be expressed as a product of transpositions in many ways.

Even and Odd Permutations: A permutation is said to be an even (odd) permutation if it can be expressed as a product of even (odd) number of transpositions .

Note :

- Identity Permutation I is always an even permutation.
- A cycle of length n can be expressed as a product of n-1 transposition. If n is odd then the cycle can expressed as the product of odd number of transposition .If n is even then the cycle can expressed as the product of odd number of transposition.
- The product of two odd permutations is an even permutation.
- The product of two even permutations is an even permutation.
- The product of an odd permutations and an even permutation is an odd permutation.

- The inverse of an odd permutation is an odd permutation.
- The inverse of an even permutation is an even permutation.

Problem:

Examine whether the following permutations are even (or) odd.

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 5 & 6 & 7 & 1 \end{pmatrix}$ **(ii)** $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ & 3 & 1 & 8 & 5 & 6 & 2 & 4 \end{pmatrix}$

(iii) (1 2 3 4 5) (1 2 3) (4 5) **(iv)** $\begin{pmatrix} \square & \square & \square & \square & \square & \square & \square & 8 & 9 \\ \square & \square & \square & \square & \square & \square & \square & 8 & 9 \end{pmatrix}$

Solution: (i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 5 & 6 & 7 & 1 \end{pmatrix}$

= (1 3 4 5 6 7) (2)

= (1 3) (1 4)(1 5)(1 6)(1 7)(2)

Therefore the number of transpositions are odd

Given Permutation is odd.

(ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 1 & 8 & 5 & 6 & 2 & 4 \end{pmatrix}$

= (1 7 2 3) (4 8) (5) (6)

= (1 7) (1 2) (1 3) (4 8) (5) (6)

Therefore the number of transpositions are even.

Given Permutation is even.

(iii) (1 2 3 4 5) (1 2 3) (4 5)

(1 2) (1 3) (1 4) (1 5) (2 3) (4 5)

Therefore the number of transpositions are even.

Given Permutation is even.

(iv) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 1 & 4 & 3 & 2 & 5 & 7 & 8 & 9 \end{pmatrix}$

= (1 6 5 2) (3 4) (7) (8) (9)

= (1 6) (1 5) (1 2) (3 4)

Therefore the number of transpositions are even.

Given Permutation is even.

Theorem: Let S_n be the permutation group on n symbols.Then of the n! Permutations (elements) in ½ n! are even permutations and ½ n! are odd permutations.

Solution : Let $S_n = \{e_1, e_2, ...ep, o_1, o_2, ... o_q\}$ be the permutation group on n symbols where $e_1, e_2, ...e_p$ are even permutations and

$o_1, o_2, ...o_q$ are odd permutations (∵any permutation can be either even (or) odd but not both).

$\therefore p+q = n!$

Let $t \in S_n$ and t be a transposition.

Then $te_1, te_2, ...te_p, to_1, to_2, ...to_q$ are elements of S_n as permutation multiplication is a binary operation in S_n

Since t is an odd permutation $te_1, te_2, ...te_p$ are all odd and to ,

$tO_1, tO_2, ...tO_q$ are all even permutations.

Let $te_i = te_j$ for $i \le p$, $j \le p$

$\Longrightarrow e_i = e_j$

which is absurd.

Therefore $te_i \neq te_j$ and hence the p permutations are all distinct in S_n .

But S_n contains exactly q odd permutations $p \le q$.

Similarly we can show that q even permutations

$tO_1, tO_2, ...tO_q$ are all distinct even permutations in S_n.

$q \le p$

$p = q = ½ n!$

So has ½ n! even permutations and ½ n! odd permutations.

Alternating set of permutations of degree n:

Let S_n be the permutation group on n symbols. The set of all ½ n! even permutations of S_n , denoted by A_n is called the alternating set of permutations of degree n.

Theorem: The set An of all even permutations of degree n forms a group oforder ½ n! With respect to permutation multiplication.

Proof: Let set An of all even permutations of degree n

- **Closure :** Let $f,g \in A_n$

  i.e., f,g are even permutations on n symbols.

