Unit -I

Group:

Definition:-

A non-empty set 'G' together with a binary operation $* : G \times G \to G$ is called a group if the following condition are satisfied

i) $*$ is associative (ie) $a*(b*c) = (a*b)*c$

$\forall a, b, c \in G$.

ii) Existence of identity:

$\exists$ an element $e \in G$ s.t

$a*e = e*a = a \ \forall a \in G$

e is an identity

iii) Existence of inverse.

$\forall a \in G$

$\exists$ an element $a' \in G$

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

a' is inverse of a.

Eg: 1.) Z, Q R and C are group under addition.

2) The set of all 2x2 matrices $\begin{pmatrix} a & b \\ c & a \end{pmatrix}$ where $a, b, c, d \in R$ is group under matrix addition.

$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is an identity

Scanned with CamScanner

i) Identity element of G is unique

ii) for any $a \in G$, the inverse of a is unique

Proof:-

i) let e and e' be two identity element of G.

consider e as an indentity

$$e'e = ee' = e'$$

Consider e' as an identity

$$ee' = e'e = e$$

$$\boxed{e = e'}$$

identity of group G is unique

ii) let a' and a'' be inverse of a consider a' inverse of a. let be e as an identity

$$aa' = a'a = e$$

Consider a''

$$aa'' = a''a = e$$

$$a' = a'e = a'(aa'')$$

Since 'G' is group we have

$$a' = (a'a)a''$$

Scanned with CamScanner

Theorem 3.2

In a group left & Right Cancellation laws hold

ie) $ab = ac \Rightarrow b = c$

$ba = ca \Rightarrow b = c$

Proof:

Now consider

$ab = ac$

Pre-multiplying a^{-1} on both side since in a group inverse exists a^{-1} is a inverse of a

$a^{-1}(ab) = a^{-1}(ac)$

since ∃ associatively

$(a^{-1}a)b = (a^{-1}a)c$ [∵ associative law]

$eb = ec$ [identity law]

Since e is identity

$b = c$

ii'y

$ba = b$

By past multiplying a^{-1} on both side

$(ba)a^{-1} = (ca)a^{-1}$ [associative law]

$b(aa^{-1}) = c(aa^{-1})$ [∵ identity law]

$b(e) = c(e)$

$b = c$

we proved that $ba = ac$

$b = c$

Scanned with CamScanner

Theorom 3.3

let 'G' be a group and $a, b \in G$ Then the equations $ax = b$ & $ya = b$ have unique solutions for x and y in G

Proof:

let we consider $x = a^{-1}b \in G$

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

$$= (aa^{-1})b \quad [\because \text{Associative Property}]$$

$$ax = eb$$

$$ax = b$$

To Prove the uniqueness

let x_1 and x_2 be the two soln of

$$ax = b$$

$$ax_1 = b \text{ & } ax_2 = b$$

$$ax_1 = ax_2$$

$$x_1 = x_2 \quad [\text{By left cancellation law}]$$

$x = a^{-1}b$ is a unique soln for $ax = b$

ii') let we consider $y = a^{-1}b \in G$

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

$$ya = b(aa^{-1}) \quad [\because \text{Associative Property}]$$

$$ya = eb$$

$$ya = b$$

Scanned with CamScanner

$y_1 a = b$ & $y_2 a = b$

$y_1 a \cdot y_2 a$

$y_1 = y_2$ [∵ By Right cancellation]

$y = a^{-1} b$ is a unique soln $ya = b$

Theorem 3.4

Let G be a group let $a, b \in G$ then $(ab)^{-1} = b^{-1} a^{-1}$ and $(a^{-1})^{-1} = a$

Proof:

Now consider

$(ab)(b^{-1} a^{-1}) = a(bb^{-1})a^{-1}$ (By associative)

$= a(e)a^{-1}$ (By inverse]

$= aa^{-1}$ (since e identity)

$(ab)(b^{-1} a^{-1}) = e$ By (inverse Property)

again,

$(b^{-1} a^{-1})(ab) = b^{-1}(a^{-1}a)b$ [By Associative]

$= b^{-1} eb$ [By inverse Property]

$= b^{-1} b$ [since e identity]

$= e$

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

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

Now

(i) $(a^{-1})^{-1} a^{-1} = e$

By post multiply a on both sides

Scanned with CamScanner

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

$e(a^{-1})^{-1} = ae$ [Inverse property

$(a^{-1})^{-1} = a$ [Since e is identity

Scanned with CamScanner

Corallary:-

If $a_1, a_2, \ldots a_n \in G$ then $(a_1 a_2 \ldots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1}$

Definition

let 'G' be a group and $a \in G$ For any the integer n, we define

$a^n = aa \ldots a$ (a written n times)

Clearly

$$(an)^{-1} = (aa \ldots a)^{-1}$$
$$= a^{-1} a^{-1} a^{-1} \ldots a^{-1}$$
$$= (a^{-1})^n$$

we know define

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

Finally we define $a^0 = e$

Thus a^n is defined for all integers n

Note:-

when the library operations on 'G' is '+' we denote $a+a+\ldots+a$ (a written n times) as na

Problems:-

D S.T in a group G $x^2 = x$ iff $x = e$

Proof

let we consider $x = e$

$$x^2 = e^2 = e \cdot e = e = x$$

$$x^2 = x$$

Scanned with CamScanner

To prove converse part

let $x^2 = x$

$x\ x = x\ e$ (e is said)

$x = e$ (By left cancellation)

Idempodent :-

An element $a \in G$ is called an Idempodent, If $a^2 = a$

In a Group 'G' the identity element is the only Idempodent element

Problems:

2. In an abelian group $(ab)^2 = a^2 b^2$

Soln L.H.S

$(ab)^2 = (ab)(ab)$

$= a(ba)b$ (Associative law)

$= a(ab)b$ (Abelian)

$= (aa)(bb)$ (Associative)

$= a^2 b^2$

L.H.S = R.H.S

3. let 'G' be a group such that $a^2 = e \ \forall\ a \in G$ Then G is abelian

Soln $a^2 = e \quad \forall\ a \in G$

$a^2 = e$

$aa = e$

$\times a^{-1}$ on both side

Scanned with CamScanner

$a(a\ a^{-1}) = ea^{-1}$ (Inverse)

$ae = ea^{-1}$

$a \cdot a^{-1}$ (e · identity)

Now: let $a, b \in G$

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

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

$\boxed{ab = ba^{-1}}$

Hence commutative property is satisfied

Hence 'G' is abelian.

4. let 'G' be a group in which $(ab)^m = a^m b^m$ for 3 consective Integers and for all $a, b \in G$ Then 'G' is abelian

Soln

let $a, b \in G$

let $(ab)^m = a^m\ b^m$

$(ab)^{m+1} = a^{m+1}\ b^{m+1}$

$(ab)^{m+2} = a^{m+2}\ b^{m+2}$

Now,

$(ab)^{m+1} = a^{m+1}\ b^{m+1}$

$(ab)^m (ab) = (a^m \cdot a)(b^m \cdot b)$

$(a^m \cdot b^m)(ab) = (a^m \cdot a)(b^m \cdot b)$

$a^m \cdot b^m\ ab = a^m \cdot a\ b^m \cdot b$

By Pre - multiply a^{-m} and post multiplying b^{-1}

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

Scanned with CamScanner

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

By (Associative)

$e\, b^m a\, e = e a b^m e$ (By inverse)

$$b^m a = a b^m$$

Ily,

$(ab)^{m+2} = a^{m+2}\, b^{m+2}$

$\Rightarrow b^{m+1} a = a b^{m+1}$

$b^m b a = a b^m b$

$b^m ba = b^m ab$ (by ①)

$ba = ab$ (By left can)

5. let $(H, \cdot)$ and $(K, *)$ be groups we define a binary operations $\square$ on $H \times K$ by $(h_1, k_1) \square (h_2, k_2) = (h_1 h_2, k_1 * k_2)$. Then $H \times K$ is a group.

To prove:

$(H \times K, \square)$ is a group

Proof.

Association property

let $(h_1, k_1), (h_2, k_2), (h_3, k_3) \in H \times K$

$[(h_1, k_1) \square (h_2, k_2)] \square (h_3, k_3)$

$= (h_1 h_2, k_1 * k_2) \square (h_3, k_3)$

$= ((h_1 h_2) h_3, (k_1 * k_2) * k_3)$

Since H and K are group the associative Property

Scanned with CamScanner

$= (h_1 (h_2 h_3), k_1 * (k_2 * k_3))$

$= (h_1, k_1) \square (h_2 h_3, k_2 * k_3)$

[By hypothesis]

$= (h_1 k_1) \square [(h_2, k_2) \square (h_3, k_3)]$

Hence Associative property is satisfied

Identity element:-

let e be identity element in H and e_1 be identity element in K

Now we've to show (e, e_1) is identity of $H \times K$

let $(h_1, k_1) \in H \times K$

Then

$(h_1, k_1) \square (e, e_1) = (h_1 e, k_1 \times e_1)$

$= (h_1, k_1)$ [since e & e_1 is Identity]

$(e, e_1) \square (h_1, k_1) = (eh_1, e_1 * k_1)$

$= (h_1, k_1)$

$(h_1, k_1) \square (e, e_1) = (e, e_1) \square (h_1, k_1) = (h_1, k_1)$

(e, e_1) is an Identity element.

Inverse identity:.

let h^{-1} be inverse to $h \in H$ and k^{-1} be inverse of $k \in K$

we've to show

(h^{-1}, k^{-1}) be inverse of $(h, k) \in H \times K$

Scanned with CamScanner

Scanned with CamScanner

$(h, k) \square (h^{-1}, k^{-1}) = (hh^{-1}, k * k^{-1})$

$= (e, e_1)$ (Inverse Property)

$(h^{-1}, k^{-1}) \square (h, k) = (h^{-1}h, k^{-1} * k)$

$= (e, e_1)$

(h^{-1}, k^{-1}) is inverse of (h, k)

$\therefore$ $H \times K$ is Group

Note:-

$H \times K$ is the direct Product of H & K.

Theorem : 3.5

i) $a^m a^n = a^{m+n}$ ..., $m, n \in Z$

ii) $(a^m)^n = a^{mn}$ ..., $m, n \in Z$

Proof

We may prove this by induction.....

(i) when $n = 0$

$a^m a^0 = a^m$

$a^{m+n} = a^m$

The result (i) is obviously true for $n = 0$

when $m \geq 0$. $a^{m+1} = a^m a^1$ (by definition)

when $m = -1$, L.H.S $\Rightarrow a^{m+1} = a^0 = e$

R.H.S $a^m a^1 = a^{-1} a = e$

$\therefore$ $\rightarrow a^{m+1} = a^m a^1$

when $m \leq -2$, let $m = -p$ $p > 2$

$a^m a = a^{-p} a = (a^{-1})^p a$ [$a^{-m} = (a^{-1})^m$]

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

$= (a^{-1})^{p-1} e$

Scanned with CamScanner

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

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

$= a^{p+1}$

$(a^m)\, a = a^{m+1}, \forall m \in \mathbb{Z}$

Hence the result is true for $n=1$

let we assume that the theorem is valid for $n = k+1$

$$a^m a^k = a^{mk} \rightarrow (1)$$

Now for $n = k+1$

$$a^m a^{k+1} = a^m (a^k\, a)$$

$= (a^m\, a^k).a$ (By Associative property)

$= a^{mk}\, a$ (By (1))

$= a^{mk+1}$

$$a^m a^{k+1} = a^{mk+1}$$

This show that the result is true for $n = k+1$

Hence by induction method the theorem holds for all +ve values of n ∈ N

If $n \neq 0$, we can prove the same result by Induction on $-n$

Scanned with CamScanner

Scanned with CamScanner

ii) $(a^m)^n = a^{mn}$, $m, n \in \mathbb{Z}$

Proof

We may know prove this by induction as in'

i) when $n = 0$

$(a^m)^0 = 1$

$a^{m \cdot 0} = 1$

The result (2) is obviously true for $n = 0$ when $m \geq 0$, $(a^m)^1 = a^{(m)(1)}$ (by definition)

when $m = 1$ $(a^m)^1 = (a^1)^1 = a^1$

$a^m = a^1$

$\therefore (a^m)^1 = a^m$

When $m \neq 0$, let $m = p$ $p \geq 0$

$(a^m)^1 = (a^p)^1 = (a^1)^1 = (a^1)^p = a^p$

$= a^{1 \cdot p}$

$= a^p$

$(a^m)^1 = a^m$ if $m \neq 0$

Hence the result is true for $n = 1$

Let we assume that the theorem is Valid for

Scanned with CamScanner

Equivalent

$n = k > 1$,

$(a^m)^k = a^{mk}$

Now for $n = k+1$

$\therefore (a^m)^{k+1} = a^{(m)(k+1)}$

This shows that result is true for $n = k+1$

Hence by induction Method the theorem hold for all the value of $n \in Z$.

