By: *Muhammad Fiaz Hussain*
fiaz.hussain24@yahoo.com

Binary operation:

A binary operation on a non-empty set A is just a function $*: A \times A \to A$. Which is denoted by $*$.

Group:

A non-empty set G is said to be group if it said to be following properties,

1) Closure law holds in G.
2) Associative law holds in G such that
   $a*(b*c)=(a*b)*c$ forall $a,b,c \in G$
3) Identity holds in G,
   $a*e=e*a=a$ forall $a \in G$
4) Inverse exist in G,
   $a*a^{-1}=a^{-1}*a=e$ forall $a \in G$

Note: If commutative law holds in G. Then G is said to be abelion group.

Examples 1:

1) Z the set of integers is group under addition.
2) R the set of real numbers is also group under addition.
3) Q the set of rational numbers is group under addition.
4) $G=\{1,-1,i,-i\}$ is group under multiplication or $(G,.)$.
5) $G=\{\pm 1, \pm i, \pm j, \pm k\}$ is also group under multiplication or $(G,.)$.

Idempotent:

The elment $x \in G$ is said to be idempotent if,
$x^2=x$ for all $x \in G$

Theorem 1:

The only idempotent element in a group G is the identity element.

Proof:

Let $x \in G$ be an idempotent element, then by the definition,

$x^2=x$
$x^{-1}.x^2=x^{-1}.x$
$(x^{-1}.x).x=e$
$e.x=e$
$x=e$

Hence proved. ■

Example 2:

$G=\{1,-1\}$

Solution: To show that G is group we have following properties,

(i). G is closed under multiplication.
(ii). G have many real numbers between -1 and 1 so the associative law holds.
(iii). Identity element also exist.
(iv). Inverse exist.

So, G is group under multiplication or $(G,.)$.

Example 3:

Let, $G=\{1,\omega,\omega^2\}$ is complex cube root of unity.

Solution: To show that G is group we have,

.	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

i). G is closed under multiplication.
ii). $1,\omega,\omega^2 \in G$,
$1.(\omega.\omega^2)=(1.\omega).\omega^2=1$
associative law holds.
iii). Identity holds.
iv). Inverse exist,
inverse of 1 is 1.
inverse of ω is ω^2.
inverse of ω^2 is ω.
So, all the properties satisfied, Hence, G is group under multiplication or $(G,.)$.

Example 4:

$C_4=\{1,-1,i,-i\}$
where, $(i)^{-1}=-i$ & $(-i)^{-1}=i$.

Solution:

C_4 is fourth root of unity to prove group we have,

.	1	−1	i	$-i$
1	1	−1	i	$-i$
−1	−1	1	$-i$	i
i	i	$-i$	−1	1
$-i$	$-i$	i	1	−1

i). C_4 is closed under multiplication.
ii). Associative law holds.
iii). Identity of every element exist.
iv). Inverse exist,
Inverse of 1 is 1.
Inverse of -1 is -1.
Inverse of i is $-i$.
Inverse of $-i$ is i.
So, C_4 is group under multiplication.

Example 5:

$Q-\{0\}$ =Set of all non-zero rational numbers.
$R-\{0\}$ =Set of all non-zero real numbers.
$C-\{0\}$ =Set of all non-zero complex numbers.
are group under multiplication.

By: *Muhammad Fiaz Hussain*
fiaz.hussain24@yahoo.com

Example 6:

$G=\{\pm 1, \pm i, \pm j, \pm k\}$

where $i.j=k;\ j.k=i;\ k.i=j$

$j.i=-k;\ k.j=-i;\ i.k=-j$

$i^2=j^2=k^2=-1$

Solution:

All the properties of the group is satisfied, So, G is the group under multiplication. But not abelion group because,

$j.i=-k\neq i.j$

$k.j=-i\neq j.k$

$i.k=-j\neq k.i$

Example 7:

$A_{2\times 2}=\{\text{Set of all } 2\times 2 \text{ non-singular real matrices}\}$ under the usual multiplication is a group. e.g.,

$$A=\begin{bmatrix}1 & 0\\ 2 & 1\end{bmatrix} \ \&\ B=\begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}$$

are group under multiplication because A & B have their inverses(Non-singular).

But not abelion because,

$AB\neq BA$

Example 8:

Show that $G=\{\bar{1},\bar{2},\bar{3},\bar{4}\}$ is agroup of non-zero residue class of modulo 5.

Solution:

.	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

i). G is closed under multiplication.

ii). Associative law holds, for all $\bar{2},\bar{3},\bar{4}\in G$

$\bar{2}.(\bar{3}.\bar{4})=\bar{2}.\bar{2}=\bar{4}$

$(\bar{2}.\bar{3}).\bar{4}=\bar{1}.\bar{4}=\bar{4}$

iii). Identity of every element of G is exist.

iv). Inverse of every element of G exist.

Inverse of $\bar{1}$ is $\bar{1}$

Inverse of $\bar{2}$ is $\bar{3}$.

Inverse of $\bar{3}$ is $\bar{2}$.

Inverse of $\bar{4}$ is $\bar{4}$.

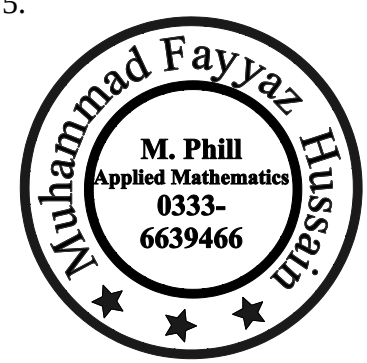
Hence all the properties of group satisfied. So, G is group under multiplication or $(G,.)$.

Example 9:

Show that $G=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\}$ is agroup of non-zero residue class of modulo 5.

Solution:

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$



i). G is closed under addition.

ii). Associative law holds, for all $\bar{2},\bar{3},\bar{4}\in G$

$\bar{2}+(\bar{3}+\bar{4})=\bar{2}+\bar{2}=\bar{4}$

$(\bar{2}+\bar{3})+\bar{4}=\bar{0}+\bar{4}=\bar{4}$

iii). Identity of every element of G is exist.

iv). Inverse of every element of G exist.

Inverse of $\bar{0}$ is $\bar{0}$

Inverse of $\bar{1}$ is $\bar{4}$

Inverse of $\bar{2}$ is $\bar{3}$.