$\Rightarrow$ fg is also an even permutation on n symbols.

$\Rightarrow fg \in A_n$

- **Associativity:** Since a permutation is a bijection, multiplication of permutations (composition of mappings) is associative.
- **Existence of identity:** Let I be the identity Permutation on n symbols, then $I \in A_n$, since I is an even permutation.

Then I is an even permutation

$\Rightarrow I \in A_n$

Also for any $f \in A_n$, $fI = If = f$

I is an identity element in A_n .

- **Existence of inverse:** Let $f \in A_n$

$\Rightarrow$ f is an even permutation.

$\Rightarrow f^{-1}$ is also an even permutation

$\Rightarrow f^{-1} \in A_n$

Also $ff^{-1} = f^{-1}f = I$

Every element of A_n is invertible and the inverse of f is f^{-1}

A_n is a group of order ½ n! since the number of permutation on n symbols is ½ n!

Thus The set An of all even permutations of degree n forms a group of order ½ n! With respect to permutation multiplication.

Theorem: The set A_n of all even permutations on n symbols is a normalsubgroup of the permutation group S_n on the n symbols.

Proof: Let A_n be the set of all even permutations on n symbols .

We know that S_n is a group on n symbols with respect to Permutation multiplication and A_n ($\subset S_n$) is the set of even permutations.

Also A_n is a group with respect to Permutation multiplication.

Let $f \in \mathbf{S}_n$ and $g \in A_n$

g is an even permutation and f is even (or) odd permutation.

If f is an odd permutation then f^{-1} is also an odd permutation.

Also fg is an odd permutation.

fgf^{-1} is an even permutation and hence $fgf^{-1} \in A_n$

If f is an even permutation then f^{-1} is also an even permutation.

Also fg is an even permutation.

fgf^{-1} is an even permutation and hence $fgf^{-1} \in A_n$.

Thus $f \in S_n$ and $g \in A_n \Longrightarrow fgf^{-1} \in A_n$.

A_n is a normal subgroup of S_n

i.e., The set A_n of all even permutations on n symbols is a normal subgroup of the permutation group S_n on the n symbols.

Cayley's theorem :

Theorem: Every finite group G is isomorphic to a Permutation group.

Proof: Let (G, ·) be a finite group.

Now consider $f_a : G \to G$ defined by $f_a(x) = ax$ for all $x \in G$.

Now to prove that f_a is a Permutation.

f_a is well- defined: Let $x, y \in G$.

Suppose $x = y$

$\Longrightarrow$ $ax = ay$

$\Longrightarrow$ $f_a(x) = f_a(y)$

f_a is well-defined.

f_a is one- one : Let $x, y \in G$.

Suppose $f_a(x) = f_a(y)$

$\Longrightarrow$ $ax = ay$

$\Longrightarrow$ $x = y$

Therefore f_a is one- one.

f_a is onto : Let $x \in G$.

Since $a \in G \Longrightarrow a^{-1} \in G$

$a^{-1} \in G$, $x \in G \Longrightarrow a^{-1}x \in G$

Now $f_a(a^{-1}x) = a(a^{-1}x) = aa^{-1}(x) = ex = x$

For $x \in G$ there exists $a^{-1}x \in G$ such that $f_a(a^{-1}x) = x$

Therefore fa is onto .

Therefore fa is a Permutation on G.

Let $G' = \{ f_a / a \in G\}$ be the set of all permutations on G corresponding to every element of G.

Now to prove that G' is a group with respect to Permutation multiplication.

Since $e \in G$, $f_e \in G'$

$G' \neq \emptyset$

Closure: Let $f_a , f_b \in G'$

For every $(f_a f_b)(x) = f_a(f_b(x))$

$= f_a(bx)$

$= a(bx)$

$= abx$

$= f_{ab}(x)$

$\Longrightarrow (f_a f_b)(x) = f_{ab}(x)$ for all $x \in G$.