Ily for $n < 0$ we can prove that same result by induction on $-n$.

Scanned with CamScanner

Scanned with CamScanner

Equivalent Definitions of a group

Definition:

let $*$ be a binary operation defined on G. An element $e \in G$ is called a left identity if $e * a = a$ for all $a \in G$.

'e' is called a right identity if $a * e = a$ for all $a \in G$.

Examples:

In 'R' we define $a * b = ab^2$. Here a 1 and -1 are right identities.

In 'C' We define $z_1 \circ z_2 = |z_1| z_2$. Here all element z such that $|z| = 1$ are left identities.

Definition:-

let $*$ be a binary operation defined on G. let $e \in G$ be the identity element Let $a \in G$. An element $a' \in G$ is called a left inverse of a if $a' * a = e$ a' is called a right inverse of a if $a * a' = e$

Theorem 3.6

Let G be a non-empty set with an associative binary operation defined on it such that there exists a left identity e in G and each element $a \in G$ has a left inverse a' with respect to e. Then 'G' is group

Scanned with CamScanner

Proof:

Given:

'a' is left inverse of a with respect to 'e' so that

$$a'a = e \quad (1)$$

let a'' be the left inverse of a' in G

$$a''a' = e \quad (2)$$

then,

$aa' = e(aa')$ → (since 'e' is left identity)

$= (a''.a')(aa')$ → [by eqn (2)]

$= a''(a'a)a'$ → [By Associative]

$= a''(ea')$ → [By equation (1)]

$= a''a'$ → [since 'e' is left identity]

$aa' = e$ → [By equation (2)]

∴ a' is the right inverse of a

Hence Inverse property satisfied

Also,

$a = ea$ → [left identity]

$= (aa')a$ → [By equation (3)]

$= a(a'a)$ → [By Associative law]

$= ae$ → [By eqn (1)]

$a = ae$

∴ e is a right identity

$a'a = aa' = e$

$ea = ae = a$

Hence 'G' is a group

Scanned with CamScanner

Theorem 3.7

Let 'G' be a non-empty set with an associative binary operation defined on it such that there exists a right identity e in G and each element $a \in G$ has a right inverse a' with respect to e. Then 'G' is a group

Soln Given the,

a' is right inverse of a with respect to e

So That,

$$aa' = e \rightarrow (1)$$

Let a'' is right inverse of a' in G

$$a'a'' = e \rightarrow (2)$$

Then

$$a'a = (aa')e \quad \text{(since 'e' is right identity)}$$

$$= (a'a)(a'a'') \quad \text{(By (2))}$$

$$= a'(aa')a'' \quad \text{(By associative)}$$

$$= a'ea'' \quad \text{(By (1))}$$

$$= a'a'' \quad \text{(since e is right identity)}$$

$$a'a = e \rightarrow (3) \quad \text{by (2)}$$

$\therefore a'$ is the left inverse of a

Hence inverse property satisfied

Also,

$$a = ae \quad \text{(e is right identity)}$$

$$= a(a'a) \quad \text{(By (3))}$$

$$= (aa')a \quad \text{(By association)}$$

Scanned with CamScanner

$= ea$ (By (1))

$a = ea$

e is a left identity of a

$\Rightarrow a'a = aa'$

$= e$

$= a$

Hence 'G' is a group.

Scanned with CamScanner

Scanned with CamScanner

Theorem 3.8

Let G be an non-empty set with an association binary operation defined on it such that the equations $ax=b$ and $ya=b$ have unique solutions for x and y in G. Then 'G' is a group.

Proof:

Let $a \in G$

Then $\exists$ a unique $e \in G$

$\ni$ $ea=a$ → (1)

Now, let $b \in G$

Then $\exists$ a unique soln x in G

$\ni$ $ax=b$ → (2)

Now,

$eb = e(ax)$ → (by (2))

$= (ea)x$ → [by Associative]

$= ax$ → [By equation (1)]

$\boxed{eb = b}$ → [By equation (2)]

∴ e is left identity in G

Let $a \in G$

Then $ya=b$ has unique solution a'

$(ba')a = b$

$b(a'a)=b$ → [By Associative]

$b^{-1}b(a'a) = b^{-1}b$ → [Pre Multiply by b^{-1}]

$e(a'a)=e$ → (e left identity)

$a'a = e$

a' is the left inverse of a in G

Scanned with CamScanner

Hence by known theorem,

" Let 'G' be a non-empty set with an associative binary operation defined on it such that ∃ be a left identity e in G and each element a ∈ G has a left identity inverse a' with respect to e. Then 'G' is a group "

∴ Here ∃ left identity and left Inverse for given 'G' defined on Associative binary operation

Hence 'G' is group

Theorem 3: 9

let 'G' be an finite set with an associative binary operation defined on G in which both cancellation laws hold good. G is group

Proof:.

let $G = \{a_1, a_2, \ldots, a_n\}$

let $a, b \in G$

Consider the elements,

$aa_1, aa_2, aa_3, \ldots, aa_n$

All these elements are distinct. for if

$aa_r = aa_s$

$a_r = a_s$ (left cancellation law)

Hence $aa_1, aa_2, \ldots, aa_n$ are

Just the elements of $a_1, a_2, \ldots, a_n$

- same order and

Scanned with CamScanner

Hence $aa_i = b$ for some i

Hence this will be in the form of $ax = b$

Thus the equations $ax = b$ has a unique a soln for x in G

II'y Taking the elements

$a_1a, a_2a, \ldots, a_na$

All these elements are distinct, for

$a_ra = a_sa$

$a_r = a_s$ [right cancellation law]

Hence $a_1a, a_2a, \ldots, a_na$ are just the elements of $a_1, a_2, \ldots a_n$ of G in some order and

Hence $a_ia = b$ for some i

Hence this will be in the Form of $xa = b$

Thus the equation $xa = b$ has a unique solution for x in G

Hence by the known theorem

let G be a non-empty set with an associative binary operation defined on it such that $\exists$ be a left identity e in G and each element $a \in G$ has a left inverse a' with respect to e Then 'G' is a group".

Scanned with CamScanner

Proof:

let $x, y \in C^*$

Then $x = ai + b$

where a & b are not simultaneously zero

now $xy = (a+ib)(c+id)$

$= ac + aid + ibc + i^2 bd$

$= (ac - bd) + i(ad + bc)$

we have to prove that $ac - bd$ and $ad + bc$ are not simulatenously zero

Suppose $ac - bd = 0 \rightarrow (1)$ and

$ad + bc = 0 \rightarrow (2)$

$(1) \times d \Rightarrow acd - bd^2 = 0 \rightarrow (3)$

$(2) \times c \rightarrow acd + bc^2 = 0 \rightarrow (4)$

Solving (3) & (4)

$(4) \Rightarrow adc + bc^2 = 0$

$(3) \Rightarrow adc - bd^2 = 0$

Scanned with CamScanner

Scanned with CamScanner

$\therefore$ either $b=0$ (or) $c^2+d^2=0$

$\therefore$ either $b=0$ (or) ($c=0$ and $d=0$)

Similarly either $a=0$ (or) ($c=0$ and $d=0$)

Thus ($a=0$ and $b=0$) or ($c=0$ and $d=0$)

$\therefore x=0$ (or) $y=0$ which is contradiction

Hence $xy \in C^*$

Now let $x=a+ib$, $y=c+id$ and $z=e+if$

Then $x(yz) = (a+ib)[(c+id)(e+if)]$

$= (a+ib)[(e-df)+i(dc+cf)]$

$= ace - adf + ibce - ibdf + iade + iacf + i^2bde + i^2bcf$

$= (ace - adf - bde - bcf) + i(bce - bdf + ade + acf)$

n'y

$(xy)z = ((a+ib)(c+id))(e+if)$

$= [ac+iad+ibc-bd](e+if)$

$= ace + iade + ibce - bde + iacf + i^2adf + i^2bcf - ibdf$

$= (ace - bde - adf - bcf) + i(ade + bce + acf - idf)$

Hence $x(yz) = (xy)z$

It satisfied the associative property

Scanned with CamScanner

Permutation Groups:-

Let A be a finite set A bijection from A to itself called permutation.

Example:-

$A = \{1, 2, 3, 4\}$

$f : A \to A$ given by

$f(1) = 2,\ f(2) = 1,\ f(3) = 4,\ f(4) = 3$

we shall write thus permutations as

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

An element in the bottom row image of the element just above it in the upper row

Note:

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

Hence any rearrangement of columns in a permutation is immaterial

Symmetric group:

Let A be a finite set comain be elements. The set all permutation of A is clearly a group and the composition of function this group is called the

Scanned with CamScanner

Symmetric group of degree n and is denoted by S_n

Example:-

$A = \{1, 2, 3\}$, then S_3 consists of

$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$: $P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

	e	P_1	P_2	P_3	P_4	P_5
e	e	P_1	P_2	P_3	P_4	P_5
P_1	P_1	P_2	e	P_4	P_5	P_3
P_2	P_2	e	P_1	P_5	P_3	P_4
P_3	P_3	P_4	P_5	e	P_2	P_1
P_4	P_4	P_3	P_5	P_1	e	P_2
P_5	P_5	P_4	P_3	P_2	P_1	e

$eP_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = P_1$

$eP_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = P_2$

$P_1 P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = P_2$

Scanned with CamScanner

$P_1 P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$

$P_1 P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = P_4 \quad P_1 P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = P_5$

$P_1 P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = P_3 \quad P_2 P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$

Scanned with CamScanner

Scanned with CamScanner

Definition

Let G be a finite group then the number of elements in G is called the order of G and is denoted by |G| or o(G)

Definition:.

Let p be a permutation on $A = \{1, 2, \ldots, n\}$. p is called a cycle of length r if there exists distinct symbols $a_1, a_2, \ldots a_r$ such that $p(a_1) = a_2, p(a_2) = a_3, \ldots p(a_{r-1}) = a_r$ and $p(a_r) = a_1$, and $p(b) = b$ for all.

$$b \in A - \{a_1, a_2, \ldots, a_r\}$$

This cycle is represented by the symbol $(a_1, a_2, \ldots a_r)$. Thus under the cycle $(a_1, a_2, \ldots a_r)$ each symbol is mapped onto the following symbol except the last one which is mapped onto the first symbol and all the other symbols not in the cycle and fixed.

Scanned with CamScanner

Definition:

Two cycles are said to be disjoint if they have no symbols in common

Definition

A cycle of length two is called a transposition. Thus a transposition $(a_1\ a_2)$ interchanges the symbols a_1 and a_2 and leaves all the other elements fixed.

Definition:-

A permutation $p \in S_n$ is called even or odd according as p can be expressed as a product of an even number of transposition or an odd number of transposition respectively.

definition

even or odd alternative group of 'n' symbols.

