IMS MATHS BOOK-08

MATHEMATICS

By K. VENKANNA

GROUPS

Some sets of numbers:

→ $N = \{1, 2, 3, \ldots\}$

→ $W = \{0, 1, 2, 3, \ldots\}$

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

→ The set of all rational numbers

$$Q = \left\{\frac{p}{q} / p, q \in I ; q \neq 0\right\}$$

→ Q' = The numbers which cannot be expressed in the form of $\frac{p}{q}$, $(q \neq 0)$ are known as irrational numbers.

Ex: $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, e, $2+\sqrt{3}$ etc.

Note: (i) A rational number can be expressed either as a terminating decimal or a non-terminating / recurring decimal.

(ii) An irrational number can be expressed as non-terminating non-recurring decimal.

→ $R = Q \cup Q'$.

i.e, the set of all real numbers R which contains the set of rational and irrational numbers.

→ $C = \{a+ib / a, b \in R, i = \sqrt{-1}\}$

→ I', Q', R' are the sets of the members of I, Q, R respectively.

→ Z^*, Q^*, R^* and C^* are the sets of non-zero members of I, Q, R and C respectively.

→ I_o and I_e are the sets of odd and even numbers of I.

Some definitions

→ Let A and B be two sets. If $a \in A$ and $b \in B$ then (a, b) is called an ordered pair.

'a' is called the first component (co-ordinate) and 'b' is called the second component of the ordered pair (a, b).

→ Let A and B be two sets then $\{(a, b) / a \in A, b \in B\}$ is called the cartesian product of A and B and is denoted by $A \times B$.

i.e, $A \times B = \{(a, b) / a \in A, b \in B\}$.

Ex: If $A = \{1, 2, 3\}$ and $B = \{3, 4\}$ then $A \times B = \{(1,3), (1,4), (2,3), (2,4), (3,3), (3,4)\}$.

Note: (1) If A and B are finite sets, $n(A) = m$ and $n(B) = k$ then $n(A \times B) = n(B \times A) = mk$.

(2) $A \times B \neq B \times A$ unless $A = B$

(3) If one of A and B is empty then $A \times B$ is also empty.
i.e., $A \times \phi = \phi$, $\phi \times B = \phi$.

→ If A and B are non-empty sets, then any subset of $A \times B$ is called a relation from A to B.

→ Let A be a non-empty set then subset of $A \times A$ is called a binary relation on A.

Ex: If $A = \{1, 2, 3\}$, $B = \{4, 5\}$;

$A \times B = \{(1,4), (1,5), (2,4), (2,5), (3,4), (3,5)\}$.

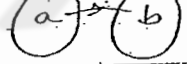
then $f = \{(1,4), (2,4)\} \subseteq A \times B$ is a relation from A to B.

and $A \times A = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3)\}$.

then $g = \{(1,1), (2,1), (3,2), (3,3)\} \subseteq A \times A$ is a binary relation on A.

Function:

Let A and B be two non-empty sets and f be a relation from A to B. If for each elt $a \in A$ $\exists$ a unique $b \in B$ s.t. $(a,b) \in f$ then f is called function (or mapping) from A to B. or A into B. It is denoted by $f: A \to B$.



Binary operation (or) Binary composition

→ Let S be a non-empty set,

$S \times S = \{(a,b) / a \in S, b \in S\}$.

If $f: S \times S \to S$ (i.e., for each ordered pair (a,b) of elts of S $\exists$ a uniquely defined an elt of S) then f is said to binary operation on S.

→ The image of the ordered pair (a,b) under the function f is denoted by $f((a,b))$ or afb.

Ex:- Let $\mathbb{R}$ be the set of all real numbers.

$+^n$, $\times^n$, and $-^n$ of any two real numbers is again a real number i.e, $\forall a, b \in \mathbb{R} \Rightarrow a+b \in \mathbb{R}$, $a \times b \in \mathbb{R}$ and $a-b \in \mathbb{R}$.

Now we define

$+: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $\times: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ and $-: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$.

are three mappings

$\therefore +((a,b))$ or $a+b \in \mathbb{R}$.
$\times((a,b))$ or $a \times b \in \mathbb{R}$
$-((a,b))$ or $a-b \in \mathbb{R}$.

A operation which combines two elements of a set to give another element of the same set is called a binary operation.

Generally the binary operation is denoted by $*$ or $\circ$

If $a * b \in S$ $\forall a, b \in S$ then $*$ is called a binary operation on S.

Examples i) $S = \mathbb{N}, \mathbb{W}, \mathbb{I}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
$\forall a, b \in S \Rightarrow a+b \in S$ and $a.b \in S$.

$\therefore +^n$ and $\times^n$ are b-o operations on S.

Here $-$ is b-o on I, Q, R & C.

i.e, $a, b \in I, Q, R, C \Rightarrow a-b \in I, Q, R, C$.

but $-$ is not b-o on N and W

i.e, $a, b \in N, W \Rightarrow a-b \notin N, W$

$\rightarrow a, b \in S \Rightarrow a \div b \notin S$.

$\therefore \div$ is not a b-o on S.

but $a, b \in Q, R, C$

$\Rightarrow a \div b \in Q, R, C$ if $b \neq 0$

$\therefore \div$ is a b-o on Q, R, C.

(2) $S = Q^*, R^*, C^*$ (Non zero sets)

$a, b \in S \Rightarrow a \div b \in S$.

$\therefore \div$ is a b-o on S.

(3) Addition and subtraction are not b-os on the set of odd integers.

Types of binary operations

Closure operations: A binary operation $*$ on a set S is said to be closure if $\forall a, b \in S$

Ex: (1) $S = N, W, I, Q, R, C$.