$f_a f_b = f_{ab} \in G'$

Associativity : Let $f_a, f_b, f_c \in G'$ for a, b, c $\in G$

$f_a(f_b f_c) = f_a(f_b f_c)$

$= f_{(ab)c}$

$= f_{ab} f_c$

$= (f_a f_b) f_c$

$f_a(f_b f_c) = (f_a f_b) f_c$

Existence of identity: Let e be the identity in G.

Let $e \in G$, $f_e \in G'$

Let $f_a \in G'$

$f_a f_e = f_{ae} = f_a$ and

$f_e f_a = f_{ea} = f_a$

Identity in G exists and it is f_e.

Existence of inverse: Let $f_a \in G'$

Since $a \in G \Longrightarrow a^{-1} \in G$

$f_a^{-1} \in G'$

$f_a f_a^{-1} = f_{aa-1} = f_e$

$f_a^{-1} f_a = f_{a-1a} = f_e$

Every element in G' is invertible and $(f_a)^{-1} = f_{a^{-1}}$

Therefore G' is a group.

Consider $\emptyset : G \rightarrow G'$ defined by $\emptyset(a) = f_a$ for $a \in G$

∅ is well- defined : Let $a,b \in G$

Suppose $a = b$

$\Longrightarrow ax = bx$

$\Longrightarrow f_a(x) = f_b(x)$

$\Longrightarrow f_a = f_b$

$\Longrightarrow \emptyset(a) = \emptyset(b)$

Therefore∅ is well-defined.

∅ is one- one : Let $a,b \in G$.

$\emptyset(a) = \emptyset(b)$

$\Longrightarrow f_a = f_b$

$\Longrightarrow f_a(x) = f_b(x)$

$\Longrightarrow ax = bx$

$\Longrightarrow a = b$

Therefore∅ is one -one.

∅ is onto : Let $f_a \in G'$

$\Longrightarrow a \in G$ and $\emptyset(a) = f_a$

For each $f_a \in G'$ there exists $a \in G$ such that $\emptyset(a) = f_a$

Therefore ∅ is onto

∅ is a Homomorphism : Let $a,b \in G$

$\emptyset(ab) = f_{ab}$

$= f_a fb$

$= \emptyset(a)\emptyset(b)$

Therefore $\emptyset$ is a Homomorphism.

The finite group G is isomorphic to the permutation group.

Thus the every finite group G is isomorphic to the permutation group.

Note : The group G' in the Cayley's Theorem is called a regular permutation group.

- **Problem : Find the regular permutation group isomorphic to the multiplicative group { 1, ω , ω²}**

Solution: We use Cayley's Theorem

If G is a group then the regular permutation group isomorphic to the group G is $\{ f_a / a \in G\}$ where $f_a : G \to G$ defined by $f_a(x) = ax$ for all $x \in G$.

Let $G = \{ 1, \omega , \omega^2\}$ be the multiplicative group then the regular permutation group isomorphic to the multiplicative group G is

$\{ f_1 , f_\omega f_{\omega^2} \}$

$$f_\omega = \begin{pmatrix} 1 & \omega & \omega^2 \\ 1.1 & 1.\omega & 1.\omega^2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \omega & \omega^2 \\ 1 & \omega & \omega^2 \end{pmatrix}$$

$$f\,\omega = \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega & \omega^2 & 1 \end{pmatrix}$$

$$f\,\omega^2 = \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega^2 & 1 & \omega \end{pmatrix}$$

- **Problem : Find the regular permutation group isomorphic to the multiplicative group { 1,-1 ,i ,-i}**

Solution: We use Cayley's Theorem

If G is a group then the regular permutation group isomorphic to the group G is { f_a/a∈G} where f_a : G → G defined by $f_a(x)$ = ax for all x∈G.