The group A_n of all even permutation, in S_n called the alternative

Scanned with CamScanner

Scanned with CamScanner

group of 'n' symbols.

length of cycle

let $A = \{1, 2, 3, 4, 5\}$ consider the cycle of length 4 given by $p = (2\ 4\ 5\ 1)$

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

$e = (2\ 4\ 5\ 1) = (4\ 5\ 1\ 2) = (5\ 1\ 2\ 4)$

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

Theorem 3.10

Any permutation can be expressed as a product of disjoint cycles

proof:

let p be a given permutation of the set $S = (1, 2, \ldots, n)$.

let us start with any symbol $a_1 \in S$

let $p(a_1) = a_2$, $p(a_2) = a_3$ .. . Since 'S' is finite, those symbols cannot all the distinct and hence there exists a least positive integer 'r' such that $1 \leq r \leq n$ and $p(a_r) = a_1$.

let $c = (a_1, a_2 \ldots a_r)$. If $r = n$ then $p = c$ so that 'p' is a cycle. If $r < n$, let b_1 be a symbol in 'S' such that $b_1 \notin (a_1, a_2, \ldots a_r)$

Starting with b_1 we can construct the cycle $d = (b_1 b_2 \ldots b_s)$ as before

Scanned with CamScanner

Clearly the cycles c and d are disjoint. If $r+s = n$ then $p = cd$.

If $r+s < n$ we repeat the above process to obtain more cycles untill all the symbols appears in one of the cycles thus we get a decomposition of p into disjoint cycles.

Definition

A cycle of length two is called a transposition Thus a transposition (a_1, a_2) interchanges the symbols a_1 and a_2 and leaves all the other elements fixed

Theorem 3.11

Any permutation can be expressed as a product of transportation

Proof

Since any permutation is a product of disjoint cycles it is enough if we prove that each cycle is a product of transportation. transposition

Hence let $c = (a_1 a_2 \dots a_r)$ be a cycle

clearly $(a_1 a_2 \dots a_r) = (a_1 a_2)(a_1 a_3) \dots (a_1 a_r)$

This prove the theorem

Scanned with CamScanner

Example:

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

Soln

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

$= (12)(14)(15)$

Also $(1245) = (2451) = (24)(25)(21)$

Thus the representation of a permutation as a product of transpositions is not multiple

2 $(1345)(26)$

Soln

$(1\ 3\ 4\ 5)(26) = (13)(14)(15)(16)$

$= (13)(12)(12)(14)(15)(21)$

Thus in the representation of a permutation as a product of transposition one can always insert $(ab)(ab)$ in any place since $(ab)(ab)$ is the identity permutations.

Theorem 3.12

If a permutation $p \in S_n$ is a product of 'r' transpositions and also a product of 's' transpositions then either r and s are both even or both odd

Scanned with CamScanner

Proof:

let $p = t_1 t_2 \ldots t_r = t_1' t_2' \ldots t_s'$ where t_i, t_i' are transpositions. Now consider the polynomial in n variables $x_1, x_2, \ldots x_n$ given by

$$\Delta = (x_1 - x_2)(x_1 - x_3) \ldots (x_1 - x_n)$$
$$\times (x_2 - x_3)(x_2 - x_4) \ldots (x_2 - x_n)$$
$$\ldots\ldots\ldots$$
$$\ldots\ldots\ldots$$
$$\times (x_{n-1} - x_n) = \prod_{i<j} (x_i - x_j)$$

For any permutation $p \in S_n$ we define

$$p(\Delta) = \prod_{i<j} (x_{p(i)} - x_{p(j)})$$

Consider the transposition $t = (ij)$. Then the factor $x_i - x_j$ in Δ becomes $x_j - x_i$. Any factor $(x_k - x_l)$ of Δ in which neither i nor j is equal to k or l is unchanged. All other factors of Δ can be paired to form products of the form $\pm (x_i - x_k)(x_l - x_j)$ the sign being determined by the relative magnitudes of i, j and k.

Since 't' interchanges x_i and x_j any such product is unchanged.

Hence the effect of the transposition 't' on Δ is just to change the sign of Δ ie, $\tau(\Delta) = -\Delta$

Scanned with CamScanner
Scanned with CamScanner

$P(\Delta) = (t_1 t_2 \ldots t_r)(\Delta) = (-1)^r \Delta$

Also $P(\Delta) = (t_1' t_2' \ldots t_s')(\Delta) = (-1)^s \Delta$

$\therefore (-1)^r = (-1)^s \Rightarrow r$ and s are both even or both odd.

Definition:-

A permutation $p \in S_n$ is called even or odd according as p can be expressed as a product of an even number of transposition or an odd number of transpositions respectively

Example:

Consider the permutation

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

Soln

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

$p = (134)(26)(57) = (13)(14)(26)(57)$

$\therefore$ Hence p is a product of 4 transpositions

Hence p is an even permutation

2 Consider the permutation

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 4 & 3 & 6 & 1 & 7 & 9 & 8 \end{pmatrix}$$

Soln

Scanned with CamScanner

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 4 & 3 & 6 & 1 & 7 & 9 & 8 \end{pmatrix}$$

$p = (1256)(34)(89) = (12)(15)(16)(34)(89)$

$\therefore$ p is a product of '5' transposition

Hence 'p' is an odd permutation

Theorem 3.13

i) The product of two even permutation is an even permutation

ii) The product of two odd permutation is an even permutation

iii) The product of an even permutation and an odd permutation is an odd permutation

iv) The inverse of an even permutation is an even permutation.

v) The inverse of an odd permutation is an odd permutation.

vi) The identity permutation of the e is an even permutation.

proof

let P_1, P_2 be two permutation. If P_1 is product of r transposition and P_2 is a product of s transpositions.

Then $P_1 P_2$ is a product of r+s

Scanned with CamScanner

transposition

Hence (i)(ii) and (iii) follow

Now suppose that a permutations p is a product of r transposition say, $P = t_1, t_2 \ldots t_r$ Then

$$p^{-1} = (t_1, t_2 \ldots t_r)^{-1}$$
$$= t_r^{-1} \ldots t_2^{-1} t_1^{-1} = t_r \ldots t_2 t_1$$

p^{-1} is also a product of r transpositions

This proves (iv) and (v)

Now, $e = (12)(12)$ and hence e is an even permutation which proves (vi)

Theorem 3.14

let A_n be the set of all even Permutation in S_n. Then A_n is a group containing $\frac{n!}{2}$ permutations

Proof.

From (i), (iv) and (vi) of theorem 3.13 we see that A_n is a group

Now let B_n be the set of all odd permutation in S_n.

Define: $A_n \to B_n$ by $f(P) = (12)P$

f is 1-1, for $f(P_1) = f(P_2) \Rightarrow$

$$(12)P_1 = (12)P_2 \Rightarrow P_1 = P_2.$$

f is onto, for if $\alpha \in B_n$ then $(12)\alpha \in A_n$

Scanned with CamScanner

and $f[(12)\alpha] = (12)(12)\alpha = \alpha$

Thus f' is a bijection and hence the number of odd permutation in S_n = the number of permutations in S_n. Since S_n contains $n!$ permutations, A_n has $\frac{n!}{2}$ elements.

Definition:

The group A_n of all even permutations in S_n is called the alternating group on 'n' symbols.

Scanned with CamScanner

Scanned with CamScanner

Normal subgroups and Quotient groups

Definition :

A subgroups 'H' of 'G' is called a normal subgroup of 'G' if $aH = Ha$ for all $a \in G$

Example

For any group G, $\{e\}$ and G are normal subgroups

Theorem 3.39

Every subgroup of a abelian group is a normal subgroup

proof:

Let 'G' be an abelian group

Let 'H' be a subgroup of 'G'

Let $a \in G$

We claim that. $aH = Ha$

Now let $x \in aH$

Then $x = ah$ where $h \in H$

Since H is a subgroup of 'G' Then $h \in G$

Since $a, h \in G$

'G' is an abelian group

$x = ha$

$x \in Ha \rightarrow (1)$

$aH \subseteq Ha \rightarrow (1)$

Hence

Let $y \in Ha$

Then $y = ha$ where $h \in H$

Since 'H' is a subgroup of G. Then $h \in G$

Since $a, h \in G$

G is an abelian group

$y = ah$

$y \in ah$

Scanned with CamScanner

Scanned with CamScanner

Theorem 3.18 Unit-2

let H be a non-empty finite subset of G If 'H' is closed under the operation in G then H is a subgroup of G

proof

$H \neq \phi \subset G$

let $a \in H$

Since H is closed

$a, a^2, a^3, \ldots a^n, \ldots$ are all elements of H.

But Since 'H' is finite the elements $a, a^2, a^3 \ldots$ cannot all be distinct

let $a^r = a^s$, $r < s$

$a^{s-r} = e \in H$

$\therefore e \in H$ is an identity element

Now

$a \in H$

We've proved that

$a^n = e$

$a a^{n-1} = e$

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

$a^{-1} = a^{n-1} \in H$

a^{-1} is inverse of $a \in H$

Scanned with CamScanner

Theorem 3.19

If H and k are subgroups of a groups G then is $H \cap k$ is also a sub group of G.

Proof:

let $e \in G$ be an identity element of G.

W.k.T

The identity e of G is in subgroup H.

$\therefore$ e is an identity element $H \& K$

Since $H \& K$ subgroup of G

$\therefore e \in H \cap K$

Therefore,

$H \cap k$ is non-empty subset of G.

Now, let $a, b \in H \cap k$

Then $a, b \in H \&$

$a, b \in k$

Since 'H' is subgroup of G.

$\therefore ab^{-1} \in H \rightarrow (1)$

Since k is a subgroup of G

$\therefore ab^{-1} \in k \rightarrow (2)$

Scanned with CamScanner

Scanned with CamScanner

From ① & ②

$\therefore ab^{-1} \in H \cap K$

By know theorem,

A non-empty subset H of a group 'G' is a sub group of 'G' iff $a, b \in H \Rightarrow ab^{-1} \in H$

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

Theorem 3.20

The union of two subgroups of a group G is a subgroup iff one is contained in the other.

Proof:

Let H & K be two subgroups of G s.t one is cointained in other.

Hence either $H \subseteq K$ (or) $K \subseteq H$

i) $H \subseteq K \Rightarrow H \cup K = K$

Since K is a subgroup of G

Hence $H \cup K$ is subgroups of G

(or)

$K \subseteq H \Rightarrow H \cup K = H$

Since 'H' is subgroup of G

$H \cup K$ is a subgroup of G

$\therefore H \cup K = K$ (or) $H \cup K = H$ when either $H \subseteq K$ (or) $K \subseteq H$ respectively

$\therefore H \cup K$ is a subgroup

Scanned with CamScanner

Conversely

Suppose $H \cup K$ is a subgroup then either $H \subseteq K$ or $K \subseteq H$

Suppose that 'H' is not contained in 'K' and 'K' is not contained in 'H'

Then $\exists$ an element

$a \in H$ and $a \notin K$ $[\because H \not\subseteq K]$

$b \in K$ and $b \notin H$

clearly $a, b \in H \cup K$

Since $H \cup K$ is a subgroup of G.

$ab \in H \cup K$

$\Rightarrow ab \in H$ or $ab \in K$

case (i)

let $ab \in H$, since $a \in H$, $a^{-1} \in H$

$a^{-1}(ab) = (a^{-1}a)b = eb = b \in H$

which is contradiction to (2)

case (ii)

let $ab \in K$, since $b \in K$, $b^{-1} \in K$

$(ab)b^{-1} = a(bb^{-1}) = ae = a \in K$

which is contradiction to (1)

Scanned with CamScanner

Scanned with CamScanner

Definition

let A and B be two distinct subset of a group G.

we define $AB = \{ab / a \in A, b \in B\}$

Note.