$\forall a, b \in S \Rightarrow a+b \in S$ & $a \cdot b \in S$.

$\therefore S$ is closed w.r.t b-o $+^n$ & $\times^n$

$\rightarrow a, b \in I, Q, R, C \Rightarrow a-b \in I, Q, R, C$

$\therefore I, Q, R, C$ are closed under b-o '$-$'

but $a, b \in N, W \Rightarrow a-b \notin N, W$.

$\therefore N, W$ are not closed under b-o '$-$'

(2) $S = Q, R, C$

$a, b \in S \Rightarrow a \div b \in S$ if $b \neq 0$.

$\therefore S$ is closed w.r.t b-o $\div$

(3) $S = Q^*, R^*, C^*$

$a, b \in S \Rightarrow a \div b \in S$

$\therefore S$ is closed w.r.t b-o $\div$

Commutative operations: A binary operation $*$ on a set S is commutative if $a * b = b * a \ \forall a, b \in S$.

Ex: $S = N, W, I, Q, R, C$

$\forall a, b \in S \Rightarrow a+b = b+a$

$a \cdot b = b \cdot a$.

$\therefore S$ is commutative w.r.t b-o $+$ & $\cdot$.

but $a, b \in S \Rightarrow a-b \neq b-a$

$\therefore S$ is not commutative w.r.t b-o '$-$'

$\rightarrow S = Q^*, R^*, C^*$

$a, b \in S \Rightarrow a \div b \neq b \div a$.

$\therefore S$ is not commutative under $\div$

$\forall A, B \in S \Rightarrow A+B = B+A$

$\therefore$ S is commutative under $b-o$ $+^n$.

but $A, B \in S \Rightarrow A-B \neq B-A$.

$\rightarrow$ S = The set of all $n \times n$ matrices

$\forall A, B \in S \Rightarrow A+B = B+A$

$A-B \neq B-A$

$A \cdot B \neq B \cdot A$.

$\rightarrow$ S = The set of all matrices with real entries.

The usual matrix addition, Subtraction, x^n are not b-o on S.

[$\because A, B \in S \Rightarrow A+B, A-B$ & $A \cdot B$ are not defined]

$\rightarrow$ S = The set of all vectors.

$\bar{a}, \bar{b} \in S \Rightarrow \bar{a}+\bar{b} = \bar{b}+\bar{a}$

$\bar{a}-\bar{b} \neq \bar{b}-\bar{a}$

$\bar{a} \times \bar{b} \neq \bar{b} \times \bar{a}$.

but the usual $\cdot$ is not b-o on S. [$\because \bar{a} \cdot \bar{b}$ is scalar. $\notin S$]

Associative operations

A binary operation $*$ on S is said to be associative if

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

$\forall a, b, c \in S$

Ex:- $S = N, W, I, Q, R, C$.

$\forall a, b, c \in S \Rightarrow (a+b)+c = a+(b+c)$

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

but $(a-b)-c \neq a-(b-c)$.

$\forall A, B, C \in S \Rightarrow (A+B)+C = A+(B+C)$

but $(A-B)-C \neq A-(B-C)$

$\rightarrow$ S = The set of all $n \times n$ matrices

$\forall A, B, C \in S \Rightarrow (A+B)+C = A+(B+C)$

$(A \cdot B) \cdot C = A \cdot (B \cdot C)$

but $(A-B)-C \neq A-(B-C)$

$\rightarrow$ S = The set of all vectors.

$\forall \bar{a}, \bar{b}, \bar{c} \in S \Rightarrow (\bar{a}+\bar{b})+\bar{c} = \bar{a}+(\bar{b}+\bar{c})$

$(\bar{a}-\bar{b})-\bar{c} \neq \bar{a}-(\bar{b}-\bar{c})$

Identity element

Let S be a non empty set and $*$ be a b-o on S. If $\exists$ an elt $b \in S$ s.t $a*b = b*a = a$ $\forall a \in S$. Then b is called an identity element in S w.r.t b-o $*$.

$\rightarrow$ The identity elt can be denoted by e. i.e. $b = e$.

Ex (1) $\exists$ an elt $b = 0 \notin N$ s.t $a+0 = 0+a = a$ $\forall a \in N$.

$\therefore$ 0 is not an identity elt in N w.r.t b-o $+$

$\exists$ an elt $b = 1 \in N$ s.t

$a \cdot 1 = 1 \cdot a = a$ $\forall a \in N$.

$\therefore$ 1 is an identity elt in N w.r.t x^n

(2) $S = I, Q, R, C$.

$\exists$ an elt $b = 0 \in S$ s.t $a+0 = 0+a = a$ $\forall a \in S$.

$\exists b = 1 \in S$ s.t $a \cdot 1 = 1 \cdot a = a$ $\forall a \in S$.

Note: In any number system identity w.r.t ordinary addition is zero and w.r.t ordinary multiplication is 1.

(3) S = The set of all $m \times n$ matrices

$A, B \in S \Rightarrow A+B = B+A = A$.

then $B = 0$ (null matrix) is the identity elt in S.

4) S = The set of all $n \times n$ matrices

$A, B \in S \Rightarrow A \cdot B = B \cdot A = A$

then $B = I$ (unit matrix) is the identity elt in S.

Inverse element:

Let S be a non empty set and $*$ be a b o on S.

for each $a \in G$ an elt $b \in S$ s.t

$a * b = b * a = e$

then b is said to be an inverse of a and it denoted by a^{-1} (or) $-a$.

Ex:-

for each $a \in G$ $\exists$ an elt $b = -a \in I$

s.t $a + (-a) = 0 = (-a) + a$.