Inverse of $\bar{3}$ is $\bar{2}$.

Inverse of $\bar{4}$ is $\bar{1}$.

Hence all the properties of group satisfied. So, G is group under addition or $(G,+)$.

Properties of group:

Theorem 2: (Cancellation laws)

For any element a,b,c in a group G.

i): $ab=ac\Rightarrow b=c$ (Left cancellation law)

ii): $ba=ca\Rightarrow b=c$ (Right cancellation law)

Proof:

For all $a,b,c\in G$

i): $ab=ac$

multiplying both sides by a^{-1}.

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

$(a^{-1}.a).b=(a^{-1}.a).c$ (By associative law)

$e.b=e.c$

$b=c$

Hence proved.

ii): $ba=ca$

multiplying both sides by a^{-1} on right side ·

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

$b.(a.a^{-1})=c.(a.a^{-1})$ (By associative law)

$b.e=c.e$

$b=c$

Hence proved. ■

By: *Muhammad Fiaz Hussain*
fiaz.hussain24@yahoo.com

Theorem 3: (Solution of linear equation)

For any two elements $a,b \in G,$ the equations $ax = b$ & $xa = b.$

Proof:

For any two elements $a,b \in G,$

$ax = b$

Multiplying both sides by a^{-1} on left side ·

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

$(a^{-1}.a).x = a^{-1}.b$ (By associative law)

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

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

Hence, $x = a^{-1}.b$ is the solution for $ax = b.$

Now, to check the unique solution we have,

$x_1, x_2 \in G$

$ax_1 = b \Rightarrow x_1 = a^{-1}.b$

$ax_2 = b \Rightarrow x_2 = a^{-1}.b$

From above relation,

$x_1 = x_2$

Hence, the solution of $ax = b$ is unique. Similarly $xa = b$ also unique solution. ■

Theorem 4:

For any $a,b \in G$

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

Proof:

Given that,

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

Consider,

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

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

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

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

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

Now,

$(ab).(ab)^{-1} = e \ (ii)$

From (i) & (ii)

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

Hence, proved. ■

Theorem 5:

For any element a of a group G, the following exponential rule holds,

i). $a^m = a.a.a....a(m \text{ factors})$

ii). $(a^{-1})^m = a^{-m}$

iii). $a^m.a^n = a^{m+n}$

iv). $(a^m)^n = a^{mn}$

Proof:

(i). $a \in G,$

$a^0 = e = 1$

$a^1 = a^0.a$

$a^2 = a.a$

$a^3 = a.a.a$

.....

$a^m = a.a.a....a(m \text{ factors})$

Hence, proved.

ii). $(a^{-1})^m = a^{-1}.a^{-1}.a^{-1}...a^{-1}(m \text{ factors})$

By (i),

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

Hence, proved.

iii). $a^m.a^n = a^{m+n}$

Case I. We have proved by induction method,

for $n = 1,$

$a^m.a^1 = a^{m+1} \ \forall \ m \in Z^+$

true for $n = 1,$

now, for $n = k,$

$a^m.a^k = a^{m+k}$

also true for $n = k,$

now for $n = k+1,$

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

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

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

Also true for $n = k+1,$ Hence true for all values of $n \in Z^+.$

So, $a^m.a^n = a^{m+n}.$

Case II.

When $m < 0$ & $n < 0,$

Let $m = -p$ & $n = -q,$

$a^m.a^n = a^{-p}a^{-q}$

$a^m.a^n = a^{-p\ -q}$

$a^m.a^n = a^{-(p+q)}$

by (ii),

$a^m.a^n = (a^{-1})^{p+q}$

Again, $a^{-p}a^{-q} = a^m.a^n$

Hence, true.

Case III.

if $m = 0$ & $n \neq 0,$

or $n = 0$ & $m \neq 0,$

$a^m.a^n = a^0.a^n = a^n$

similarly,

$a^m.a^n = a^m.a^0 = a^m$

So, true.
Case IV.
for $m<0$ & $n>0 \Rightarrow m+n<0$,
and $-m-n>0$,
$a^{-m-n}.a^m = a^{-m-n+m} = a^{-n}$ (1)
$a^{m+n} = a^{m+n}.e$
$a^{m+n} = a^{m+n}.(a^{-n}.a^n)$
$a^{m+n} = a^{m+n}.(a^{-m-n}.a^m).a^n$
by (1),
$a^{m+n} = (a^{m+n}.a^{-m-n}).a^m.a^n$
$a^{m+n} = e.a^m.a^n$
$a^{m+n} = a^m.a^n$
So, true.
Case V.
for $m>0$ & $n<0 \Rightarrow m+n?0$,
$a^m.a^{-n} = a^m.a^{-1}.a^{-1}.a^{-1}...a^{-1}(n \text{ factor})$
by (i),
$a^{m+n} = a^{m+n}.e$
$a^{m+n} = a^{m+n}.(a^{-n}.a^n)$
$a^{m+n} = a^{m+n}.(a^{-m-n}.a^m).a^n$
by (1),
$a^{m+n} = (a^{m+n}.a^{-m-n}).a^m.a^n$
$a^{m+n} = e.a^m.a^n$
$a^{m+n} = a^m.a^n$
So, true.
Hence proved for all values of $m,n \in Z$, so,
$a^{m+n} = a^m.a^n$.
iv). $(a^m)^n = a^{mn}$
Case I. we have to prove by induction method,
for $n=1$,
$(a^m)^1 = a^m \ \forall \ m \in Z^+$
true for $n=1$,
now, for $n=k$,
$(a^m)^k = a^{mk}$
also true for $n=k$,
now for $n=k+1$,
$(a^m)^{k+1} = a^{mk+m}$
$(a^m)^{k+1} = a^{(m+k)}.a^1$
$(a^m)^{k+1} = a^{m(k+1)}$
Also true for $n=k+1$, Hence true for all values of $n \in Z^+$.
So, $(a^m)^n = a^{mn}$.
Case II.
for $n<0$,
let, $n=-p$,
$(a^m)^{-p} = ((a^m)^{-1})^p$
$(a^m)^{-p} = (a^{-m})^p$ by (i)
So, true.
Case III.
for $n=0$,
$(a^m)^0 = e = a^0 = a^{m(0)}$
Hence, $(a^m)^n = a^{mn} \ \forall \quad m,n \in Z$. ■

Order of a group:

The number of element in a group G is called order of G. Which is denoted by $|G|$.