Let G ={ 1,-1 ,i ,-i} be the multiplicative group then the regular permutation group isomorphic to the multiplicative group G is

{ f_1 , f_{-1} ,f_i ,f_{-i} }

$$f_1 = \begin{pmatrix} 1 & -1 & i & -i \\ 1 & -1 & i & -i \end{pmatrix}$$

$$f_{-1} = \begin{pmatrix} 1 & -1 & i & -i \\ -1 & 1 & -i & i \end{pmatrix}$$

$$f_i = \begin{pmatrix} 1 & -1 & i & -i \\ 1 & -i & 1 & i \end{pmatrix}$$

$$f_{-i} = \begin{pmatrix} 1 & -1 & □ & -□ \\ -i & -□ & 1 & -1 \end{pmatrix}$$

Cyclic Groups

Note : Let G be a group and 'a' be an element of G. Then H = {a^n/n∈Z} is a subgroup of G. Further H is the smallest subgroup of G Which contained the element 'a'.

Cyclic subgroup generated by 'a' : Suppose G is a group and 'a' is an element of G. Then the subgroup H = $\{a^n / n \in Z\}$ is called a cyclic subgroup generated by 'a'. 'a' is called generator of H . This will be written as H = ‹a› (or) (a) (or) {a}.

Note : Let G be a cyclic groupgenerated by 'a' if O(a) = n , then an = e and { $a^1, a^2, \ldots a^{n-1}, a^n = e$} is preciously the set of distinct elements belonging to G , where 'e' is the identity in the group (G, ·).

Cyclic subgroup : Suppose G is a group and there is an element of a∈G such that G = $\{a^n / n \in Z\}$ then G is called a cyclic group and 'a' is called generator of G .We denote G by ‹a› (or) (a) (or) {a}.

Theorem: If G is a finite group and a∈G , then O(a)/O(G).

Proof : G is a finite group.

Let O(G) = m

Let H be the cyclic subgroup of G generated by'a' O(a) = n

Therefore O(H) = n

But by Lagranges theorem O(H)/O(G) ⟹ n/m

⟹ i.e., O(a)/O(G)

Note : If G is a finite group of order n and if a∈G. Then $a^n = e$

(identity in G)

Problem : Prove that (Z,+) is a cyclic group.

Solution : Given that (Z,+) is a group and 1∈Z

$1^0 = 0.1 = 0$

$1^1 = 1.1 = 1$, $1^2 = 2.1 = 2$.... etc

$1^{-1} = -1.1 = -1$, $1^{-2} = -2.1 = -2$. ..etc

1 is generator of the cyclic group (Z,+) i.e., Z =‹1›

Similarly we can prove that Z =‹-1›

Problem: Show that G = { 1 ,-1 , i , -i} the set of all fourth roots of unity is acyclic group with respect to multiplication.

Solution : Given that G = { 1 ,-1 , i , -i}

Clearly (G, ·) be a group.

$(i)^1 = i$, $(i)^2 = -1$, $(i)^3 = i^2.i = -1.i = -i$,

$(i)^4 = i^2.i^2 = -1.-1. = 1$

Thus all the elements of G are the power of $i \in G$

G is a cyclic group generated by i , G = ‹i›

Similarly we can have G = ‹-i›

Problem : Show that the set of all cube roots of unity is a cyclic group withrespect to multiplication.

Proof : The set of all cube roots of unity G = { 1, ω , ω²}

$(\omega)^1 = \omega$, $(\omega)^2 = \omega^2$, $(\omega)^3 = 1$

Then the elements of G are the power of the single element $\omega \in G$.

G is a cyclic group generated by 'ω'. i.e., G = ‹ω›

We can also have G = ‹ω²›

Problem : Show that the set nth roots of unity with respect to multiplicationis a cyclic group.

Proof : We know that $G = \{\omega^0 = 1 , \omega^1 , \omega^2 , ..., \omega^{n-1}\}$

$\omega^k = e^{2k\pi/n}$, k = 0,1,2,... (n-1) is a group under multiplication.

$(\omega)^0 = 1 = e$, $(\omega)^1 = \omega$, $(\omega)^2 = \omega.\omega = \omega^2$,

$(\omega)^3 = \omega^2.\omega = \omega^3$ ...... $(\omega^{n-1}) = \omega^{n-1}$

Thus, every element of G is some power of ω .