$\therefore -a$ is an inverse of a in I

(2) for each $a \in G$ $\exists$ $b = \frac{1}{a} \notin I$ s.t $a \cdot \frac{1}{a} = 1 = \frac{1}{a} \cdot a$ $(a \neq 0)$

$\therefore \frac{1}{a}$ is an inverse of a.

→ $S = Q, R, C$; for each $a \in S$ $\exists$ $b = -a \in S$ s.t

$a + (-a) = (-a) + a = 0$

for each $a \in S$ $\exists$ $b = \frac{1}{a} \in S$ (if $a \neq 0$) s.t

$a \cdot \frac{1}{a} = 1 = \frac{1}{a} \cdot a$

$\therefore \frac{1}{a}$ is an inverse of a.

→ S = the set of all $m \times n$ matrices.

for each $A \in S$ $\exists$ $B = -A \in S$ s.t

$A + (-A) = O_{m \times n} = (-A) + A$

then $-A$ is the inverse of A

→ S = the set of all $n \times n$ matrices.

$\exists$ $B = A^{-1} = \frac{\text{adj } A}{|A|}$ (if $|A| \neq 0$)

s.t $A \cdot A^{-1} = A^{-1} A = I$.

Note: In any number system the inverse of 'a' w.r.t ordinary addition is '-a' and the inverse of 'a' w.r.t ordinary multiplication is $\frac{1}{a}$.

Problems

Determine whether the binary operation $*$ defined is commutative and whether $*$ is associative.

1) $*$ defined on Z by letting $a * b = a - b$.

3) $*$ defined on $\mathbb{Q}$ by letting $a*b=\frac{ab}{2}$

4) $*$ defined on $\mathbb{Z}^+$ by letting $a*b=a^b$

5) $*$ defined on $\mathbb{Z}$ by letting $a*b=a+b-ab$.

6) $*$ defined on $\mathbb{Q}$ by letting $a*b=\frac{ab}{3}$.

Determine whether the b-o $*$ defined is identity

7) $*$ defined on $\mathbb{Q}$ by letting $a*b=\frac{ab}{3}$

8) $*$ defined on $\mathbb{Z}^+$ by letting $a*b=a+b+ab$

Answers:

1. Since $a*b=a-b \quad \forall a,b\in\mathbb{Z}$

$b*a=b-a$

$\therefore a*b \neq b*a$.

$\therefore *$ is not commutative in $\mathbb{Z}$

Since $a*b=a-b \quad \forall a,b\in\mathbb{Z}$

Let $a,b,c\in\mathbb{Z}$

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

$=a-b-c$

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

$=a-(b-c)$

$=a-b+c$

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

$\therefore *$ is not associative in $\mathbb{Z}$

(2) Not associative

3) not associative

4) both not a

(7) Since $a*b=\frac{ab}{3} \quad \forall a,b\in\mathbb{Q}$

Let $a\in\mathbb{Q}$, $e\in\mathbb{Q}$ then

$a*e=a=e*a$

$\Rightarrow \frac{ae}{3}-a=0$

$\Rightarrow \frac{a}{3}(e-3)=0$

$\Rightarrow e-3=0$ Cif $\frac{a}{3}\neq 0$

$\Rightarrow e=3$.

$\therefore a*e=\frac{ae}{3}=\frac{a}{3}\times 3$

$=a$

$=e*a$.

$\therefore$ 3 is the identity elt in $\mathbb{Q}$

Algebraic Structure

Let G be a non empty set and $*$ is a b.o on it. G together with the b.o is called an algebraic structure and is denoted by $(G,*)$.

(or)

A non empty set equipped with one or more b.o is called an algebraic structure.

Ex: $(\mathbb{N},+)$, $(\mathbb{N},+,\cdot)$, $(\mathbb{I},+,\cdot,-)$ etc are algebraic structures.

but $(\mathbb{N},-)$, $(\mathbb{I},\div)$ etc are not algebraic structures.

Groupoid (or) Quasi group:

An algebraic structure $(G,*)$ is said to be groupoid if it satisfies the closure property

i.e., $\forall a,b\in G \Rightarrow a*b\in G$

Ex: $(\mathbb{N},+)$, $(\mathbb{I},+)$ etc are groupoid

Semigroup or Demigroup

An algebraic structure $(G, *)$ satisfies the closure and associative properties then $(G, *)$ is called semigroup.

Ex: $(I, +)$, $(I, \cdot)$ etc are semigroups but $(I, -)$ is not a semigroup because it is closure but not associative

Monoid

A semigroup $(G, *)$ with an identity elt w.r.t $*$ is known as a monoid.

Ex:- A semigroup $(I, +)$ is a monoid and the identity is '0'.

- A semigroup $(I, \cdot)$ is a monoid and the identity elt is 1.
- A semigroup $(N, +)$ is not monoid because the identity elt is $0 \notin N$.

Group

A monoid $(G, *)$ with the inverse elt w.r.t $*$ is known as a group.

i.e. the algebraic structure $(G, *)$ is said to be a group if the binary operation $*$ satisfies the following properties

1) Closure prop: $\forall a, b \in G$, $a * b \in G$
2) Asso. prop: $\forall a, b, c \in G$, $(a * b) * c = a * (b * c)$
3) Existence of identity: $\exists e \in G$ s.t $a * e = a = e * a$ $\forall a \in G$. 'e' is called the identity elt of G
4) Existence of inverses: For each $a \in G$, $\exists b \in G$ s.t $a * b = e = b * a$. 'b' is inverse of a in G

Abelian or Commutative group

A group $(G, *)$ which satisfies the commutative prop is known as the abelian group.

Otherwise it is known as non abelian group.