Note:

(i). A Group G is said to be finite if G is consist of finite number of elements.
(ii). A Group G is said to be infinite if G is consist of infinite number of elements.

Order of elements of group:

Let $(G,*)$ be a group and $a \in G$ if there exist smallest positive integer n such that, $a^n = e$. Then n is called order of element n in G.

Theorem 6:

Let G be a group. Let $a \in G$ have order n then for any integer k, $a^k = e$ iff $k = qn$, where k is any integer.

Proof:

Suppose that $a \in G$ and order of a is n then,
$a^n = e$
Now, by division algorithm,
$k = qn + r; \ 0 \le r < n$ (1)
Where r and q are any integers,
as given,
$a^k = e; \ k \in Z$
From (1),
$a^k = a^{qn+r}$
$a^k = (a^n)^q.a^r$
since order of a is n, so,
$e = (e)^q.a^r$
Hence,
$a^r = e$
Proved.
Conversely, suppose that $k = qn$ then we have to prove that order of a is k,
$k = qn$
$a^k = a^{qn} = (a^n)^q$
since order of a is n, so,
$a^k = e^q = e$

By: *Muhammad Fiaz Hussain*
fiaz.hussain24@yahoo.com

$a^k = e$ for $k \in Z$

Hence, proved. ■

Example 10:

Show that $G = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ is group under multiplication of modulo 8. Find the order of each element of G.

Solution:

.	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

From teh Caley's table.

The order of $\bar{1}$ is 1.

The order of $\bar{3}$ is $2. \Rightarrow \bar{3}^2 = \bar{1}$

The order of $\bar{5}$ is $2. \Rightarrow \bar{5}^2 = \bar{1}$

The order of $\bar{7}$ is $2. \Rightarrow \bar{7}^2 = \bar{1}$

Example 11:

Let G be group and $a, b \in G,$ then show that,

i). The order of a and a^{-1} are equal.

ii). The order of ba and ab are equal.

iii). The order of a and $b^{-1}ab$ are equal.

Proof:

(i). Let $a \in G,$ and order of a is n then,

$a^n = e,$ (1)

Where n is the smallest positive integer.

Because G is the group so inverse of every element exist, Let $a^{-1} \in G,$

and order of a^{-1} is $m,$ then,

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

$a^{-m} = e$

mulpying boths ides by a^m

$a^m.a^{-m} = a^m.e$

$e = a^m$ (2)

where m is smallest positive integer,

from (1) and (2),

$a^n = a^m \Rightarrow m = n$

Hence proved.

ii). Let $a, b \in G$ the order of ab is m such that,

$(ab)^m = e$ (3)

As we know that,

$(ab)^m = ab.ab.ab...ab(m \text{ factor})$

by (3)

$ab.ab.ab...ab(m \text{ factors}) = e$

multiplying left sides by a^{-1} and right side by $a,$

$a^{-1}.ab.ab.ab...ab.a(m \text{ factors}) = a^{-1}.e.a$

$ba.ba.ba....ba(m \text{ factors}) = e.a^{-1}.a$

$ba.ba.ba....ba(m \text{ factors}) = e.e$

$ba.ba.ba....ba(m \text{ factors}) = e$

Also we can write by using the theorem,

$(ba)^m = e$ (3)

from (3) and (4),

$(ab)^m = (ba)^m$

which shows that order of ab and ba are same.

iii). Let $a \in G$ and order of a is $m.$

$a^m = e$ (5)

multiplying left sides by b^{-m} and right side by $b^m,$

$b^{-m}a^m b^m = b^{-m}eb^m$

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

$(b^{-1}ab)^m = e$ (6)

from (5) and (6),

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

Which shows that order of a and $b^{-1}ab$ are equal.

Example 12:

In a group of even order, prove that there is at least one element of order 2.

Proof:

Let G be a group of even order then there is a non-identity element in G are the odd in number.

Because G is group then the inverse of every element exist.

Suppose,

$e \in G \Rightarrow e^{-1} = e$ (1)

Let $a \in G$ be the fnon- identity elemnet, then by (1),

$a^{-1} = a$

multiplying both sides by $a,$

$a.a^{-1} = a.a \Rightarrow e = a^2$

Which shows that order of a is 2.

Hence, proved.

Example 13:

Let G be a group and a be an element of odd number in G. Then, there exist an element b in G such that, $b^2 = a.$

Proof:

Let $a \in G,$ and n be the positive integer, given that order of a is odd number, then,

$a^{2n+1} = e$ (1)

$a^{2n}.a^n = e$

$a.a^2.a^3...a^n, a^{m+1}..a^{2m} \in G$

By: *Muhammad Fiaz Hussain*
fiaz.hussain24@yahoo.com

$b = a^{m+1} \Rightarrow b^2 = a^{2m+2}$

$b^2 = a^{2m+1}.a^1$

by (1),

$b^2 = e.a$

$b^2 = a$

Hence, proved.

Subgroup:

Let $(G,*)$ be a group and H be a non-empty subset of G. Then H is said to be subgroup of G. If itself a group under the same binary operation $*$ with the following axioms of group.

Examples 14-16:

$(Z,+)$ set of all integers is subgroup of $(Q,+)$.

$(Q,+)$ set of rational is subgroup of $(R,+)$.

The set of cube root of unity is subgroup of complex numbers without zero. e.g. $C-\{0\}$.

Trivial and non-trivial subgroups:

Every group G has at least two subgroups namely, G itself and $\{e\}$. These subgroups are called trivial subgroups.

Any other subgroups of G are called non-trivial subgroups.

Theorem 7:

Let $(G,*)$ be a group. Then a non-empty subset H of G is subgroup of G iff $\forall\, a,b \in H \Rightarrow ab^{-1} \in H$.

Proof:

Suppose that H is the subgroup of G. Then we have to prove that $\forall\, a,b \in G \Rightarrow ab^{-1} \in H$.

Let, $a \in H$ and $b \in H$.

Since H is the subgroup of G then by the definition H itself a group so the every element of H has inverse. Hence,

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

S0,

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

Conversely suppose that,

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

then we have to prove that G is group.

To prove G is group we satisfy the following axioms (properties).

1). Since $\forall\, a,b \in H \Rightarrow ab^{-1} \in H$ so G is closed.