If A and B are two subgroups of G. AB need not be a subgroup of G

Theorem 3.21

let A and B be two subgroups of a group G. then AB is a subgroup of G iff $AB = BA$.

Proof:

let AB be a subgroups of G

we claim that $AB = BA$

let $x \in AB$

Since AB is subgroup

Then $x^{-1} \in AB$

let $x^{-1} = ab$ whose $a \in A, b \in B$

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

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

Since $A \leq B$ subgroup.

$a \in A \rightarrow a^{-1} \in A, b \in B \Rightarrow b^{-1} \in B$

$\therefore x = b^{-1} a^{-1} \in BA$

$x \in BA \rightarrow (2)$

Scanned with CamScanner

From ① & ②

$AB \subseteq BA \rightarrow ③$

Now that

let $x \in BA$

then $x = ba$. where $b \in B$, $a \in A$.

$\therefore x^{-1} = (ba)^{-1} = a^{-1} b^{-1}$

$\therefore x^{-1} = a^{-1} b^{-1} \in AB$

Now, since AB is a subgroup

$x^{-1} \in AB$. we've $x \in AB$

$\therefore x \in AB \rightarrow ⑤$

From ④ & ⑤

$BA \subseteq AB \rightarrow ⑥$

From ⑤ & ⑥

$\boxed{AB = BA}$

Conversely

let $AB = BA$

we claim that.

AB is a subgroup of G

Since 'G' is a group and A & B are subgroups of 'G', their identity element are same

clearly $e \in AB$

Hence AB is non-empty subset of 'G'.

Now, let $x, y \in AB$

Scanned with CamScanner

Then $x = a_1 b_1$, $y = a_2 b_2$

where $a_1, a_2 \in A$ & $b_1, b_2 \in B$

$\therefore xy^{-1} = (a_1 b_1)(a_2 b_2)$

$= (a_1 b_1)(b_2^{-1} a_2^{-1})$

$= a_1 b_1 b_2^{-1} a_2^{-1}$

Now. $b_2^{-1} a_2^{-1} \in BA$

$b_2^{-1} a_2^{-1} \in AB$ [$\because AB = BA$]

$b_2^{-1} a_2^{-1} = a_3 b_3 \in AB$ where $a_3 \in A$, $b_3 \in B$

$\therefore xy^{-1} = a_1 b_1 a_3 b_3$

Now $b_1 a_3 \in BAB$

$b_1 a_3 \in A \quad B$ [$\because AB = BA$]

$\therefore b_1 a_3 = a_4 b_4 \in AB$ where $a_4 \in A$, $b_4 \in B$

$xy^{-1} = a_1 (a_4 b_4) b_3$

$= (a_1 a_4)(b_4 b_3)$

$\therefore xy^{-1} \in AB$

$\therefore AB$ is a subgroup of G

:

Subgroups.

Definitions

Let G be a set with a binary operation $*$ defined on it. Let $S \subset G$

If for each $a, b \in S$, $a * b$ (computed in G) in is S.

We say that S is closed with

Scanned with CamScanner

respect to the binary operation '*'.

Definition:

A subset H of G is called a sub group of G if H forms a group with respect to the binary operation in G.

Theorem 3.23

Order of an element:

let 'G' be a group and let $a \in G$. The least the integer n (if it exists) such that $a^n = e$ is called the order of a. If there is no positive integer 'n' such that $a^n = e$, then order of a is said to be infinite.

Theorem 3.24

let G be a group and $a \in G$. Then the order of 'a' is the same as the order of the cyclic group generated by a.

proof

let a be an element of order 'n'.

Then $a^n = e$.

We claim that,

$a, a^2, a^3, \ldots a^{n-1}$ all are distinct

Suppose $a^r = a^s$ where $0 < r < s < n$

Scanned with CamScanner

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

$a^{s-r} = e$

Hence $s-r < n$ which contradicts the definition of order of a.

Hence $e, a, a^2, \ldots a^{n-1}$ are all distinct

$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ is a cyclic group of order 'n'.

If 'a' is of infinite order, the sequence of elements $a, a^2, \ldots, a^n$, are all distinct and are in $\langle a \rangle$, cyclic

Hence $\langle a \rangle$ is an infinite group

Theorem 3.25

In a finite group every element is of finite order.

proof:

Let $a \in G$. If a is of infinite order then $\langle a \rangle$, is an infinite subgroup of G which is a contradiction since G is finite.

Hence the order of 'a' finite order.

Theorem 3.26

Let 'G' be a group and a be an element of order 'n' in G The $a^m = e$ if 'n' divides 'm'

proof:

$a^n = e$

Suppose $n|m$

Scanned with CamScanner

Then $m = nq$ where $q \in z$

$a^m = a^{nq}$

$= (a^n)^q \quad (\because a^{mn} = (a^m)^n)$

$= e^q \cdot e$

$\boxed{a^m = e}$

Conversely

Let $a^m = e$

let $m = nq + r$ where $0 \leq r < n$

$a^m = a^{nq+r}$

$= a^{nq} a^r \quad [a^{m+n} = a^m \cdot a^n]$

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

$= e^q \cdot a^r$

$= a^r$

$a^r = e$ and $0 \leq r < n$

Now, since 'n' is the smallest positive integer such that

$a^m = e$

we have $r = 0$

Hence $m = nq$

Theorem 3.15

let 'H' be a subgroup of G.

then

a) the identity element of H, is the same as that of 'G'.

Scanned with CamScanner

b) for each $a \in H$ the inverse of a in H is the same as the inverse of a in G.

proof.

(a) let e and e' be the identities of G and H respectively

let $a \in H$. Now,

$e'a = a$ (since e' is the identity of H)

$= ea$ (since e is the identity of G and $a \in G$)

$\therefore e'a = ea$

$\therefore e' = e$ (by cancellation law)

b) let a' and a'' be the inverse of a in G. and H respectively.

Since by (a), G and H have the same identity element e,

we have $a'a = e = a''a$

Hence by cancellation law

$a' = a''$

Scanned with CamScanner

Theorem 3.27

let 'G' be a group and $a, b \in G$

then,

i) order of a = order of a^{-1}

ii) order of a . order of $b^{-1}ab$

iii) order of ab - order of ba

proof:

let a be an element of order 'n'.

ie) $a^n = e$

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

$(a^{-1})^n = e^{-1} \cdot e$

$= e$

Now if possible $0 < m < n$ and $(a^{-1})^m = e$

$(a^m)^{-1} = e$

$a^m = e$

which contradicts order of a

$\therefore$ Then 'n' is the least +ve integer such that $(a^{-1})^n = e$

$\therefore$ order of a^{-1} is 'n'.

$\Rightarrow$ order of a = order of a^{-1}

(ii)

$(b^{-1}ab)^r = b^{-1}a^r b \rightarrow (1)$

If $r = 1 \Rightarrow b^{-1}ab = b^{-1}ab$

Scanned with CamScanner

Theorem 3.27

let 'G' be a group and a, b ∈ G

then: i) order of a = order of a^{-1}

ii) order of a = order of $b^{-1}ab$

iii) order of ab = order of ba

proof:

let a be an element of order 'n'.

ie) $a^n = e$

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

$(a^{-1})^n = e^{-1} \cdot e$

$= e$

Now if possible $0 < m < n$ and $(a^{-1})^m = e$

$(a^m)^{-1} = e$

$a^m = e$

which contradicts order of a

∴ Then 'n' is the least +ve integer

such that $(a^{-1})^n = e$

∴ order of a^{-1} is 'n'.

⇒ order of a = order of a^{-1}

(ii) $(b^{-1}ab)^r = b^{-1}a^rb \rightarrow (1)$

If $r = 1 \Rightarrow b^{-1}ab = b^{-1}ab$

∴ It is trivial

Now assume that (1) is true for $r = k$

∴ $(b^{-1}ab)^k = b^{-1}a^kb \rightarrow (2)$

Scanned with CamScanner

Now $r = k+1$

$$(b^{-1}ab)^{k+1} = (b^{-1}ab)^k (b^{-1}ab)$$

$$= (b^{-1}a^k b)(b^{-1}ab) \quad [\text{by } ②]$$

$$= b^{-1}a^k (bb^{-1}) ab \quad [\text{By } A(i)]$$

$$(b^{-1}ab)^{k+1} = b^{-1}a^k e\, ab$$

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

$$= b^{-1}a^{k+1}b.$$

Hence by induction method

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

Let a be an element of order n

$$\text{i.e. } a^n = e$$

$$(b^{-1}ab)^n = b^{-1}a^n b \quad [\text{By } ①]$$

$$= b^{-1}eb \quad [\because a^n = e]$$

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

$$\therefore (b^{-1}ab)^n = e$$

Now, if possible $o(m) < n$

$$(b^{-1}ab)^m = e$$

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

Pre-multiply b, b^{-1} post x

$$bb^{-1}a^m bb^{-1} = beb^{-1}$$

$$e a^m e = bb^{-1}$$

$$a^m = e$$

Scanned with CamScanner

∴ which contradicts definition order of a

Thus n is the least +ve positive integer such that $(b^{-1}ab)^n = e$

Order of a = order of $b^{-1}ab$

iii) order of ab = order of $a^{-1}(ab)a$

= order of $(a^{-1}a)(ba)$

= order of $e(ba)$

= order of ba.

iii) order of ab = order of ba.

Theorem 3.26.

Let 'G' be a group and let a be an element of order n in G. Then the order of a, where order is n/d where d is the g.c.d of n & s

Proof

Let $n/d = k$ and $s/d = t$

where 'k' and t relative primes

$\therefore (a^s)^k = a^{sk} = a^{tdk}$

$a^{tn} = (a^n)^t = e^t = e$

$\therefore (a^s)^k = e$

Further if 'm' is any +ve integer such that

$(a^s)^m = e$

$a^{sm} = e$

By the theorem

Scanned with CamScanner

Since a be an element of order n

$\therefore n \mid sm$

$kd \mid sdm$

$k \mid sm$

Since k and s are relatively primes

$\therefore k \mid m$

$\Rightarrow m \geq k$

Thus 'k' is the least +ve integer such that

$(as)^k = e$

$(as)^{n/d} = e$

$\therefore$ The order of a^s is n/d

Since a be and element of order n

Corollary 1:

The order of any power can be exceed of a cannot exceed the order of a.

Corollary 2:

let G be a finite cyclic group of order n generated by an element a. Then a^s generates a cyclic group of n/d where d is the g.c.d of n and s

Corollary 3:

let G be a finite cyclic group of order 'n' generated by an element a. a^s is a generator of G iff s and n are relatively prime. Hence the number of generator of a

Scanned with CamScanner

cyclic group of order n is $\phi(n)$ where $\phi(n)$ is the number of positive integers less than n and relatively prime to n.

Problem : 1

If 'G' is an finite group with even number of elements then 'G' contains atleast one element of order 2.

Proof

a is an element of order 2

$\Leftrightarrow a^2 = e$

$\Leftrightarrow aa = e$

$\Leftrightarrow a = a^{-1}$

Hence it is enough if we prove that there exists an element different from 'e' whose inverse is itself.

let $S = \{a / a \in G, a \neq a^{-1}\}$

clearly $a \in S \rightarrow a^{-1} \in S$ where $a \neq a^{-1}$

Hence 'S' contains an even and no of elements

Also $e \notin S$

Hence $S \cup \{e\}$ has odd no. of elements.

Since the order of group is even then there exists atleast one element $a \neq S \cup \{e\}$ ie $a = a^{-1}$

$a \cdot a = e$

$a^2 = e$

Problem 2:

The order of a permutation 'p' is the L.C.M of the length of its disjoint cycles.