Finite and Infinite group

If the number of elts in the group $(G, *)$ is finite then the group $(G, *)$ is called a finite group. Otherwise it is called infinite group

The number of elts in a finite group is called the order of the group. It is denoted by $o(G)$ or $|G|$.

Note 1) The order of infinite group is infinite.

2) $G=\{e\}$, (i.e., the set consisting of identity elt e alone) is a group, w.r.t given composition which is known as the smallest group.

Problems

(1) The algebraic structure $(I,+)$ where $I=\{\ldots -3,-2,-1,0,1,2,3,\ldots\}$ is an abelian group.

Note: (i) The set Z^+ under $+^n$ is not a group. There is no identity elt for $+^n$ in Z^+

(ii) The set of all non-negative integers (including 0) under $+$ is not a group because there is no inverse of $a\in Z$.

(2) The set I_E of all even integers is an abelian group w.r.t $+^n$

Note: The set I_O of all odd integers is not a group w.r.t $+^n$ because the closure property is not satisfied.

(3) The sets Q, R and C of all rational, real and complex numbers are abelian groups under $+^n$.

4) $G=$ The set of $m\times n$ matrices and is an abelian group w.r.t b-o $+^n$.

5) The set of multiple of integers by fixed integers m is an abelian group w.r.t $+^n$.

6) The set $G_1=\{\ldots -3m,-2m,-m,0,m,2m,3m,\ldots\}$ of multiple of integers by fixed integers m is an abelian group w.r.t $+^n$.

7) The set N under x^n is not a group because there is no inverse of $a\in N$.

8) The sets Q, R, C of all rational, real and complex numbers are not groups w.r.t x^n because the inverse of 0 is not defined.

9) The sets Q^+ and R^+ of all +ve rational and real numbers are abelian groups under x^n.

10) The sets Q^*, R^* and C^* of all non-zero rational, real and complex numbers are abelian groups w.r.t x^n.

11) Is the set of all rational nos x s.t $0<x\le 1$, a group w.r.t x^n?

Soln Let $G=\{x/x$ is a rational no. and $0<x\le 1\}$

Then it is not a group under x^n because if $a\in G$ and $0<a<1$ then inverse of 'a' is not possible in G.

Ex Let $a=\frac{1}{5}\in G$ then the inverse of $\frac{1}{5}$ is $5\notin G$.

12) The set of all +ve rational numbers forms an abelian group under the composition $*$ defined by $a*b=ab/2$.

Elementary Properties of Groups

Let G be a group with $b-o$. Then the left and right cancellation laws hold in G.

i.e, $\forall a, b, c \in G$ (i) $ab = ac \Rightarrow b = c$ (L.C.L)

and (ii) $ba = ca \Rightarrow b = c$ (R.C.L)

proof Given that G is a group w.r.t $b-o$ $\therefore$

for each $a \in G$ $\exists\ a^{-1} \in G$ s.t

$a^{-1}a = a \cdot a^{-1} = e$ (where e is identity)

Now suppose $a \cdot b = a \cdot c$

multiplying both sides a^{-1} on left

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

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$ (Asso. prop.)

$\Rightarrow eb = ec$ (Inverse law)

$\Rightarrow b = c$ (identity)

Similarly $b \cdot a = c \cdot a$

$\Rightarrow b = c$.

Note: If G is a group with $b-o$ '$+$' then the left and right cancellation laws hold in G

i.e, $a+b = a+c \Rightarrow b = c$ (L.C.L)

and $b+a = c+a \Rightarrow b = c$ (R.C.L) $\forall a, b, c \in G$

If G is a group with $b-o$ '$\cdot$' and a & b are elts of G then the linear eqn $ax = b$ and $ya = b$ have unique sol^{n}s x and y in G.

proof: Given that G is a group w.r.t. $b-o$ '$\cdot$'.

for each $a \in G$ $\exists\ a^{-1} \in G$ s.t $aa^{-1} = a^{-1}a = e$ where e is identity

Now we have $ax = b$

multiply both sides a^{-1} on left

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

$\Rightarrow (a^{-1}a)x = a^{-1}b$ (by Asso. prop)

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

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

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

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

Now substituting $a^{-1}b$ for x in the left hand side of the eqn $ax = b$

we have $a(a^{-1}b) = (aa^{-1})b$

$= eb$

$= b$.

$\therefore x = a^{-1}b$ is the sol^n in G of the $ax = b$.

To show that the sol^n is unique

Now if possible suppose that $x = x_1$ and $x = x_2$ are two sol^{n}s of the eqn $ax = b$ then $ax_1 = b$, $ax_2 = b$

$\therefore ax_1 = ax_2 \Rightarrow x_1 = x_2$ (By L.C.L)

$\therefore$ the sol^n is unique

Similarly we prove that $ya = b$ has unique sol^n

If G is a group with the b-g pair a & b are two elements of G then the linear equations $ax=b$ and $ya=b$ have unique solutions in G.

Note [1]. Cancellation laws hold in a group i.e, $\forall a,b,c \in G$

$\Rightarrow$ (i) $ab=ac \Rightarrow b=c$ (LCL)

(ii) $ba=ca \Rightarrow b=c$ (RCL)

In a semigroup, the cancellation laws may or may not hold.

Ex: Let S be the set of all 2×2 matrices with their elements as integers and x^n is 0-0 on's then S is a semi group but not satisfy the cancellation laws because if $A=\begin{bmatrix}1&0\\0&0\end{bmatrix}$, $B=\begin{bmatrix}0&0\\0&1\end{bmatrix}$

$C=\begin{bmatrix}0&0\\1&0\end{bmatrix}$

then $A,B,C \in S$ and $AB=AC$ but $B \neq C$

$\therefore$ left cancellation law is not true in the semi group.