2). $a,b,c \in H \Rightarrow a.(bc)^{-1} \in H$

$a.c^{-1}b^{-1} \in H$ (Since H is subgroup so every element have inverse)

Associative law holds.

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

$e \in H$

identity exist.

4). $e,a \in H \Rightarrow e.a^{-1} \in H$

$a^{-1} \in H$

Inverse exist.

Hence, all the properties of group satisfied so, $(G,*)$ is group. ■

Theorem 8:

The intersection of any collection of subgroups of a group G is subgroup of G.

Proof:

Let, $H = \cap\{H_i; i \in I\}$

where $\{H_i; i \in I\}$ is the family of subgroups of group G.

Let, $i \in I, a,b \in H_i \Rightarrow ab^{-1} \in H_i$ (By previuos theorem)

so, $ab^{-1} \in \cap\{H_i; i \in I\} = H$

Hence, H is subgroup of G. ■

Theorem 9:

Let G be a group H be the subgroup of G. Then the set $aHa^{-1} = \{aha^{-1}; h \in H\}$ is a subgroup of G.

Proof:

Suppose that, $x \in aHa^{-1}$ and $y \in aHa^{-1}$ then,

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

$xy^{-1} = ah_1(a^{-1}.a)h_2^{-1}a^{-1}$

$xy^{-1} = ah_1(e)h_2^{-1}a^{-1}$

$xy^{-1} = ah_1h_2^{-1}a^{-1}$

$xy^{-1} = (ah_1).(a.h_2)^{-1}$

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

So,

$xy^{-1} = (ah_1).(a.h_2)^{-1} \in aHa^{-1}$.

Hence, aHa^{-1} is a subgroup of G. ■

Theorem 10:

The union $H \cup K$ of two subgroups H and K of a group G is the subgroup of G if and only if $H \subset K$ or $K \subset H$.

Proof:

Let H and K are two subgroups of group G. Then we have to prove that $H \cup K$ is subgroup of G.

Then,

$H \cup K = H$ or $H \cup K = K$

Hence, H and K aare subgroups of G. So, $H \cup K$ also subgroup of G.

Conversely suppose that $H \cup K$ is subgroup of G then we have to show that $H \subset K$ or $K \subset H$.

Contrary, suppose that $H \not\subset K$ or $K \not\subset H$.

Let $a \in H / K$ or $b \in K / H$

butt there, $a,b \in H$ or $a,b \in K$, then,

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

$b, ab \in K \Rightarrow (ab).b^{-1} \in K \Rightarrow a \in K$

which is contradiction, because,

$H / K = \Phi$ and $K / H = \Phi$

Hence, $H \subset K$ or $K \subset H$. ■

Note:

Let H and K be the two subgroups of group G. Then there is not need to be subgroup of G. e.g.

$G = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ modulo 8.

$H = \{\bar{1}, \bar{3}\}$; $K = \{\bar{1}, \bar{5}\}$

$H \cup K = \{\bar{1}, \bar{3}, \bar{5}\}$

$\bar{3}.\bar{5} = \bar{7}$ or $\bar{5}.\bar{3} = \bar{7} \notin H \cup K$

So, $H \cup K$ is not closed. Hence, $H \cup K$ is not subgroup of G.

Example 18:

Find the subgroups of group $G = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ with the following table.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Solution:

Given table shows that operation is addition with modulo 4. In which, subgroups are,

$H_1 = \{\bar{0}\}$, $H_2 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = G$

$H_3 = \{\bar{0}, \bar{2}\}$

where, H_1 and H_2 are trivial subgroups and H_3 non-trivial subgroup of G.

Example 18:

Find the subgroups of group $G = \{e, a, b, c\}$ with the following table.

.	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Solution:

The given table show Klein's four group,

$a^2 = b^2 = c^2 = e$

$ab = c$; $ac = b$

The subgroups are,

$\{e, a\}, \{e, b\}, \{e, c\}$ are non-trivial subgroups.

Example 20:

Let $C - \{0\}$ be the group of all non-zero complex numbers under multiplication, prove that $H = \{a + ib \in C - \{0\}; a^2 + b^2 = 1\}$ is subgroup.

Proof:

Suppose that,

$a_1 + ib_1, a_2 + ib_2 \in H$

$\Rightarrow (a_1 + ib_1)(a_2 + ib_2)^{-1} = \frac{a_1 + ib_1}{a_2 + ib_2} \times \frac{a_2 - ib_2}{a_2 - ib_2}$

(By theorem)

$(a_1 + ib_1)(a_2 + ib_2)^{-1} = \frac{(a_1a_2 + b_1b_2) + i(a_2b_1 - a_1b_2)}{a_2^2 + b_2^2}$

$(a_1 + ib_1)(a_2 + ib_2)^{-1} = (a_1a_2 + b_1b_2) + i(a_2b_1 - a_1b_2) \in H$

where, $a_2^2 + b_2^2 = 1$

Now,

$(a_1a_2 + b_1b_2)^2 + (a_2b_1 - a_1b_2)^2 = a_1^2a_2^2 + b_1^2b_2^2$

$+ 2a_1a_2b_1b_2 + a_2^2b_1^2 + a_1^2b_2^2 - 2a_1a_2b_1b_2$

$(a_1a_2 + b_1b_2)^2 + (a_2b_1 - a_1b_2)^2 = a_1^2a_2^2 + b_1^2b_2^2$

$+ a_2^2b_1^2 + a_1^2b_2^2$

$(a_1a_2 + b_1b_2)^2 + (a_2b_1 - a_1b_2)^2 = a_1^2(a_2^2 + b_2^2)$

$+ b_1^2(b_2^2 + a_2^2)$

$(a_1a_2 + b_1b_2)^2 + (a_2b_1 - a_1b_2)^2$

$= (a_1^2 + b_1^2).(a_2^2 + b_2^2)$

$(a_1a_2 + b_1b_2)^2 + (a_2b_1 - a_1b_2)^2 = 1.1$

$(a_1a_2 + b_1b_2)^2 + (a_2b_1 - a_1b_2)^2 = 1$

Hence, H is subgroup.

Cyclic group:

A group G is said to be cyclic if every element of G is power of one, and same element say $a \in G$.

These elements are called generator of G.

If there at least positive integer n such that $a^n = e$ then G is said to be finite cyclic group and written as,

$G = < a; a^n = e >$

(Read as G is cyclic of order n).