Proof

let $P = c_1 c_2 \ldots c_r$ when the c_i's are

Scanned with CamScanner

mutually disjoint cycle of length l_i. Now let

$p^m = e$

Since product of disjoint cycles is commutative

$e = p^m = (c_1 c_2 \ldots c_r)^m = c_1^m c_2^m \ldots c_r^m$

Now, since the elements moved by one cycle are left fixed by all the other cycles,

$c_1^m = c_2^m = \ldots = c_r^m = e$

Now $c_1^m = e \rightarrow l_1 | m$

Since the order of c_1 is l_1

Similarly $l_2 l_3 \ldots l_r$ divide m

Thus 'm' is a common multiple of $l_1 l_2 \ldots l_r$

$\therefore$ the order of 'p' is the least such 'm' which is obviously the l.c.m of $l_1 l_2 \ldots l_r$

Problem 3

If 'a' is a generator of the cyclic group G and if there exists two unequal integers m and n such that $a^m = a^n$, prove that G is a infinite group.

Proof.

Since m and n are unequal we may assume that $m > n$.

Hence $m - n$ is a positive integer.

Also. $a^m \cdot a^{-n} = a^{m-n} = e$

$\therefore$ order of a is finite

$\therefore$ $G = \{a^r\}$ is a finite group (by theorem 3.2.1)

Scanned with CamScanner

Scanned with CamScanner

Theorem 3.2.9

Let G be group & H be subgroup of G. Then

i) $a \in H \Rightarrow aH = H$

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

iii) $a \in bH \Rightarrow a^{-1} \in Hb^{-1}$

iv) $a \in bH \Rightarrow aH = bH$

Proof

Let $a \in H$

We've to claim

$aH = H$

Let $x \in aH$

Then $x = ah$ where $h \in H$

Since $a \in H$ & $h \in H$

$ah \in H$

$\Rightarrow x \in H$

$\Rightarrow aH \subseteq H$

Let $x \in H$

Then $x = a(a^{-1}x)$

Since $a \in H \Rightarrow a^{-1} \in H$ & $x \in H$

Hence $a^{-1}x \in H$

$\therefore x \in aH$

$\Rightarrow H \subseteq aH$

$\therefore aH = H$

ii) Let $aH = bH$

Pre x by a^{-1}

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

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

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

By (i)

Scanned with CamScanner

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

conversely

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

By (i)

$H = a^{-1}bH$

pre multiply by a.

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

$= (aa^{-1})bH$

$= ebH$

$aH = bH$

(iii) let $a \in bH$

then $a = bh$ where $h \in H$

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

$= h^{-1}b^{-1} \in Hb^{-1}$

$\therefore a^{-1} \in Hb^{-1}$

Conversely

let $a^{-1} \in Hb^{-1}$

let $h \in H \Rightarrow h^{-1} \in H$

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

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

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

$a = bh$

$\therefore a \in bH$

(iv) let $a \in bH$

we've to claim $aH = bH$

let $x \in aH$.

Scanned with CamScanner

Then $x = ah_1$ where $h_1 \in H$

Also $a \in bH$

Then $xa = bh_2$ where $h_2 \in H \rightarrow (1)$

$$x = bh_2 h_1$$

$$= b(h_2 h_1)$$

since $h_2 h_1 \in H$

$$b(h_2 h_1) \in bH$$

$$\rightarrow x \in bH$$

$$\therefore aH \subseteq bH$$

Now,

let $x \in bH$

Then $x = bh_3$ where $h_3 \in H$

From (1),

$$b = ah_2^{-1}$$

$$x = ah_2^{-1} h_3$$

since $h_2^{-1} h_3 \in H$

$$a(h_2^{-1} h_3) \in aH$$

$$\Rightarrow x \in aH$$

$$bH \subseteq aH$$

$$\therefore aH = bH$$

conversely

let $aH = bH$

Then $a = ae$ [$\because e$ is an identity of H]

$\therefore a \in aH$.

$\therefore a \in bH$

Scanned with CamScanner

Theorem 3.30

Let H be a subgroup of G then

i) any two left cosets of H are either identity and are disjoint

ii) union of all the left cosets of H in G

iii) the number of elements in any left coset is the same as the number of element in H.

Proof:

i) let aH and bH be two left cosets

Suppose aH, bH are not disjoint

we claim $aH = bH$

Since aH, bH are not disjoint

$\therefore aH \cap bH \neq \phi$

$\therefore$ there exists an element

$c \in aH \cap bH$

$\therefore c \in aH \rightarrow (1)$ and $c \in bH \rightarrow (2)$

By the known result,

$a \in bH \Rightarrow aH = bH$

$(1) \rightarrow c \in aH \Rightarrow aH = cH \rightarrow (3)$

$(2) \rightarrow c \in bH \Rightarrow bH = cH \rightarrow (4)$

From (3) & (4)

$aH = bH$

ii) let $a \in G$

then $a = ae$ [since 'e' is an identity of H]

$a = ae \in aH$

$\therefore a \in aH$

Scanned with CamScanner

Every element of 'G' belongs to left cosets of H.

∴ The union of left cosets of H in 'G'

(iii) The map $f : H \to aH$

Defined by $f(H) = ah$

clearly 'f' is bijection

∴ Hence every left cosets has the same no. of elements in H.

Note 1: This theorem shows that the collection of all left cosets forms a partition of the group.

Note 2: The above result is true if we replace left cosets by right cosets. In what follows the result we prove for left cosets are also true for right cosets.

Remarks.

Let H be a subgroup of G. we define a relation in 'G' as follows. Define $a \sim b \Leftrightarrow a^{-1}b \in H$

Proof:

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

Then a is an equivalence relation

Reflexive

For any,

Scanned with CamScanner

$a^{-1}a = e \in H$

$a'a \in H$

$a \sim a$

Symmetric

$a \sim a$. Hence $\sim$ is reflexive

Symmetric

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

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

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

$a \sim b \rightarrow b \sim a$

Hence is symmetric

Transitive

$a \sim b \;\&\; b \sim c \Rightarrow a^{-1}b \in H \;\&\; b^{-1}c \in H$

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

$a^{-1}(bb^{-1})c \in H$

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

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

$a \sim c$

Hence $\sim$ is transitive

Hence $\sim$ is in equivalence relation

$[a] = aH$

let $b \in [a]$. Then $b \sim a$

$a \sim b - a^{-1}b \in H$

$b \in aH$

$[a] \subseteq aH$

Scanned with CamScanner

Also

$b \in aH \Rightarrow b = ah$ for some $h \in H$

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

$\Rightarrow a \sim b$

$\Rightarrow b \in [a]$

Theorem 3.31

Let H be a subgroups of G the number of left cosets of H, is same as the number of cosets of H.

Proof:

Let L and R be the set of left and right cosets of H.

We define a map $f: L \to R$ by

$f(aH) = Ha^{-1}$

i) f is well defined for $aH = bH$

$\Rightarrow a^{-1}b \in H$ [by (ii)

$= a^{-1} \in Hb^{-1}$

$= Ha^{-1} = Hb^{-1}$ (by (i))

$f(a_1) = h_1$
$a_1 = a_2$
$h_1 = h_2$

f is 1-1, for

$f(aH) = f(bH)$

$\to Ha^{-1}$

$= Hb^{-1}$

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

$\Rightarrow a^{-1} = hb^{-1}$ for some $h \in H$

Scanned with CamScanner

Scanned with CamScanner

$\Rightarrow a = bh^{-1}$

$\Rightarrow a \in bH$

$\Rightarrow aH = bH$

'f' is onto For every right coset Ha has a pre-image under f namely $a^{-1}H$

Hence 'f' is a bijection from L to R.

Hence the number of left cosets is the same as the number of right cosets.

Definition

Let H be a subgroup of G The number of distinct left (right) cosets of H in G is called the index of H in 'G' and is denoted by $[G:H]$

Example:

In $(\mathbb{Z}_8, \oplus)$, $H = \{0,4\}$ is a subgroup. The left cosets of H are given by

$0+H = \{0,4\} = H$

$1+H = \{1,5\}$

$2+H = \{2,6\}$

$3+H = \{3,7\}$

Those are the four distinct left cosets of H.

Hence the index of the subgroup H is 4.

Note that $[\mathbb{Z}_8 : H] \times [H] = 4 \times 2 = 8 = [\mathbb{Z}_8]$

Scanned with CamScanner

Theorem 3 :

A group 'G' has no proper subgroups if it is a cyclic group of prime order.

Proof:

Suppose 'G' is a group of prime order p where 'p' is prime

Since 'p' is prime it is only divisible by 1 and p.

By lagrange's theorem,

The order of subgroup divides, order of group.

So that the only subgroups exists for this 'G' having order p are {e} and 'G' itself.

Hence 'G' has no proper subgroup.

Conversely,

Scanned with CamScanner

r. normaliser

Let 'G' be a group and let a be a fixed element of 'G'

let $H_a = \{x / x \in G \text{ and } ax = xa\}$

ie) H_a is the set of all elements in 'G' which commute with a.

Show that H_a is a subgroup of 'G'.

H^a is called the normaliser of a in 'G'.

Problem 1

Let $a \in R^*$ let $H = \{a^n / n \in Z\}$. Then 'H' is a subgroup of R^*.

Soln

Clearly 'H' is non-empty

Now let, $x, y \in H$

Then $x = a^s$ and $y = a^t$ where $s, t \in Z$

$\therefore xy^{-1} = a^s (a^t)^{-1} = a^{s-t} \in H$

Hence 'H' is a subgroup of R^*

Scanned with CamScanner

Problem 2: let 'H' denotes the set of all permutations in S_n fixing the symbol 1. Then 'H' is a subgroups of S_n.

Soln

Clearly $e \in H$ and hence 'H' is non-empty

let $\alpha, \beta \in H$. Then α and β fix the symbol 1.

Now β fixes the symbol $1 \Rightarrow \beta^{-1}$ first the symbol 1.

Hence $\alpha\beta^{-1}$ fixes the symbol 1.

Hence $\alpha\beta^{-1} \in H$.

Problem 3:

let 'G' be the set of all 2×2 matrices with entires from R. Then 'G' is a group under matrix addition.

let $H = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} / a, b \in R \right\}$. Then 'H' is a subgroup of G.

Soln.

let $A, B \in H$

Then $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ and $B = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$

Now $A - B = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} - \begin{pmatrix} c & 0 \\ 0 & a \end{pmatrix}$

$= \begin{pmatrix} a-c & 0 \\ 0 & b-d \end{pmatrix} \in H$

Hence 'H' is a subgroup of 'G'.

Scanned with CamScanner

Problem 11:

let 'G' be group.

Let $H = \{ a / a \in G \text{ and } ax = xa \text{ for all } x \in G \}$

i.e) H is set of all elements which commute with every other element. Show that 'H' is a subgroup of G.

Soln.

Clearly $ex = xe = x$ for all $x \in G$

Hence $e \in H$. So that 'H' is non empty

Now, let $a, b \in H$

Then $ax = xa$ and $bx = xb$ for all $x \in G$.

Now.

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

$$\Rightarrow (b^{-1}b)xb^{-1} = b^{-1}x(bb^{-1})$$

$$\Rightarrow exb^{-1} = b^{-1}xe$$

$$\Rightarrow xb^{-1} = b^{-1}x$$

$$\therefore (ab^{-1})x = a(b^{-1}x)$$

$$= a(xb^{-1}) \quad (\text{by } ①)$$

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

$$= (xa)b^{-1} \quad (\text{since } ax = xa)$$

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

Thus ab^{-1} commutes with every element of 'G'.

$\therefore ab^{-1} \in H$ and hence 'H' is a subgroup of 'G'.

Scanned with CamScanner

Note: The above subgroup of 'G' is called the centre of 'G' and is denoted by $Z(G)$.