[3]: $(N,+)$ is a semi group:

for $a,b,c \in N$ $a+b=a+c$ and $b+a=c+a$

$\Rightarrow b=c$

But $(N,+)$ is not a group.

If a semigroup $(G,\cdot)$ satisfy the cancellation laws is a group.

(or)

A finite set G with a binary operation '$\cdot$' is a group if '$\cdot$' is associative and cancellation laws hold in G.

Uniqueness of identity

The identity element in a group is unique.

Proof: Let $(G,\cdot)$ be the given group. If possible suppose that e_1 & e_2 are two identity elements in G.

Since e_1 is an identity in G then $e_1e_2=e_2=e_2e_1$ ——①

Since e_2 is identity in G then $e_1e_2=e_1=e_2e_1$ ——②

From (1) & (2) we have

$e_1=e_1e_2=e_2$

$\Rightarrow \boxed{e_1=e_2}$

Uniqueness of inverse

Inverse of each element of a group is unique.

proof: Let $(G,\cdot)$ be the given group.

Now suppose that $a \in G$ has two inverses a' & a''.

Since a' is an inverse of a in G.

$\therefore aa' = a'a = e$ —①

Since a'' is an inverse of a in G

$\therefore aa'' = a''a = e$ —②

From ① & ② we have

$aa' = e = aa''$

$\Rightarrow a \cdot a' = a \cdot a''$

$\Rightarrow a' = a''$ (By LCL)

$\therefore$ inverse of $a \in G$ is unique.

Note: The identity element is its own inverse

since $ee = e$

$\therefore e' = e$.

→ If the inverse of a is $\bar{a}^{-1}$ then inverse of $\bar{a}^{-1}$ is a

i.e, $(\bar{a}^{-1})^{-1} = a$.

proof: Let $(G,\cdot)$ be the given group.

For each $a \in G$ $\exists\, \bar{a}^{-1} \in G$ such that

$a\bar{a}^{-1} = \bar{a}^{-1}a = e$.

Now $a\bar{a}^{-1} = e$

Multiplying both sides with $(\bar{a}^{-1})^{-1}$ on the right.

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

$\Rightarrow a(\bar{a}^{-1}(\bar{a}^{-1})^{-1}) = (\bar{a}^{-1})^{-1}$ (By assoc and e is identity)

$\Rightarrow a(e) = (\bar{a}^{-1})^{-1}$ ($\because (\bar{a}^{-1})^{-1}$ is inverse of $\bar{a}^{-1}$)

$\Rightarrow a = (\bar{a}^{-1})^{-1}$ ($\because$ e is identity)

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

Note: If $(G,+)$ is a group and inverse of a is $-a$ then inverse of $-a$ is a

i.e, $-(-a) = a$.

→ Let $(G,\cdot)$ be a group.

P.T $(ab)^{-1} = b^{-1}a^{-1}$ $\forall a,b \in G$

proof Given that $(G,\cdot)$ is a group.

For each $a \in G$, $\exists\, \bar{a}^{-1} \in G$ such that

$a\bar{a}^{-1} = \bar{a}^{-1}a = e$ and

For each $b \in G$, $\exists\, b^{-1} \in G$ such that $bb^{-1} = b^{-1}b =$

and $a \in G, b \in G \Rightarrow ab \in G$

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

Now we have

$(ab)(b^{-1}\bar{a}^{-1}) = a(bb^{-1})\bar{a}^{-1}$ (by as

$= aea^{-1}$ by inverse

$= aa^{-1}$ by identity

$= e$ by inverse

$\therefore (ab)(b^{-1}\bar{a}^{-1}) = e$ —①

$(b^{-1}a^{-1})(ab) = e$ — (2)

From (1) & (2) we have

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

$\therefore$ The inverse of ab is $b^{-1}a^{-1}$

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

Note: (1) Let $(G, +)$ be a group then $-(a+b) = (-b)+(-a)$.

(2) Generalization

$(a_1 a_2 a_3 \ldots\ldots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1}$.

Definition of a group based upon left Axioms (or) Right Axioms

The algebraic structure $(G, \cdot)$ is said to be group if the binary operation '$\cdot$' satisfies the following properties:

(i) Closure property: $ab \in G, \forall a, b \in G$

(ii) Asso prop: $(ab)c = a(bc)$ $\forall a, b, c \in G$

(iii) Existence of left identity: $\exists e \in G$ such that $ea = a$ $\forall a \in G$. The element 'e' is called left identity in G.

(iv) Existence of left inverse: For $a \in G$, $\exists a^{-1} \in G$ such that $a^{-1}a = e$. The element a^{-1} is called the left inverse of a in G.

Theorem:

The left identity is also the right identity i.e., if e is the left identity then $ae = a$ $\forall a \in G$.

Proof: Let $(G, \cdot)$ be the given group and let e be the left identity. To prove that e is also the right identity.

Let $a \in G$ and e be the left identity then a has the left inverse in G.

$\therefore \bar{a}^1 a = e$

Now we have $\bar{a}^1(ae) = (\bar{a}^1 a)e$ (by Asso)

$= ee$ (by inverse)

$= e$ (by identity i.e., e is left identity)

$= \bar{a}^1 a$ $(\because \bar{a}^1 a = e)$

$\therefore \bar{a}^1(ae) = \bar{a}^1 a$

$\Rightarrow ae = a$ (by LCL in G)

$\therefore$ If e is the left identity then e is also right identity

Theorem: If the left inverse is also right inverse then if a^{-1} is the left inverse of a then also $aa^{-1} = e$

Proof: Let $(G, \cdot)$ be the given group.