Theorem 11:

Every subgroup of cyclic group is cyclic.

Proof:

Suppose that G be a cyclic group and generated by a. Let H be the subgroup of G. Suppose that $k \in G$ such that, $a^k = e \in H$. We have to show that every element of H is power of k.

For these let $a^m \in H$.

By division algorithm,

$m = qk + r$; $0 \le r < k$

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

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

$(a^k)^{-q}.a^m = .a^r \in H;\ r > k$

Which is contradiction because $r = 0$.

Then,

$m = qk$

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

Hence, H is cyclic. ■

Theorem 12:

Let G be a cyclic group of order n generated by a. Then for each positive divisor d of n, there is unique subgroup (of G) of order d.

Proof:

Let, $G =< a; a^n = e >$

Let d is the positive divisor of n then there is integer q such that,

$n = dq$

consider,

$b = a^q$

$b^d = a^{dq}$

$b^d = a^n$

$b^d = e$

So,

$H =< b; b^d = e >$

is required subgroup.

To show that H is unique suppose that K is another subgroup of G of order then K is generated by single element $c = a^k$. Where k is least positive integer.

$c = a^k$

$c^d = a^{dq}$

$c^d = a^n$

$c^d = e$

where, $dk = n \Rightarrow k = \frac{n}{d} = q,$

Hence,

$b = a^q = a^k = c$

$b = c$

So, H is unique. ■

Theorem 13:

Every cyclic group is abelion.

Proof:

Let G be a cyclic group generated by a single element a.

Let, $x, y \in G,$ then there is positive integers m and k such that,

$x = a^k;\ y = a^m$

$xy = a^k.a^m$

$xy = a^{k+m} = a^{m+k}$

$xy = a^m.a^k$

$xy = yx$

Hence, G is abelion cyclic group. ■

Example 21:

If G is cyclic group of even order then prove that there is only one subgroup of order 2 in G.

Proof:

Let, G be a cyclic group of even order such that,

$G =< a; a^{2n} = e >$

2n show that the order of G is even.

(By using the theorem "If a positive integer d divides the order of G (|G|) then G has exactly one subgroup of order d.")

Now,

$|G| = 2n$

where 2 divides 2n. So, G has only one subgroup of order 2.

Example 22:

Find all subgroups of a cyclic subgroup of order 12.

Proof:

The divisor of 12 are,

1,2,3,4,6,12.

subgroup of order $1 = \{e\}$

subgroup of order $12 = G$ itself.

subgroup of order $2 = (a^6)^2 = \{a^6, a^{12} = e\}$

subgroup of order $3 = (a^4)^3 = \{a^4, a^8, a^{12} = e\}$

subgroup of order $4 = (a^3)^4 = \{a^3, a^6, a^9, a^{12} = e\}$

subgroup of order $6 = (a^2)^6 = \{a^2, a^4, a^6, a^8, a^{10}, a^{12} = e\}$

Cosets:

Let H be the subgroup of G and $a \in G$. Then the set,

$aH = \{ah; h \in H\}$ Left coset

$Ha = \{ha; h \in H\}$ Right coset

is said to coset of H in G.

Note: The left or right cosets of H in G with identity element is H itself.

$eH = \{eh; h \in H\} = H$

$He = \{he; h \in H\} = H$

If the binary operation is "+" then the coset can be written as,

$a + H = \{a + h; h \in H\}$

Example 23:

$G = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ be the group of residue classes modolu 6. Then, $H = \{\bar{0}, \bar{2}, \bar{4}\}$ is subgroup G. There are only two left cosets of H in Gand these are

$\bar{0} + H = H$ and $\bar{1} + H = \{\bar{1}, \bar{3}, \bar{5}\}.$

By: *Muhammad Fiaz Hussain*
fiaz.hussain24@yahoo.com

Example 24:

$G=\{\bar{1},\bar{3},\bar{5},\bar{7}\}$ be the group of residue classes modulo 8. Find the cosets.

Solution:

$\cdot$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

Here proper subgroups are,

$H_1=\{\bar{1},\bar{3}\},\ H_2=\{\bar{1},\bar{5}\},\ H_3=\{\bar{1},\bar{7}\}$

The cosets are,

$\bar{1}.H_1=\{\bar{1},\bar{3}\}=H_1$

$\bar{5}.H_1=\{\bar{5},\bar{7}\}$

$\bar{7}.H_1=\{\bar{7},\bar{5}\}$

Partition:

The collection of subsets is known as the partition of sets.

The partition of set A is,

$\{A_i;i\in I\}$ of the set $A=\cup\{A_i;i\in I\}$ and $A_i\cap A_j=\Phi\ \forall\ i,j\in I$ and $i\neq j$.

Theorem 14:

Let H be the subgroup of group G. Then the set of all left or right cosets of H in G define the partition of G.

Proof:

Suppose, $\Omega=\{ah;a\in G;h\in H\}$ be the collection of all the left cosets of H in G.

Now, $a\in G\Rightarrow ae\in H$ (Because H is subgroup of G so identity exist.)

So,

$G\subset\cup\Omega$

wherer $\cup\Omega$ is the collection of the subsets contained in G.

Hence, $G=\cup\Omega$.

consider aH and bH are the cosets of H in G, then,

$x\in aH\cap bH\Rightarrow x=ah_1=bh_2$ for some $h_1,h_2\in H$.

$\Rightarrow a=bh_2h_1^{-1}=bh_3$ (1)

where, $h_2h_1^{-1}=h_3\in H$

Since H si subgroup thus $a\in bH$

From (1).

$ah=bh_3h$ also an element of bH.

Hence, $aH\subset bH$ or $bH\subset aH$

which shows,

$aH=bH$

contradiction because we have

$aH\cap bH=\Phi$

therefore Ω shows the partition of G. ■

Index H in G: [G:H]

The number of distinct left or right cosets of subgroup H in G is called the index H in G and denoted by, [G:H].

Example 25:

Find the distnict right (left) cosets of $E=\{0,\pm2,\pm4,.....\}=\{2n;n\in Z\}$ in a group $(Z,+)$.

Solution:

There are two right cosets of E in Z.

Which are 0 and 1,

$0+E=\{0+2n;n\in Z\}=E$

$1+E=\{2n+1;n\in Z\}=O$ (odd numbers)

Now,

$(0+E)\cup(1+E)=E\cup O=Z$ (set of integers)

$(0+E)\cap(1+E)=\Phi$

Therefore index of E in Z is 2.