Problem 5:

let G be a group and let a be a fixed element of G.

let $H_a = \{x / x \in G \text{ and } ax = xa\}$

ie) H_a is the set of all elements in G which commute with a.

Show that H_a is a subgroup of 'G'.

Soln

clearly $ae = ea = a$

Hence $e \in H_a$. So that H_a is non-empty

Now, let $x, y \in H_a$

Then $ax = xa$ and $ay = ya$

Now, $ay = ya \Rightarrow y^{-1}a = ay^{-1}$ (as the previous Problem)

Hence

$$\begin{aligned} a(xy^{-1}) &= (ax)y^{-1} \\ &= (xa)y^{-1} \quad (\text{since } ax = xa) \\ &= x(ay^{-1}) \\ &= x(y^{-1}a) \\ &= (xy^{-1})a \end{aligned}$$

Hence xy^{-1} commutes with a.

$\therefore xy^{-1} \in H_a$ and hence H_a is a subgroup of 'G'.

Note H_a is called the normaliser of a in 'G'

Scanned with CamScanner

Cyclic groups..

let 'G' be a group. Let $a \in G$

Then $H = \{a^n / n \in \mathbb{Z}\}$ is a subgroup of G (verify)

'H' is called the cyclic subgroup of 'G' generated by a and is denoted by $\langle a \rangle$.

Definition:

let 'G' be a group and let $a \in G$. a is called a generator of 'G' if $\langle a \rangle = G$

A group 'G' is cyclic if there exists an element $a \in G$ such that $\langle a \rangle = G$.

Note:

If 'G' is a cyclic group generated by an element a. there every element of 'G' is the form a^n for some $n \in \mathbb{Z}$..

Theorem 3.22

Any cyclic group is abelian.

proof.

· let $G = \langle a \rangle$ be a cyclic group.

let $x, y \in G$. Then $x = a^r$ and $y = a^s$ for some $r, s \in \mathbb{Z}$

Hence $xy = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = yx$

∴ 'G' is abelian

Scanned with CamScanner

Theorem 3.03

A subgroup of cyclic group is cyclic

Proof

Let 'G' be a cyclic group generated by a and let 'H' be a subgroup of 'G'. We claim that 'H' is cyclic

Clearly every element of 'H' is of the form a^n for some integer 'n'

Let m be the smallest positive integer such that $a^m \in H$. We claim that a^m is a generator of H

Let $b \in H$. Then $b = a^n$ for some $n \in \mathbb{Z}$.

Let $n = mq + r$ where $0 \leq r < m$.

Then $b = a^n = a^{mq+r} = a^{mq} a^r$

$= (a^m)^q a^r$

$\therefore a^r = (a^m)^{-q} b \rightarrow (1)$

Now $a^m \in H$. Since 'H' is a subgroup $(a^m)^{-q} \in H$

Also $b \in H$.

By (1) $a^r \in H$ and $0 \leq r < m$

But m is the least positive integer such that $a^n \in H$.

$\therefore r = 0$ Hence $b = a^n = a^{qm} = (a^m)^q$

$\therefore$ Every element of H is a power of a^m

$H = \langle a^m \rangle$ and 'H' Hence is cyclic

Scanned with CamScanner

Theorem 3.36

Euler's theorem

If 'n' is any integer and $(a,n)=1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$

where $\phi(n)$ is the no. of the integers less than 'n' relatively prime to 'n'

Proof:

Let $G = \{m / m<n \text{ \& } (m,n)=1\}$ multiplication mod n

let $(a,n)=1$

let $a = q.n + r$, where $0 \le r < n$

$a \equiv r \pmod{n}$

Since $(a,n)=1$ & we've $(n,r)=1$

so $r \in G$ [$r<n$, $(n,r)=1$]

$\therefore r^{\phi(n)} = 1$ [by theorem 3.35]

$r^{\phi(n)} \equiv 1 \pmod{n}$

$a^{\phi(n)} \equiv r^{\phi(n)} \pmod{n}$

$a^{\phi(n)} \equiv 1 \pmod{n}$

Theorem 3.38

A group 'G' has no proper subgroup iff it was a cyclic group of prime order.

Proof:

Suppose 'G' is a group of prime order p. where 'p' is prime.

Since 'p' is prime it is not only divisible by 1 and p.

Scanned with CamScanner

By Lagrango's Theorem.

The order of subgroup divides order of group

So that the only subgroups exists for this 'G' having order 'p' are {e} and 'G' itself.

Hence 'G' has no proper subgroup

conversely.

let 'G' be a group having no proper subgroup. First we shall prove that 'G' is cyclic

suppose 'G' is not cyclic

let $a \in G$ and $a \neq e$

Then the cyclic group $\langle a \rangle$ is a proper subgroup of 'G' which is a contradiction

Hence 'n' is cyclic

Also 'G' cannot be infinite. for an infinite cyclic group contains a proper subgroup (a^2)

Hence 'G' must be of finite order, say n

we claim that, 'n' is prime

If possible let 'n' be a composite number.

Let $n = pq$ where $p, q > 1$

Let $a \in G$ be a generator of the group

Scanned with CamScanner

Then $\langle a^p \rangle$ is a subgroup of order, q and hence is proper subgroup of 'G', which is a contradiction

Hence 'n' is prime

∴ 'G' is a cyclic group of Prime order.

order of an element:-

Problem 2:

The order of a permutation 'p' is the L.C.M of the length if it is disjoint cyclic

proof:

Let $p = c_1, c_2 \ldots c_r$ and where c_i are mutually disjoint cycles of length l_i. Now let

$p^m = e$

since product of disjoint cycle is commutative $e = p^m = (c_1, c_2, \ldots c_r)^m = c_1^m, c_2^m \ldots c_r^m$.

now since the elements moved by one cycle are left fixed all other cycles,

$$c_1^m = c_2^m = \ldots = c_r^m = e$$

now $c_1^m = e \Rightarrow l_1 | m$ since the order

$l_1 l_2 l_3 \ldots$

$l_2, l_3, \ldots l_r$ divides m

'm' is common multiple of $l_1, l_2 \ldots l_r$

The order of 'p' is the least such m which is obviously the L.C.M of $l_1, l_2 \ldots l_r$

Scanned with CamScanner

Lagrange's theorem

Let G be a finite group of order n and H be any subgroup of G Then the order of H divides the order of G.

Proof:

Let 'H' be a subgroup of 'G' having m elements,

Let $|H| = m$ and let $[G:H] = r$

Then the number of left cosets of H in 'G' is 'r'

By the known theorem.

The number of elements in any left cosets all in same as the no. of elements in 'H'.

Hence every left cosets of 'H' has m element.

Hence 'r' left cosets 'H' has rm elements.

By the known theorem.

The union of all the left cosets of H in 'G'.

Since these 'r' left cosets are mutaly disjoint coset of H in 'G' and has same no. of elements namely m.

Then $|r| =$ union of all left cosets of H

$n = rm$

Hence m divides 'n'

Note Hence order subgroup the divides order of group.

Scanned with CamScanner

Corollary

$$[G : H] = \frac{|G|}{|H|}$$

Note 1:

Any group of prime order has no proper subgroup.

Note 2:

The converse of Lagrange's theorem is false.

Ex) If 'G' is a group of order 'n' and m divides n. Then 'G' need not have a subgroup of order 'm'.

Theorem 3.1b.

A subset 'H' of a group 'G' is a sub group of 'G' iff

i) it is closed under the binary operation in 'G'.

ii) The identity of 'G' is in 'H'

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

Proof:

Let H be subgroup of 'G'.

i) From the definition of subgroup 'H' satisfies all the group conditions under the binary operation so that 'H' is closed under the binary operation in 'G'.

Scanned with CamScanner

(ii) Let e and e' be the identity of 'G' and H respectively

Let $a \in H$.

$e'a = a$ (since e' identity of H)

$= ea$ (since e identity of G and $a \in G$)

$e'a = ea$

$e' = e$ (Right cancellation law)

(iii) Let a' and a'' be the inverse of a in G and H respectively

Let $a \in G$

$a'a = e \rightarrow ①$ (by (a) e unique identity for both G & H)

Since a' inverse of a in 'G'.

Now, $a \in H$.

$a''a = e \rightarrow ②$ (by (a) e unique identity for both G & H)

Since a'' inverse of a in 'H'.

from ① & ②

$a'a = a''a$

$a' = a''$

To prove the converse part.

Let 'H' be subset of G, and (i), (ii) and (iii) are true.

It is obviously that 'H' is subgroup of 'G'.

Scanned with CamScanner

$\therefore \alpha\phi\alpha^{-1} \in H \quad \forall \alpha$

$\therefore H$ is Normal subgroup of A_4.

Scanned with CamScanner

and $f[(12)\alpha] = (12)(12)\alpha = \alpha$

Thus f' is a bijection and hence the number of odd permutation in S_n = the number of permutations in S_n. Since S_n contains $n!$ permutations, A_n has $\frac{n!}{2}$ elements.

Definition:

The group A_n of all even permutations in S_n is called the alternating group on 'n' symbols.

Scanned with CamScanner

UNIT – III

Normal subgroups and Quotient groups

Definition:

A subgroups 'H' of 'G' is called a normal subgroup of 'G' if $aH = Ha$ for all $a \in G$

Example

For any group G, $\{e\}$ and G are normal subgroups

Theorem 3.39

Every subgroup of an abelian group is a normal subgroup

Proof:

Let 'G' be an abelian group
Let 'H' be a subgroup of 'G'.
Let $a \in G$.
We claim that $aH \subseteq Ha$
Now let $x \in aH$
Then $x = ah$ where $h \in H$
Since H is a subgroup of 'G'. Then $h \in G$
Since $a, h \in G$
'G' is an abelian group
$x = ha$
$x \in Ha \rightarrow (1)$
Hence $aH \subseteq Ha \rightarrow (1)$
Let $y \in Ha$
then $y = ha$ where $h \in H$
(Since 'H' is a subgroup of G. Then $h \in G$
Since $a, h \in G$)
G is an abelian group
$y = ah$
$y \in ah$

Scanned with CamScanner

$Ha \subseteq aH \rightarrow (2)$

from (1) & (2)

$$aH = Ha$$

∴ 'H' is an normal subgroup

Theorem 3.40

Let 'H' be a subgroup of index 2 in a group 'G'. Then 'H' be is a normal subgroup of G.

proof:

case (i)

If $a \in H$

Then $H = aH = Ha$

Hence 'H' is a normal subgroup of 'G'.

case (ii)

If $a \notin H$

Then aH is left coset different from H.

Hence $H \cap aH = \phi$

Since index of H in G is 2.

So that left coset of 'H' in 'G' are $aH \& H$.

W.K.T

The union of all left cosets of H in 'G'.

$$aH \cup H = G$$

hence $aH = G - H \rightarrow (1)$

Ni'y, If $a \notin H$

Ha is right coset different from H.

Hence $H \cap Ha = \phi$

Since index of 'H' in G is 2.

So that right coset of H in 'G' are $Ha \& H$

W.K.T

The union of all right cosets of H in 'G'

$$Ha \cup H = G$$

Hence $Ha = G - H \rightarrow (2)$

Scanned with CamScanner

From ① & ②

$aH = Ha$

'H' is a normal subgroup.

Theorem 3.4.1.

Let N be a subgroup of G then the equivalent are following

i) N is a normal subgroup of G

ii) $aNa^{-1} = N \ \forall \ a \in G$

iii) $aNa^{-1} \subseteq N \ \forall \ a \in G$

iv) $ana^{-1} \in N \ \forall \ n \in N$ & $a \in G$.