Let $a \in G$ and e be the left identity in G.

Let $\bar{a}^{-1}$ be the left inverse of a then $\bar{a}^{-1}a = e$

To prove that $a\bar{a}^{-1} = e$.

Now we have

$\bar{a}^{-1}(a\bar{a}^{-1}) = (\bar{a}^{-1}a)\bar{a}^{-1}$ (by Asso.)

$= e\bar{a}^{-1}$ (by inverse)

$= \bar{a}^{-1}$ ($\because e$ is the left identity)

$= \bar{a}^{-1}e$ ($\because e$ is also right identity)

$\therefore \bar{a}^{-1}(a\bar{a}^{-1}) = \bar{a}^{-1}e$

$\Rightarrow a\bar{a}^{-1} = e$ (by LCL)

$\therefore$ If $\bar{a}^{-1}a = e$ then $a\bar{a}^{-1} = e$

Note: We cannot assume the existence of left identity and the existence of right inverse or we cannot assume the existence of right identity and the existence of left inverse.

Problems

(1) Show that the set $G = \{a + b\sqrt{2} \mid a, b \in Q\}$ is a group w.r.t $+$.

(2) If the set of all $m \times n$ matrices having their elements as integers is an infinite abelian group w.r.t $+$ of matrices.

(3) Show that the set of all $n \times n$ non-singular matrices having their elements as rational (real or complex) numbers is an infinite non-abelian group w.r.t matrix multiplication.

Sol^n: Let M be the set of all $n \times n$ non-singular matrices with their elements as rational numbers.

(i) Closure prop:

Let $A, B \in M$; $|A| \neq 0, |B| \neq 0$

then $AB \in M$ ($\because |AB| = |A||B|$

Here $|AB| \neq 0$ because $|A| \neq 0$ $|B| \neq 0$)

(ii) Asso. prop:

Matrices multiplication is associative.

(iii) Existence of left identity:

$\forall A \in M$, $\exists B = I_{n \times n} \in M$ $|I| = 1 \neq 0$

$|A| \neq 0$

such that $IA = A$.

$\therefore B = I_{n \times n}$ is the left identity in M.

(iv) Existence of left inverse:

Here $A_{n \times n} \in M$; $|A| \neq 0$ $\exists \bar{A}^{-1} = \frac{\text{adj } A}{|A|}$ ($\because |A| \neq 0$

such that $A^{-1}A = I_{n\times n}$ (Left identity)

$\therefore A^{-1}$ is the left inverse of A in M with their elements as rational.

(v) Comm. prop:

$\forall A, B \in M$; $|A| \neq 0$, $|B| \neq 0$

$\Rightarrow AB \neq BA$.

$\therefore (M, \cdot)$ is not an abelian group.

Note: M is the set of all nxn non-singular matrices with their elements as integers is not a group w.r.t x^n because there is no inverse of all matrices in the given set:

Ex: $A = \begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix}$; $|A| = -4 \neq 0$.

$\therefore A^{-1} = \frac{adjA}{|A|} = \begin{bmatrix} -1/2 & 1/2 \\ 3/4 & -1/4 \end{bmatrix}$

Now we have

$A^{-1}A = \begin{bmatrix} -1/2 & 1/2 \\ 3/4 & -1/4 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$= I_{2\times 2}$

But $A^{-1} \notin M$ because the elements of this matrix are not integers.

4) S.T the set of matrices $A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$ where α is a real number forms a group under matrix multiplication.

Soln: Let $G = \{A_\alpha / \alpha \in \mathbb{R}\}$ and '.' is b-o.

(i) Let $A_\alpha, A_\beta \in G \Rightarrow A_\alpha A_\beta = A_{\alpha+\beta} \in G$ where $\alpha+\beta \in \mathbb{R}$

Closure prop: which is true

Since $A_\alpha A_\beta = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}\begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix}$

$= \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix}$

$= A_{\alpha+\beta}$.

$\therefore$ closure prop. is satisfied.

(ii) Asso. prop: Matrix multiplication is associative.

(iii) Existence of left identity:

Since $0 \in \mathbb{R}$

$\therefore A_0 = \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$

Let $A_\alpha \in G$, $\alpha \in \mathbb{R}$ $\exists$ $A_0 \in G$; $0 \in \mathbb{R}$ such that $A_0 A_\alpha = A_{0+\alpha} = A_\alpha$.

$\therefore A_0$ is left identity

(iv) Existence of left inverse:

Since $\alpha \in \mathbb{R} \Rightarrow -\alpha \in \mathbb{R}$.

$\therefore A_\alpha \in G \Rightarrow A_{-\alpha} \in G$

Now $A_{(-\alpha)} A_\alpha = A_{-\alpha+\alpha} = A_0$ (left identity)

$\therefore A_{(-\alpha)}$ is the left inverse of A_α

$\therefore$ Each element of G possesses left inverse.

$\therefore$ G is a group under x^n.

Note: The sets of all nxn matrices with the elements as rational, real, complex numbers are not groups w.r.t matrix multiplication. Because the nxn matrix with entries '0' has no inverse.

→ S.T $G = \left\{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} / a \text{ is any non-zero real number}\right\}$ is a commutative group w.r.t x^n.

→ S.T the set $G = \{x / x = 2^a 3^b \text{ and } a, b \in \mathbb{Z}\}$ is a group w.r.t x^n.

for each $a \in \mathbb{Q}-\{1\}$, $\exists\ b = \frac{a}{a-1} \in \mathbb{Q}-\{1\}$

such that $\frac{a}{a-1} * a = 0$.

$\therefore b = \frac{a}{a-1}$ is left inverse of a in $\mathbb{Q}-\{1\}$ w.r.t. $*$.