G is a cyclic group generated by 'ω'. i.e., G = ‹ω› .

Theorem : Every cyclic group is an abelian group.

Proof : Let G be a cyclic group generated by'a'then

$G = \{a^n/n \in Z\}$

Let a^r , $a^s \in G$, $r,s \in Z$

$a^r . a^s = a^{r+s} = a^{s+r} = a^s . a^r$

Therefore G is abelian.

Theorem : If 'a' is a generator of a cyclic group G then a^{-1} is also a generator of G.

(OR)

If G = ‹a› , then G = ‹a^{-1}›

Proof: Let G = ‹a› be a cyclic group.

If $G = \{a^n/n \in Z\}$

Let $a^r \in G$, $r \in Z$

$(a^r) = (a^{-1})^{-r}$, $-r \in Z$

Thusa^{-1} is the generator of G . i.e., G = ‹a^{-1}› .

Theorem : Every subgroup of cyclic group is cyclic.

Proof : Let G = ‹a› is a cyclic group then $G = \{a^n/n \in Z\}$.

Let H be a subgroup of G.

Then every element of H is an element of G.

Thus every element of H is of the form a^n, $n \in Z$

Let 'd' be the smallest positive integer such that $a^n \in H$.

To prove that H = ‹a^d›.

Let $a^m \in H$, where $m \in Z$.

By division algorithm, $\exists$ q,r $\in Z \ni m = dq+r$ where r = 0 (or) 0 < r < d.

Therefore $a^m = a^{dq+r} = a^{dq} . a^r = (a^d)^q . a^r \rightarrow (1)$

But $a^d \in H \Longrightarrow (a^d)^q \in H \Longrightarrow a^{dq} \in H \Longrightarrow a^{-dq} \in H$

Now a^m , $a^{-dq} \in H \Longrightarrow a^{m-dq} \in H$

$$\Longrightarrow a^r \in H$$

But $0 < r < d$ and $a^r \in H$ is a contradiction to our assumption.From (1) , therefore $r = 0$.

$$a^m = (a^d)^q$$

Therefore H is a cyclic group generated by a^d.

$$\text{i.e., } H = \langle a^d \rangle.$$

Theorem : The quotient of a cyclic group is cyclic.

Proof : Let $G = \langle a \rangle$ be a cyclic group with 'a' as generator.

Let N be a subgroup of G.

Since G is abelian.

Therefore N is normal in G.

We know that $G/N = \{Nx / x \in G\}$.

Now , $a \in G$, $Na \in G/N \Longrightarrow \langle Na \rangle \subseteq G/N \rightarrow (1)$

Also, $Nx \in G \Longrightarrow x \in G = \langle a \rangle$

Therefore $x = a^n$ for some $n \in Z$.

$Nx = Na^n = N$ (a ,a , ...a(n times))

= (Na)(Na) ....(Na)(n times)

$= (Na)^n$

Therefore $Nx \in G/N \Longrightarrow Nx \in \langle Na \rangle$

Therefore $G/N \subseteq \langle Na \rangle \rightarrow (2)$

From (1) & (2) $G/N = \langle Na \rangle$

i.e., quotient group of a cyclic group is cyclic.

Theorem : If P is a prime number then every group of order p is cyclicgroup i.e., a group of prime order is cyclic.

Proof : Let P ≥2 be a prime number.

Let G be a group of order p.

Claim : G is a cyclic group.

O(G) = p then there exists at least one element a other than element e in G.

‹a› is cyclic subgroup of G.

$a \neq e$, $a \in$‹a›

‹a› ≠ ‹e›

O(‹a›) = h

By Lagranges theorem, O(‹a›)/O(G) i.e., h/p

h = 1 (or) h = p

‹a› ≠ ‹e›.

Therefore h = p

O(‹a›) = O(G)

G = ‹a›

G is a cyclic group.

Theorem : The order of a cyclic group is equal to the order of its generator.