Theorem 15: (Lagrange's theorem)

The order of a subgroup of a finite group divides the order of group.

Proof:

Let G be the group and H be the subgroup of G.

Suppose that the order of G is n and the order of H is m. Then by the definition,

$|H|=m$ and $|G|=n$

Since, the order of G is finite, So, the set of all distnict left cosets of H in G are also finite.

(By the previous theorem, "Let H be the subgroup of G then the all left (right) cosets of H in G define the partition in G.")

So, $G=\bigcup_{i=1}^{k}a_iH$ (1)

where, $a_iH\cap a_jH=\Phi$ for $i\neq j$.

let we define a mapping,

$\Psi:H\to a_iH$

$\Psi(h)=a_ih;\ h\in H$

Ψ is onto, also,

$\Psi(h_1)=\Psi(h_2);\ h_1,h_2\in H$

$a_ih_1=a_ih_2$

$h_1=h_2$ (By left cancellation law)

Hence, Ψ is one-to-one. So, the numbers of H and a_iH are the same.

From (1),

$G=\bigcup_{i=1}^{k}a_iH$

$n=m+m+m+...+m$ (k times)

By: *Muhammad Fiaz Hussain*
fiaz.hussain24@yahoo.com

$n = km$
$|G| = k|H|$
$|H| \backslash |G|$
Hence, proved. ■

Corollary:
The index of an element of finite group divides the order of group.

Proof:
By the Lagrange's theorem,
$|G| = k|H|$ (1)
k being the numbers of the distnict left(right) cosets of H in G,
From (1) k divodes the ordder of G. But $k = [G : H]$,
$k \backslash |G| \Rightarrow [G : H] \backslash |G|$
Hence, proved.

Corollary:
A group G whose order is prime number is necessarily cyclic.

Proof:
Let G be a group of prime order p.
$|G| = p$
Let $a \in G$ be the non-identity element of G. Let H be the cyclic gro\up of order k.
$|H|=k$
By the Lagrange's theorem
$k \backslash p$ (Order of H divides the order of G)
since p is prime number and the divisor of p is 1 and p itself. But we choose already H is non-identity element so,
$k = p$
Hence, order of H and G are same.
By this equality, H is cyclic so G also cyclic.

Permutation:
Let X be a non-empty set. A bijective mapping $f : X \to X$ is called permutation on X. The set of all permutation on X is denoted by S_x .

Theorem 16:
The set S_n of all permutation on a set X with n-elements is a group under operation of composition of permutation.

Proof:
to show group we have following axioms,
i). Let f and g be two mappings on X,
$f : X \to X$ and $g : X \to X$
$fog(x) = f(g(x)); \ x \in X$
Since the composition of bijective mapping also bijective mapping. So, the fog also the permutation on X. Hence, S_n is closed under composition.
ii). Let *f, g* and *h* be the mappings on X, then,
$((fog)oh)(x) = fog(h(x)); \ x \in X$
$((fog)oh)(x) = f(g(h(x))); \ x \in X$
$((fog)oh)(x) = f(goh(x)); \ x \in X$
$((fog)oh)(x) = fo(goh)(x); \ x \in X$
$(fog)oh) = fo(goh)$
Associative law holds.
iii). Let *I* be the identity on X,
$I : X \to X$
$I(x) = x; \ x \in X$
So, $foI(x) = f(I(x)); \ x \in X$
$foI(x) = f(x); \ x \in X$
$foI = f$
So, identity exist.
iv): Let $f^{-1} : X \to X$
$f(x) = y \Rightarrow f^{-1}(y) = x$
$(f^{-1}of)(x) = f^{-1}(f(x)); \ x \in X$
$(f^{-1}of)(x) = f^{-1}(f(x)); \ x \in X$
$(f^{-1}of)(x) = f^{-1}(y); \ x \in X$
$(f^{-1}of)(x) = x; \ x \in X$
Now,
$(fof^{-1})(y) = f(f^{-1}(y)); \ x \in X$
$(fof^{-1})(y) = f(x); \ x \in X$
$(f^{-1}of)(y) = y; \ x \in X$
Inverse exist.
Hence, all the properties of group satisfied.
So, S_n is group under composition. ■

Note:
i). The group S_n is called the symmetric group of degree *n*.

ii). Every element of S_n is permutation of n objects takes n-time. There are $n!$ permutations.
Hence the order of S_n is $n!$.

Example 26:
Find the permutations, if, $X = \{1, 2, 3\}$

Solution:
$n = 3$ so the order of S_3 is $3! = 6$. (means 6 permutations)
$I = (1\,2\,3); \ f_1 = (2\,3\,1); \ f_2 = (3\,1\,2)$
$f_3 = (1\,3\,2); \ f_4 = (3\,2\,1); \ f_5 = (2\,1\,3)$
$S_3 = \{I, f_1, f_2, f_3, f_4, f_5\}$
To calculate the permutations we have,

$$I=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix};\ f_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix};\ f_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$
$$f_3=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix};\ f_4=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix};\ f_5=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

To find the composition, $f_5 of_1$.

$(f_5 of_1)(1)=f_5(f_1(1))=f_5(2)=1$
$(f_5 of_1)(2)=f_5(f_1(2))=f_5(3)=3$
$(f_5 of_1)(3)=f_5(f_1(3))=f_5(1)=2$

So, $f_5 of_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=f_3$

Similarly,

$$f_1 of_5=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=f_4$$

Hence, $f_5 of_1\neq f_1 of_5$

So, S_3 is non-abelion.

Consider, $f_1=a;\ f_5=b$

then, $f_2=a^2,\ f_4=ab$

$a^3=b^2=(ab)^2=I$

$ba=f_3=a^2b$

using this relation we construct the Caley's table,

o	I	a	a^2	b	ab	a^2b
I	I	a	a^2	b	ab	a^2b
a	a	a^2	I	ab	a^2b	b
a^2	a^2	I	a	a^2b	b	ab
b	b	a^2b	ab	I	a^2	a
ab	ab	b	a^2b	a	I	a^2
a^2b	a^2b	ab	b	a^2	a	I

Example 27:

Find fog and gof, if,

$$f=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix};\ g=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$$
$$fog=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$$
$$fog=\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}$$
$$gof=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$$
$$gof=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}$$

Which show that,

$fog\neq gof$

Example 28:

Find the composition of the permutation,

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

Similarly,

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

Hence, $\alpha\beta=\beta\alpha$.