Proof:

(i) $\Leftrightarrow$ (ii)

Suppose N is a normal subgroup

$aN = Na \ \forall \ a \in G$

Post multiplying a^{-1} on both side

$aNa^{-1} = Naa^{-1}$

$= Ne$ [a^{-1} is the inverse of a]

$aNa^{-1} = N$ [e is the identity element]

(ii) $\Leftrightarrow$ (iii)

Suppose $aNa^{-1} = N \ \forall \ a \in G$

So it is obvious that

$aNa^{-1} \subseteq N \ \forall \ a \in G$

(iii) $\Leftrightarrow$ (iv)

Suppose $aNa^{-1} \subseteq N \ \forall \ a \in G$

let $x = ana^{-1} \in aNa^{-1} \subseteq N$

But $aNa^{-1} \subseteq N$

Hence $x \in N$

($ana^{-1} \in N \ \forall \ n \in N$ & $a \in G$)

Scanned with CamScanner

(iv) → (i)

Suppose $ana^{-1} \in N$ $\forall$ $n \in N$ & $a \in G$

We claim that,

$$aN = Na$$

Now, let $x \in aN$

Then $x = an$ where $n \in N$

$= an(a^{-1}a)$ [$a^{-1}.a = aa^{-1} = e$]

$= (ana^{-1})a$ [Associative property]

Since $ana^{-1} \in N$

$x = (ana^{-1})a \in Na$

$\Rightarrow x \in Na$

Hence $aN \subseteq Na \rightarrow (1)$

Again let $x \in Na$

Then $x = na$ where $n \in N$

$= (aa^{-1})na$ [$aa^{-1} = a^{-1}a = e$]

$= a(a(a^{-1})^{-1})$ [By Associative property]

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

Since

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

$x = a(a^{-1}n(a^{-1})^{-1}) \in aN$

Hence $Na \subseteq aN \rightarrow (2)$

from (1) & (2)

$aN = Na$

Hence 'N' is a Normal subgroup of 'G'.

Problem 1:

Prove that the intersection of two normal subgroup of 'G' is a normal subgroup of 'G'.

Scanned with CamScanner

Soln

Let H & K be two normal subgroup of G.

Since H & K are subgroup

Hence $H \cap K$ is also a subgroup

Now let $a \in G$

let $x \in H \cap K$

Then $x \in H$ & $x \in K$

Since H & K is a normal subgroup of G.

$$axa^{-1} \in H \text{ & } axa^{-1} \in K \quad \forall a \in G$$

Hence $axa^{-1} \in H \cap K$

$H \cap K$ is a normal subgroup.

Problem 2.

The centre H of a group 'G' is a normal subgroup of 'G'.

Soln

The centre H of G is given by,

$$H = \{a \mid a \in G,\ ax = xa \ \forall\ x \in G\}$$

Now, let $x \in H$ and $a \in G$

Hence $ax = xa$

Post multiplying by a^{-1}

$$axa^{-1} = xaa^{-1}$$

$$= x \cdot e \quad [aa^{-1} = a^{-1}a = e]$$

$$= x \quad [e \text{ is the identity element}]$$

Since $x \in H$,

$$axa^{-1} \in H$$

Hence 'H' is a normal subgroup of 'G'.

Problem 3:

Let H be subgroup of G. Let $a \in G$. Then aHa^{-1} is a subgroup of G.

Scanned with CamScanner

Soln

$e = aea^{-1}$

Since 'H' is a subgroup

$e \in H$,

since $e \in H$,

$e = aea^{-1} \in aHa^{-1}$

$\therefore aHa^{-1} \neq \phi$

Let $x, y \in aHa^{-1}$

then $x = ah_1a^{-1}$

$y = ah_2a^{-1}$ where $h_1, h_2 \in H$

$xy^{-1} = (ah_1a^{-1})(ah_2a^{-1})^{-1}$

$= (ah_1a^{-1})((a^{-1})^{-1}h_2^{-1}a^{-1})$ $[(ab)^{-1} = b^{-1}a^{-1}]$

$= (ah_1a^{-1})(ah_2^{-1}a^{-1})$

$= ah_1(a^{-1}a)h_2^{-1}a^{-1}$ [By Associative property]

$= ah_1eh_2^{-1}a^{-1}$ [Inverse property]

$= ah_1h_2^{-1}a^{-1}$ [Identity property]

Since $h_1, h_2 \in H \Rightarrow h_1h_2^{-1} \in H$

$a(h_1h_2^{-1})a^{-1} \in aHa^{-1}$

$xy^{-1} \in aHa^{-1}$

Hence aHa^{-1} is a subgroup of 'G'.

Problem 4:

S.T if a group 'G' has exactly one subgroup 'H' of given order, then 'H' is an normal subgroup of 'G'.

Scanned with CamScanner

Soln.

Let the order of H be m'.

Let $a \in G$

$$e = aea^{-1}$$

Since 'H' is a subgroup

$$e \in H$$

Since $e \in H$

$$e = aea^{-1} \in aHa^{-1}$$

$$\therefore aHa^{-1} \neq \phi$$

Let $x, y \in aHa^{-1}$

Then $x = ah_1a^{-1}$, $y = ah_2a^{-1}$ where $h_1, h_2 \in H$.

$$xy^{-1} = (ah_1a^{-1})(ah_2a^{-1})^{-1}$$

$$= (ah_1a^{-1})((a^{-1})^{-1}h_2^{-1}a^{-1}) \quad [(ab)^{-1} = b^{-1}a^{-1}]$$

$$= (ah_1a^{-1})(ah_2^{-1}a^{-1})$$

$$= ah_1(a^{-1}a)h_2^{-1}a^{-1} \quad [\text{Associative property}]$$

$$= ah_1(e)h_2^{-1}a^{-1} \quad [\text{Inverse property}]$$

$$= ah_1h_2^{-1}a^{-1} \quad [\text{Identity property}]$$

Since $h_1, h_2 \in H \Rightarrow h_1h_2^{-1} \in H$.

$$a(h_1h_2^{-1})a^{-1} \in aHa^{-1}$$

$$xy^{-1} \in aHa^{-1}$$

Hence aHa^{-1} is a subgroup of 'G'

We claim that,

$$|aHa^{-1}| = |H|$$

Now, consider $f : H \to aHa^{-1}$ defined by,

$$f(h) = aha^{-1}$$

(i) f is 1-1

$$f(h_1) = f(h_2) \text{ for some } h_1, h_2 \in H$$

Scanned with CamScanner

$$ah_1a^{-1} = ah_2a^{-1}$$

By applying right & left cancellation law.

$$h_1 = h_2$$

$\therefore f$ is 1-1.

(ii) f is onto

let $x = aha^{-1} \in aHa^{-1}$

then $f(h) = aha^{-1} = x$

Hence every image has pre-image

Hence f is onto

from (i) & (ii)

'f' is bijection

$\therefore |aHa^{-1}| = |H| = m$

But 'G' has only one subgroup of order of m.

$$aHa^{-1} = H$$

post multiplying by a.

$$aHa^{-1}a = Ha$$

$$aH = Ha \qquad [a^{-1}a = aa^{-1} = e]$$

Hence 'H' is a Normal subgroup of 'G'.

Problem 5:

S.T if H & N are subgroups of G & N is Normal in G then $H \cap N$ is normal in H. Show by an example that $H \cap N$ need not be normal in G.

Sol.

Let $x \in H \cap N$, $a \in H$

we claim that.

$$axa^{-1} \in H \cap N$$

Scanned with CamScanner

since $x \in HnN$

$x \in N$

since 'N' is normal in G.

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

since $x \in HnN$

$\therefore x \in H$

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

$\therefore a x a^{-1} \in H \rightarrow (2)$

from (1) & (2)

$$a x a^{-1} \in HnN$$

Hence HnN is normal in H.

Example for HnN need not be normal in G'.

$G = S_3 = \{e, P_1, P_2, P_3, P_4, P_5\}$

$N = G$

$H = \{e, P_3\}$

$HnN = \{e, P_3\} = H$

$HnN = H$

since 'H' is a subgroup of 'G'.

Hence HnN is a subgroup of G'.

Hence $HnN = H$ is need not be normal in G.

Scanned with CamScanner

Problem 6.

If 'H' is a subgroup of G & N is a normal subgroup of G. Then HN is a subgroup of G.

Soln

to prove HN is subgroup of G.

It is enough to prove that.

$$HN = NH$$

Now, let $x \in HN$

Then $x = hn$ where $h \in H$ & $n \in N$

$\therefore x \in hN$ (right left coset)

Since 'N' is Normal

But $hN = Nh$

$x \in Nh$

Hence $x = n_1 h$ where $n_1 \in N$

$x \in NH$

Hence $HN \subseteq NH \rightarrow (1)$

again let $y \in NH$

Then $y = nh$ where $n \in N$ & $h \in H$

$\therefore y \in Nh$ (right coset)

Since 'N' is Normal

$Nh = hN$

$\therefore y \in hN$

Hence $y = hn_2$ where $n_2 \in N$

$\therefore y \in HN$

$NH \subseteq HN \rightarrow (2)$

from (1) & (2)

$HN = NH$

Scanned with CamScanner

Scanned with CamScanner

By known theorem,

Let A and B be a two subgroups of G then AB is a subgroup iff AB=BA Hence HN is a subgroup of G.

problem 7:

If M & N are normal subgroups of group G. such that $M \cap N = \{e\}$. Show that every element of M commutes with every element of N.

Soln.

Given $M \cap N = \{e\}$

let $a \in M$, $b \in N$

we claim that,

$$ab = ba$$

Consider the element $aba^{-1}b^{-1}$

Since $a \in M$, $a^{-1} \in M$

M is normal in G.

$$aba^{-1} \in N$$

Since $b \in N \Rightarrow b^{-1} \in N$

$$aba^{-1}b^{-1} \in N \rightarrow (2)$$

from (1) & (2)

$$aba^{-1}b^{-1} \in M \cap N$$

$$aba^{-1}b^{-1} = e$$

$$(ab)(ba)^{-1} = e$$

Post multiplying ba on both sides

$$(ab)(ba)^{-1}(ba) = e(ba)$$

$$(ab)(e) = (ba)$$

$$ab = ba$$

Scanned with CamScanner

Theorem 3.42.

A subgroup N of 'G' is normal iff the product of two right cosets of 'N' is again a right coset of N.

Proof: Suppose 'N' is normal subgroup of 'G'.

let Na, Nb be a right coset of 'N' where $a, b \in G$.

Then $NaNb = N(aN)b$

$= N(Na)b$ [∵ N is normal subgroup $\Rightarrow aN = Na$]

$= (NN)ab$

$= Nab$ [$\because NN = N$]

Hence the product two right cosets is again a right coset.

conversely,

suppose that the product of two right coset is again a right coset of N.

$ab = (ea)(eb) \in NaNb$

since identity of N

Hence NaNb is right coset containing ab

$NaNb = Nab$

we claim that

aN is normal subgroup of 'G'.

Let $n \in N$ and $a \in G$

then

$ana^{-1} = cana^{-1} \in NaNa^{-1} = Naa^{-1} = Ne = N$

Scanned with CamScanner

since 'e' is identity of N

$aNa^{-1} \in N$

∴ Hence N is a normal subgroup of G

Hence proved.

theorem 3.43.

Let N be a normal subgroup of a group G. then G/N is a group under the operation defined by $NaNb = Nab$

proof.

Let N be Normal subgroup of G

let Na, Nb be right cosets of N in G.

where $a, b \in G$

$$NaNb = N(aN)b$$
$$= N(Na)b \quad (\because N \text{ is Normal})$$
$$= (NN)ab$$
$$= Nab \quad (\because NN = N)$$
$$NaNb = Nab$$

which is well defined.