$\therefore (\mathbb{Q}-\{1\}, *)$ is a group.

Let S be the set of all real numbers except -1. Define $*$ on S by $a*b = a+b+ab$

a) Show that $*$ gives a binary operation on S.

b) Show that $(S, *)$ is a group.

c) Find the solution of the equation $2*x*3 = 7$ in S.

Soln,

(a) Since S is the set of all real numbers except -1 and $*$ is an operation defined in $S = \mathbb{R}-\{-1\}$ such that

$a*b = a+b+ab \quad \forall a, b \in S$

When $a, b \in S$

$a*b = a+b+ab \in S$.

$\therefore a*b \in S$

$\therefore *$ is a b-o on S.

$\therefore a*b = a+b+ab \quad \forall a, b \in S$. — (1)

If possible let
$a*b = -1$
$\Rightarrow a+b+ab = -1$
$\Rightarrow (a+1)+b(a+1) = 0$
$\Rightarrow (a+1)(b+1) = 0$
$\Rightarrow a+1 = 0$ or $b+1 = 0$
$\Rightarrow a = -1$ or $b = -1$
clearly which is contradiction to hypothesis $a \neq -1, b \neq -1$ in S

(b) (i) Closure prop:

$\forall a, b \in S$

$a*b = a+b+ab \in S$ by (1)

$\therefore S$ is closed under $*$.

(ii) Associative prop:

$\forall a, b, c \in S \Rightarrow (a*b)*c = (a+b+ab)*c$

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

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

Similarly $a*(b*c) = a+b+c+ab+bc+ca+abc$.

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

$\therefore$ Associative law holds.

(iii) Existence of left Identity:

Let $a \in S$, $e \in S$ then $e*a = a$

Now $e*a = a$

$\Rightarrow e+a+ea = a$

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

$\Rightarrow e = 0 \in S \quad (\because a \neq -1)$

$\therefore e*a = 0*a$

$= 0+a+0(a)$

$= a$

$\therefore \forall a \in S \ \exists\ 0 \in S$ such that $0*a = a$.

$\therefore 0$ is the left identity in S.

(iv) Existence of left inverse:

Let $a \in S$, $b \in S$ then $b*a = e$

Now $b*a = e$

$\Rightarrow b+a+ba = 0 \quad (\because e = 0)$

$\Rightarrow b(1+a) = -a$

$\Rightarrow b = \frac{-a}{1+a} \in S \quad (\because a \neq -1)$

$\therefore b*a = \frac{-a}{1+a} * a$

$$= \frac{-a}{1+a} + a + \left(\frac{-a}{1+a}\right) a \qquad (10)$$

$$= \frac{-a}{1+a} + a - \frac{a^2}{1+a}$$

$$= \frac{-a + a(1+a) - a^2}{1+a}$$

$$= 0$$

for each $a \in S$ $\exists$ $b = \frac{-a}{1+a} \in S$ such that $\frac{-a}{1+a} * a = 0$

$\therefore$ $b = \frac{-a}{1+a}$ is left inverse of a in S w.r.t $*$.

$\therefore (S, *)$ is a group.

(c) $2 * x * 3 = 7$

$\Rightarrow (2+x+2x) * 3 = 7$ by (1)

$\Rightarrow (2+3x) * 3 = 7$

$\Rightarrow (2+3x) + 3 + (2+3x)\,3 = 7$ by (1)

$\Rightarrow 5 + 3x + 6 + 9x = 7$

$\Rightarrow 11 + 12x = 7$

$\Rightarrow 12x = -4$

$\Rightarrow x = -\frac{1}{3} \in S$

Now $2 * \left(-\frac{1}{3}\right) * 3 = \left[2 + \left(-\frac{1}{3}\right) + 2\left(-\frac{1}{3}\right)\right] * 3$ by (1)

$= \left(\frac{5}{3} - \frac{2}{3}\right) * 3$

$= 1 * 3$

$= 1 + 3 + 3$

$= 7$

$\therefore x = -1/3$ is a solution of the equation $2 * x * 3 = 7$ in S

→ Let G be the set of all those ordered pairs (a, b) of real numbers for which $a \neq 0$ and define in G an operation $\otimes$ as follows:

$(a,b)\otimes(c,d) = (ac, bc+d)$

Examine whether G is a group w.r.t the operation $\otimes$. If it is a group, is G abelian?

Soln: Let $G = \{(a,b) / a \neq 0, b \in \mathbb{R}\}$ and an operation $\otimes$ defined by

$$(a,b)\otimes(c,d) = (ac, bc+d) \quad \text{---} (1)$$

(i) **Closure prop:**

$\forall (a,b), (c,d) \in G$; $a,b,c,d \in \mathbb{R}$ & $a \neq 0, c \neq 0$.

$\Rightarrow (a,b)\otimes(c,d) = (ac, bc+d) \in G$

($\because a \neq 0, c \neq 0 \Rightarrow ac \neq 0$ & $bc+d \in \mathbb{R}$)

$\therefore$ G is closed under $\otimes$.

(ii) **Asso. prop:**

$\forall (a,b), (c,d), (e,f) \in G$ where $a,b,c,d,e,f \in \mathbb{R}$ & $a, c, e \neq 0$

$\Rightarrow [(a,b)\otimes(c,d)]\otimes(e,f) = (ac, bc+d)\otimes(e,f)$ by (1)

$= (ace, (bc+d)e+f)$

$= (ace, bce+de+f)$

Similarly $(a,b)\otimes[(c,d)\otimes(e,f)] = (ace, bce+de+f)$

$\therefore$ Asso. law holds.