Proof : Let G be a cyclic group generated by'a'. i.e., G = ‹a›

(i) Let O(a) = n, n is finite number then $e = a^0$, a^1, a^2,...$a^{n-1} \in G$

Now we prove that this elemens are distinct and this are the only elements of G such that O(G) = n .

Let i,j (≤(n-1)) be two non-negative integer such that $a^i = a^j$ for $i \neq j$.

Now either i > j (or) i < j

Suppose i > j

Then $a^i a^{-j} = a^j a^{-j}$

$a^{i-j} = a^{j-j}$

$a^{i-j} = a^0 = e$ and $0 < (i-j) < n$

But this contradiction the fact that $O(a) = n$

Therefore $a^i \neq a^j$

Therefore a^0, a^1, a^2 , ...are all distinct.

Consider any $a^p \in G$, where p is any integer.

By Euclid's algorithm , $\exists$ q,r $\in Z \ni p = nq+r$ where $0 \leq r \leq n$.

Then $a^p = a^{nq+r} = a^{nq} .a^r = (a^n)^q.a^r = a^q.a^r = e. a^r = a^r$

But a^r is on of $a^0 , a^1, a^2,...a^{n-1}$

Hence each $a^p \in G$ is equal to one of the elements $a^0 , a^1, a^2,...a^{n-1}$ i.e., $O(G) = n = O(a)$.

(ii) Let O(a) be infinite.

Let m ,n be two positive integers such that $a^m = a^n$ for $m \neq n$.

Suppose $m > n$

Then $a^m a^{-n} = a^n a^{-n}$

$a^{m-n} = a^{n-n}$

$a^{m-n} = a^0 = e$

$\Rightarrow$ O(a) is finite

It is a contradiction to the fact that O(a) is infinite.

Therefore $a^m \neq a^n$ for $m \neq n$.

Hence , G is of infinite order .

Thus from (1) & (2) ,

The order of a cyclic group is equal to the order of its generator.

Note : A cyclic group of order n has ∅(n) generators.

Problem : Show that the group G = ({ 1,2,3,4,5,6}×7) is cyclic also writedown all its generators.

Solution : Clearly O(G) = 6

If there exists an element a∈G such that O(a) = 6

Then G is cyclic group with generator 'a'

$3^1 = 3$, $3^2 = 3\times_7 3 = 2$, $3^3 = 3^2\times_7 3 = 6$, $3^4 = 3^3\times_7 3 = 4$,

$3^5 = 3^4\times_7 3 = 5$, $3^6 = 3^5\times_7 3 = 1$,the identity element

Therefore G is a cyclic group with generator 3.

Since 5 is relatively prime to 6, 3^5 is a generator of G.

i.e., '5' is a generator of G.

Note : If n = $P_1\alpha1$,$P_2\alpha2$,...P_k. αk where P_1, P_2,.... P_k are all prime factors of n then ∅(n) = n(1- 1/P_1) (1- 1/P_2)... (1- 1/P_k)

Problem : Find the number of cyclic groups of orders 5 , 6 , 8 , 12 , 15 , 60.

Solution : O(G) = 5 the number of generators of

G = ∅(5) = 5(1- 1/5) = 5(4/5) = 4.

O(G) = 6, the number of generators of

G = ∅(6) = 6(1- 1/2) 1- 1/3) = 6(1/2) (2/3) = 2.

O(G) = 8, the number of generators of

G = ∅(8) = 8(1- 1/2) = 4

O(G) = 12, the number of generators of

G = ∅(12) = 12(1- 1/2) (1- 1/3) = 12(1/2)(2/3) = 12(1/6) = 4

O(G) = 15, (3 ,5 are the only prime factors of 15)

the number of generators of

G = $\emptyset(15) = 15(1- 1/3)(1- 1/5) = 15(2/3)(4/5) = 8$

O(G) = 60, (2, 3 ,5 are the only prime factors of 60)

the number of generators of

G = $\emptyset(60)$

$= 60(1- 1/2)(1- 1/3)(1- 1/5)$

$= 60(1/2)(2/3)(4/5)$

$= 16.$