(ii) Association property:.

let $Na, Nb, Nc \in G/N$

$$Na\cdot(NbNc) = Na(Nbc)$$
$$= N a(bc)$$
$$= N(ab)c \quad (\text{since } 'G' \text{ hold associative})$$
$$= (Nab)Nc$$
$$= (NaNb)Nc$$

Hence G/N hold association property

Scanned with CamScanner

iii) Identity element

let $Ne \in G/N$

$Ne = N \in G/N$

let $Na \in G/N$

$NaNe = Nae = Na$

$NeNa = Nea = Na$

$NaNe = NeNa = Na$

Hence Ne is the identity of G/N

iv) Inverse element

let $Na^{-1} \in G/N$

let $Na \in G/N$

$NaNa^{-1} = Naa^{-1} = Ne$

$Na^{-1}Na = Na^{-1}a = Ne$

$Na\ Na^{-1} = Na^{-1}Na = Ne$

$\therefore Na^{-1}$ is inverse of Na

Hence G/N is group

Definition

Then the group G/N is called the quotient group (factor group) of G modulo N.

Example: $3\mathbb{Z}$ is a normal subgroup of $(\mathbb{Z}, +)$. The quotient group $\mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z}+0, 3\mathbb{Z}+1, 3\mathbb{Z}+2\}$. Hence $\mathbb{Z}/3\mathbb{Z}$ is a group of order 3.

Scanned with CamScanner

Isomorphism.

Let G and G' be two groups. A map $f : G \to G'$ is called an isomorphism if

i) 'f' is a bijection

ii) $f(xy) = f(x) f(y)$ for all $x, y \in G$

Two group G and G' are said to be isomorphic if there exists an isomorphism $f : G \to G'$. If two groups G and G' are isomorphic we write $G \cong G'$

Theorem 3.44

Isomorphism is an equivalent relation among groups.

proof: i) Reflexive

For any group G,

$i_G : G \to G$

clearly identity mapping is bijection

$i_G(x,y) = xy \quad \forall\ x, y \in G$

$i_G(x)\, i_G(y) = xy \quad \forall\ x, y \in G$

$i_G(xy) = i_G(x)\, i_G(y)$

Hence i_G is isomorphism

Hence isomorphism is reflexive.

ii) symmetric

let $G \cong G'$ and let $f : G \to G'$ be an isomorphism.

Since 'f' is bijection

Scanned with CamScanner

Then let $f^{-1}: G' \to G$ is also an ... isom

let $x', y' \in G'$

$f^{-1}(x') = x$ & $f^{-1}(y') = y$

Then $f(x) = x'$ and $f(y) = y'$

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

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

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

Hence f^{-1} is also isomorphism.

∴ Hence isomorphism is symmetric

(iii) Transitive:-

let $f: G \to G'$ be an isomorphism

and $g: G' \to G''$.

Then $g \circ f : G \to G''$

since f and g are bijection

Hence $g \circ f$ is also bijection.

let $x, y \in G$

$(g \circ f)(xy) = g[f(xy)]$

$= g[f(x) f(y)]$ [∵ f is isomorphis

$= g'(f(x)) g(f(y))$ [g is isomorph

$= (g \circ f)(x) (g \circ f)(y)$

$(g \circ f)$ is an isomorphism.

$\therefore G \cong G''$

Scanned with CamScanner

Hence isomorphism is transitive

Hence isomorphism is an equivalence relation among groups.

theorem 3.45

let $f: G \to G'$ be an isomorphism

Then:

i) $f(e) = e'$ where e and e' are the identity element of G and G' respectively (ie). In an isomorphism identity is mapped onto identity

ii) $f(a^{-1}) = [f(a)]^{-1}$

proof:

$f(e) = e'$

ii) To prove $f(e) = e'$ it is enough to prove $a' f(e) = f(e) a' = a' \ \forall \ a' \in G'$

let $a' \in G'$. Since 'f' is bijection

Then $f(a) = a' \ \forall \ a \in G$

$$a' f(e) = f(a) f(e)$$
$$= f(ae) \quad [\because f \text{ is isomorphism}]$$
$$= f(a) \quad [\because e \text{ is identity of } G]$$
$$= a'$$

$$f(e) a' = f(a) f(e)$$
$$= f(ea) \quad [\because f \text{ is isomorphism}]$$
$$= f(a) \quad [\because e \text{ is identity of } G]$$
$$= a'$$

Scanned with CamScanner

Hence $a' f(e) = f(e) a' = a'$

$\therefore f(e)$ is an identity of G'

Since e' is identity of G' by hypothesis

$$f(e) = e'$$

(ii) It is enough to prove

$$f(a^{-1}) f(a) = f(a) f(a^{-1}) = e' \quad \forall a \in G$$

$f(a^{-1}) f(a) = f(a^{-1} a)$ [f is iso]

$= f(e)$ [since e is id G]

$= e'$ (by (i)]

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

$= f(e)$

$= e'$ (by (i)

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

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

Theorem 3.4b

Let $f: G \to G'$ be an isomorphism If 'G' is abelian, than G' is also abelian.

Proof.

Let $a', b' \in G'$.

There exists element $a, b \in G$

Such that $f(a) = a'$ and $f(b) = b'$

Scanned with CamScanner

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

$= f(ab)$

$= f(ba)$

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

Hence G' is abelian.

theorem 3.47

Let $f : G \to G'$ be an isomorphism

let $a \in G$. Then the order of a is equal to the order of $f(a)$. ie) Isomorphism preserves the order of each element in a group

proof..

let the order of a element is 'n'

Then 'n' is the least positive integer such that $a^n = e$.

Now,

$[f(a)]^n = f(a) \cdots f(a)$ ($f(a)$ written 'n' times)

$= f(a^n)$ (since f is an isomorphism)

$= f(e)$

$= e'$

Now, it possible let 'm' be a least positive integer such that $0 < m < n$ and $[f(a)]^m = e'$

$f(a^m) = f(a, a \cdots a)$ (a written 'm' times

$= f(a)f(a) \cdots f(a)$

$= [f(a)]^m = e'$

$f(a^m) = e'$

Scanned with CamScanner

w.k.T

$f(a) = e'$

$\therefore f(a^m) = f(e)$

since f bijection so that 1-1

we have $a^m = e$ which is contradicts and the definition of the order of a.

$\therefore$ 'n' is the least positive integer such that $[f(a)]^n = e'$

$\therefore$ The order of $f(a)$ is 'n'.

Theorem 3.48

let $f: G \to G'$ be an isomorphism.

If 'G' is cyclic then 'G' is also cyclic

Proof:

let a be generator of the group 'G'.

we shall prove that $f(a)$ is a generator of the group G'.

since 'f' is bijection, there exists $x \in G$, such that $f(x) = x'$

since $G = \langle a \rangle$

so that $x = a^n$ for some integer n.

Hence $x' = f(x)$

$= f(a^n)$

$= f(a, a \ldots \text{an time})$

Scanned with CamScanner

since $x' \in G'$ is arbitrary every element of G' is of the form $[f(a)]^n$ so that $G' = \langle f(a) \rangle$

Hence G' is cyclic

Theorem 3.5:

Cayley's Theorem.

Any finite group is isomorphic to a group of permutations

Step (1) → Finding a set of permulation G'

Step (2) → To prove G' is group

Step (3) → To map $\phi: G \to G'$ is isomorphism

Step 1:

let 'G' be a group of finite order n.

let $a \in G$.

Define $f_a: G \to G$ by $f_a(x) = ax$

In order said f_a is well-defined we may said f_a is bijection.

i) f_a is 1-1

$$f_a(x) = f_a(y)$$

$$ax = ay \quad \text{(By left cancelation law)}$$

$$x = y$$

$\therefore f_a$ is 1-1

ii) f_a is onto

let $y \in G$

$$f_a(a^{-1}y) = aa^{-1}y = ey = y$$

Scanned with CamScanner

Closure property

let $f_a, f_b \in G'$

$$(f_a \circ f_b)(x) = f_a(f_b(x))$$

$$= f_a(bx) \quad \text{(by (1))}$$

$$= (ab)x$$

$$= f_{ab}(x)$$

$$f_a \circ f_b = f_{ab} \in G'$$

Hence G' is closure under composition on mapping

ii) Identity property:-

let $f_e \in G'$ where 'e' is identity of G

let $f_a \in G$

$$(f_a \circ f_e)(x) = f_a(f_e(x))$$

$$= f_a(ex)$$

Scanned with CamScanner

$= f_a(x)$

$f_a \circ f_e = f_a$

$(f_e \circ f_a)(x) = f_e(f_a(x))$

$= f_e(ax) = e(ax) = ax = f_a(x)$

$f_e \circ f_a = f_a$

$\Rightarrow f_a \circ f_e = f_e \circ f_a = f_a$

$\therefore f_e$ is the identity of G_1

iii) Inverse property:

let $f_{a^{-1}} \in G_1$

$(f_a \circ f_{a^{-1}})(x) = f_a(f_{a^{-1}}(x))$

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

$= f_e(x)^a$

$f_a \circ f_{a^{-1}} = f_e$

$(f_{a^{-1}} \circ f_a)(x) = f_{a^{-1}}(f_a(x))$

$= f_{a^{-1}}(a(x)$

$= a^{-1}a\,x = ex$

$= f_e(x)^a$

$f_{a^{-1}} \circ f_a = f_e$

$\therefore f_{a^{-1}}$ is inverse of f_a

$\therefore f_e$ is the G_1 is group.

Step 3:

Define $\phi : G \to G_1$

by $\phi(a) = f(a) = f_a$

Scanned with CamScanner

i) ϕ is 1-1

$$\phi(a) = \phi(b)$$

$$f_a = f_b$$

$$f_a(x) = f_b(x)$$

$$ax = bx$$

$$a = b$$

ϕ is 1-1

ii) ϕ is onto

Let $f_a \in G$ then $\exists\ a \in G$ s.t $\phi(a) = f_a$

$\therefore \phi$ is onto

iii) ϕ is isomorphic

$$\phi(ab) = f_{ab}$$

$$= f_a \circ f_b = \phi(a) \circ \phi(b)$$

ϕ is an isomorphism

Hence $G \cong G$

Automorphism.

An isomorphism of a group 'G' to itself is called an Automorphism

Example.

Let G be any group. let $a \in G$.

Then $\phi_a : G \to G$ defined by $\phi_a(x) = axa^{-1}$ is an automorphism of G

Scanned with CamScanner

for let $x, y \in G$. Then.

$\phi_a(x) - \phi_a(x) = axa^{-1} - aya^{-1}$

$= x = y$ (by cancellation law)

$\therefore \phi_a$ is 1-1

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

$= (aa^{-1})x(aa^{-1}) = exe = x$

Hence $a^{-1}xa$ is the pre-image of x under ϕ_a.

Also.

$\phi_a(xy) = axya^{-1}$

$= (axa^{-1})(aya^{-1})$

$= \phi_a(x)\phi_a(y)$

Thus ϕ_a is an automorphism of G.

Definition.

Inner automorphism

The automorphism $\phi_a : G \to G$ defined in example '4' is called an inner automorphism of the group G.

Let G be a group. The set of all automorphism of G is denoted by $A(G)$ or G. The set of all inner automorphisms of G is denoted by $I(G)$.

Scanned with CamScanner

$\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ is an inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

3) The set of all 2×2 non-singular matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in R$ is a group under multiplication

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity

The inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = A^{-1} = \frac{1}{|A|}(\text{adj}^{\circ} A)$

$$= \frac{1}{|(ab - cb)|} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

where $(ad - bc) \neq 0$

4) N is not a group under usual addition

Since there is no element $e \in N \ni : x + e = x \ \forall x \in$

C^* is a group under usual multiplicatio

given by $(a+b)(c+id) : (ac - bd) + i(ad + bc)$

1) C^* is a group under usual multiplication

given by $(a+ib)(c+id) = (ac - bd) + i(ab + bc)$

2) $G = \{ a + b\sqrt{2} \ / a, b \in Z \}$

$G, +$ is a group.

Scanned with CamScanner

Scanned with CamScanner