Cycles:

Let $a_1,a_2,a_3,..,a_k$ where $a_k\in\{1,2,3,..,k\}$.

A permutation $\sigma\in S_n$ is called a cycle of length k and $\sigma(x)=x,\ \forall x=\{1,2,3,..,k\}$. We can write a cycle as $\{a_1,a_2,a_3,..a_k\}$ and say that σ acts on $\{a_1,a_2,a_3,..a_k\}$ e.g.

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

we can write these cycles as,

$1\to 2\to 3\to 4\to 5\to 6$

one cycle of length 6.

so,

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

Note:

The composition of two cyclic permutations need not be cyclic permutaions.

e.g.

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

Let,

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

Hence,

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

Disjoint cycles:

Two or more than two cycles which have no common elements are called mutually disjoint cycles. e.g.

$(2\ \ 6)$ and $(4\ \ 5)$ are disjoint cycles.

$(1\ \ 5\ \ 2)$ and $(5\ \ 2)$ are not disjoint cycles.

Example 29:

$\alpha=(1\ \ 2\ \ 3);\ \beta=(4\ \ 5\ \ 6)$

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

From (1) and (2),

$\beta\alpha=\alpha\beta$

So, α and β are mutually disjoint cycles.

Theorem 17:

Every permutation of degree n can be written as a product of cycles acting on mutually disjoint cycles.

Proof:

Let S^n be the set of all cycles of *n*-elements, and α be the permutation of *n*-degree. Let α has only one element in which α acts. Suppose,

$$a_1\overset{\alpha}{\to}a_2, a_2\overset{\alpha}{\to}a_3\overset{\alpha}{\to}....a_{k-1}\overset{\alpha}{\to}a_k, a_k\overset{\alpha}{\to}a_1$$

since k is the finite then there is a number *n* such that,

$$a_n\overset{\alpha}{\to}a_1$$

α is the cyclic permutation so, the α is the part of cyclic permutation.

$\alpha_1=(a_1,a_2,...,a_n)$

Now put $n=k$ then $\alpha=\alpha_1$ is the required cyclic decomposition of α as cyclic permutation.

Now, if $n<k$ then *b*, is different from $(a_1,a_2,...,a_n)$.

$$b_1\overset{\alpha}{\to}b_2, b_2\overset{\alpha}{\to}b_3\overset{\alpha}{\to}....b_{p-1}\overset{\alpha}{\to}b_p, b_p\overset{\alpha}{\to}b_1;\ 1\le i\le p$$

Hence, the given permutation is injective mappings. So, effect of part α on cyclic permutation is,

$\alpha_2=(b_1,b_2,...,b_p)$

So, we have two α cyclic permutations, if $n+p=k$, then α is the composition of two cycles α_1 and α_2. If $n+p<k$ then the process repeated again.

Every time process extracting the cycles. After the finite number of each because k is finite. Thus there is a natural number q, such that,

$\alpha_q=(c_1,c_2,...,c_q)$ (1)

Where, c_i's occurs between a_i's and b_i's.

Where each α acts as mutually disjoint subset of X and are uniquely determined. Since, any two permutations acting on mutually disjoint sets commute. So, the part from the order in which α_i's are taken. The expression (1) for α is unique. ■

Transposition:

A cycled of length 2 is called a transposition e.g.

$$\tau=\begin{pmatrix}a&b\\b&a\end{pmatrix}$$

a and *b* are interchanging in this permutation and other element remain fixed is a transposition.

Theorem 18:

Every cyclic permutation can be expression as a product of transposition.

Proof:

Suppose, $\alpha_1=(a_1,a_2,...,a_n)$ be the cyclic permutation. Consider,

$\alpha'=(a_1\ \ a_2)(a_1\ \ a_3)..(a_1\ \ a_k)$ (1)

which shows that,

$$a_1\overset{\alpha}{\to}a_2, a_2\overset{\alpha}{\to}a_3\overset{\alpha}{\to}....a_{k-1}\overset{\alpha}{\to}a_k, a_k\overset{\alpha}{\to}a_1$$

Hence, the effect of α and α' are same. So, $\alpha=\alpha'$ is the product of transposition.

Now, $(a\ \ b)(b\ \ a)=I$ be the number such pair of transposition can be inserted between the pairs $(a_1\ \ a_i),(a_i\ \ a_{i+1})$ involved in α. Hence, α be the expressed as the product of transpositions. Possibly in infinitely many ways. ■

Theorem 19:

Every permutation of degree n can be expressed as a product of transposition.

Proof:

As we know that the every permutation can be as a product of dis joint cycles. Conversely, every cycle can be expressed as a product of transposition in

infinitely many ways. (By the above theorem). So, any element of S_n can be expressed as a product of transposition in infinitely many ways. ■

Theorem 20:

Let a permutation α in S_n be written as a product of m transpositions and as a product of p transpositions. Then m-p is a multiple of 2. This implies that both m and p are even or both of them are odd.

OR

Let α be the permutation as a product of transposition, $\Rightarrow m \equiv p \pmod 2$.

Proof:

Suppose the product of transpositions,

$$p = \prod_{i<j}^{n}(x_i - x_j)$$

$$p = (x_1 - x_2)(x_1 - x_3)...(x_1 - x_n)$$

$$(x_2 - x_3)(x_2 - x_4)...(x_2 - x_n)$$

$$.....(x_{n-1} - x_n)$$

$$p\alpha = \prod_{i<j}^{n}(x_{(i)a} - x_{(j)q})$$

Now for any transpositions,

$\tau = (k,l)$ in S_n. Where $k \neq l$.

$$(p)\tau = \prod_{i<j}^{n}(x_{(i)t} - x_{(j)t})$$

every factors of p that contains neither x_k nor x_l remain unchanged in $\tau(p)$. The factor $(x_k - x_l)$ of p becomes $-(x_l - x_k)$ in $\tau(p)$.those factors of p which contain either x_k of x_l But not both x_k and x_l.

$\pm \quad (x_m - x_k) \quad (x_m - x_l)$ where $m \neq k,l$.

Such the product remain unchanged in $\tau(p)$. Thus it follows that, $\tau(p) = -p$,

By successive applications of transpositions in α, in both cases,

$$(p)\alpha = (p)\lambda_1\lambda_2...\lambda_m = (-1)^m p \quad (1)$$

$$(p)\alpha = (p)\mu_1\mu_2..\mu_m = (-1)^p p \quad (2)$$

From (1) and (2),

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

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

$p - m$ is multiple of 2.

$\Rightarrow 2 \setminus p - m \Rightarrow m \equiv p \pmod 2$. ■

Even and odd permutation:

A permutation α is called even if it can be expressed as a product of even number of transpositions.

A permutation α is called odd if it can be expressed as a product of odd number of transpositions.

e.g.

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

$$\alpha = (1\ \ 2)(3\ \ 4)$$

α Shows that even permutations.

Similarly,

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

$$\beta = (1\ \ 2\ \ 3\ \ 4)$$

β shows odd permutation.

Theorem 21:

i). The product of even or odd permutations is an even permutations.

ii). The product of an even permutation and odd permutation is an odd permutation.

Proof:

Let α_1 and α_2 be the permutations of n degree. Let α_1 and α_2 can be expressed as a product of m_1 and m_2 transposition respectively.

So, the product of $\alpha_1\alpha_2$ contained $m_1 + m_2 + 2k$ where k is 0 or $k \in N$ transpositions, possible if $2k$ is cancelled of simplify.

i). if α_1 and α_2 are the even permutations in which case both $m1$ and $m2$ are even, or both α_1 and α_2 are the odd permutations in which case both m_1 and m_2 are odd, hence, $m_1 + m_2 + 2k$ is also an even integer. So, $\alpha_1\alpha_2$ are even permutations.

ii). Consider one of the permutation α_1 is even and other α_2 is odd then $m_1 + m_2 + 2k$ is also an odd integer. So, $\alpha_1\alpha_2$ are odd permutations. ■

Corollary:

Let α be any permutation of degree n and τ a transposition then $\tau\alpha$ or $\alpha\tau$ is an even or odd according as α is even or odd.

Proof:

If α is an even permutation then $\alpha\tau$ or $\tau\alpha$ is an odd permutation.

Theorem 22:

Let $n \geq 2$, the number of even permutation in S_n is equal to the number of odd permutation is S_n.

Proof:

Let,

$$\alpha_1, \alpha_2, ..., \alpha_k \quad (1)$$

be all even permutations and

$\beta_1, \beta_2, .., \beta_m$ (2)

are odd permutations in S_n , So, $k + m = n!$.

Let τ be the transposition. then,

$\alpha_1\tau, \alpha_2\tau, .., \alpha_k\tau$ (3)

are all odd. (By corollary)

$\beta_1\tau, \beta_2\tau, .., \beta_k\tau$ (4)

are all even.

From (1) and (4),

$m \le k$

From (2) and (3),

$k \le m$

So, $m = k = \frac{n!}{2}$ is required proof. ■

Note:

All even permutation in S_n are denoted by A_n . From the above theorem the number of element in A_n are $\frac{n!}{2}$.

Theorem 23:

The set A_n of all even permutation in S_n forms a subgroup of S_n .

Proof:

Suppose, $\alpha_1, \alpha_2 \in A_n$ then we have to prove that,

$\alpha_1\alpha_2^{-1} \in A_n$ (1)

By the theorem (if $\alpha_1\alpha_2$ is in even permutations)

Since, the inverse of transposition also transposition.

Then the inverse of even transposition is even transposition. So, (1) satisfied and A_n is subgroup in S_n . ■

Example 30:

Find all the subgroups of S_3.

Solution:

As we know that,

$S_3 = \{I, a, a^2, b, ab, a^2b\}$

where,

$$I = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix};\ a = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix};\ a^2 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$$

$$b = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix};\ ab = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix};\ a^2b = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$$

Here, $a^3 = b^2 = (ab)^2 = I$

So, the subgroups of S_3 are,

$\{I\}, \{I, a, a^2\}, \{I, b\}, \{I, ab\}, \{I, a^2b\}$ and S_3.

Order of permutation:

Let α be the permutation in S_n then the order of α is at least positive integer n such that,

$\alpha^n = I$.

e.g.

$S_3 = \{I, a, a^2, b, ab, a^2b\}$

where,

$$I = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix};\ a = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix};\ a^2 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$$

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

Hence, order of S_3 is 3.

Let, $\tau = \begin{pmatrix}a & b\\ b & a\end{pmatrix}$

$$\tau^2 = \begin{pmatrix}a & b\\ a & b\end{pmatrix} = I$$

So, the order of transposition τ is 2.

Theorem 24:

The order of cyclic permutation of length m is m.

Proof:

Suppose,

$\alpha = (a_1, a_2, .., a_m)$

be a cyclic permutation of length m. Then under the action,

$\alpha^2 : a_1 \to a_2, a_2 \to a_4, .., a_m \to a_2$

$\alpha^3 : a_1 \to a_3, a_2 \to a_5, .., a_m \to a_3$

.....

$\alpha^m : a_1 \to a_1, a_2 \to a_2, .., a_m \to a_m$

So, that,

$\alpha^m = I$

also for no-smaller power of k of α ,

$\alpha^k = I$

Hence, order of α is *m.* ■

Note:

i). To find the order of permutation, convert α into cyclic permutation, $\alpha_1, \alpha_2, ..., \alpha_k$ of length $m_1, m_2, .., m_k$ respectively. Ignore the cycle of length 1.

ii). The order of α can be find by taking least common multiple (L.C.M) of lengths of cycle.

Example 31:

Find the order of

$$\alpha = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12\\ 2 & 3 & 4 & 1 & 7 & 9 & 6 & 5 & 8 & 12 & 11 & 10\end{pmatrix}$$

$\alpha = (1\ 2\ 3\ 4)(5\ 7\ 6\ 9\ 8)(10\ 12)$

Cycles α_1 , α_2 and α_3 have length 4,5 and 2.

L.C.M=20

So, $\alpha^{20} = I$

Hence, order of α is 20.

By: *Muhammad Fiaz Hussain*[1]
Applied & Analytic Mathematics Research Center
fiaz.hussain24@yahoo.com
Contact # 0333-6639466
0300-5041173

[1] ***M.sc, M.Phil. in Applied & Analytic Mathematics***
Comsats Institute of Information Technology Islamabad.