(iii) **Existence of left identity:**

Let $(a,b) \in G$ where $a \neq 0$

Let $(x,y) \in G$, where $x \neq 0$ such that

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

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

$\Rightarrow (xa, ya+b) = (a,b)$ by (1)

$\Rightarrow xa = a$ & $ya+b = b$

$\Rightarrow x=1$ & $ya=0$

$\Rightarrow y=0 \quad (\because a\neq 0)$

$\therefore x=1$ & $y=0$

$\therefore (1,0)\in G$ such that $(1,0)\otimes(a,b)=(a,b)$

$\therefore (1,0)$ is the left identity in G.

(iv) Existence of left inverse:

Let $(a,b)\in G$ where $a\neq 0$

Let $(x,y)\in G$ where $x\neq 0$ such that

$(x,y)\otimes(a,b)=(1,0)$

Now $(x,y)\otimes(a,b)=(1,0)$

$\Rightarrow (xa, ya+b)=(1,0)$

$\Rightarrow xa=1 \; ; \; ya+b=0$

$\Rightarrow x=\frac{1}{a} \; ; \; y=-\frac{b}{a} \quad (\because a\neq 0)$

$\therefore (x,y)=\left(\frac{1}{a},-\frac{b}{a}\right)\in G$ such that

$\left(\frac{1}{a},-\frac{b}{a}\right)\otimes(a,b)=(1,0)$

$\therefore \left(\frac{1}{a},-\frac{b}{a}\right)$ is the left inverse of (a,b) in G

$\therefore (G,\otimes)$ is a group.

(v) Commutative:

$\forall (a,b),(c,d)\in G \; ; \; a,b,c,d\in R \; ; \; a\neq 0, c\neq 0$

$(a,b)\otimes(c,d)=(ac,bc+d) \quad (\text{by } i)$

and $(c,d)\otimes(a,b)=(ca,da+b)$

$\because (a,b)\otimes(c,d)\neq(c,d)\otimes(a,b)$

$\therefore G$ is not commutative under $\otimes$

$\therefore$ the group $(G,\otimes)$ is not an abelian group.

Ex 11 → Let R_0 be the set of all real numbers except zero. Define a binary operation $*$ on R_0 as: $a*b=|a|\cdot b$, where $|a|$ denotes absolute value of a. Does $(R_0,*)$ form a group? Justify.

H.W → Let $G = \{(a,b) ; a,b \in \mathbb{R} \text{ and not both zero}\}$ and $*$ be a binary operation defined by

$(a,b) * (c,d) = (ac-bd, ad+bc)$

Show that $(G,*)$ is a commutative group.

H.W → Let $G = \{(a,b) ; a,b \in \mathbb{R}\}$ and $*$ be a b-o defined by $(a,b) * (c,d) = (a+c, b+d)$ $\forall a,b,c,d \in \mathbb{R}$

Show that $(G,*)$ is a commutative group.

Composition table for finite sets

Let $G = \{a_1, a_2, a_3, \ldots, a_n\}$ be a finite set having n distinct elements. Suppose there is a binary operation $*$ on G can be shown in tabular form known as composition table

- write the elements of G in a horizontal row and vertical column.
- If a_i, a_j are two elements of G then $a_i * a_j$ at the intersection of a row headed by a_i and column headed by a_j

(i) All the entries in the composition table are the elements of the set G.

∴ G is closed w.r.t $*$

(ii) If any row of the composition table coincides with the top row of the composition table identity property is satisfied.

Extremely left column of the corresponding row (first element) is the identity element

(iii) From the composition table, every row and every column contains the identity element.

∴ Inverse property is satisfied.

Problems:

→ Do the following sets form groups w.r.t the b-o * on them as follows.

(i) The set I of all integers with operation defined by $a * b = a+b+1$

(ii) The set $\mathbb{Q}$ of all rational numbers otherthan 1. (i.e, $\mathbb{Q}-\{1\}$) with operation defined by

$a * b = a+b-ab$

(iii) The set I of all integers with the operation defined by $a * b = a+b+2$

Sol^n: (ii) Since $a * b = a+b-ab \quad \forall a, b \in \mathbb{Q}-\{1\}$ ——— (A)

(1) Closure prop:

Let $a, b \in \mathbb{Q}-\{1\}$

$a * b = a+b-ab \in \mathbb{Q}-\{1\}$ (by (A))

$\therefore \mathbb{Q}-\{1\}$ satisfies closure prop. w.r.t *

(2) Asso. property:

$\forall a, b, c \in \mathbb{Q}-\{1\}$

$\Rightarrow (a * b) * c = (a+b-ab) * c$ (by (A))

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

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

$= a+b+c-(ab+bc+ca)+abc.$

Similarly $a*(b*c) = a+b+c-(ab+bc+ca)+abc.$

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

$\therefore \mathbb{Q}-\{1\}$ satisfies Asso. prop. w.r.t *

Existence of left identity prop:

Let $a \in Q-\{1\}$, $e \in Q-\{1\}$

then $e*a = a$

Now $e*a = a$

$\Rightarrow e+a-ea = a$

$\Rightarrow e(1-a) = 0$

$\Rightarrow e = 0 \quad (\because a \neq 1)$.

$\in Q-\{1\}$

$\therefore e*a = 0*a$.

$= 0+a-0(a)$

$= a$

$\therefore \forall a \in Q-\{1\}$, $\exists\ 0 \in Q-\{1\}$ such that

$0*a = a$.

$\therefore 0$ is the left identity in $Q-\{1\}$.

(ii) Existence of left inverse:

Let $a \in Q-\{1\}$, $b \in Q-\{1\}$

then $b*a = e$

Now $b*a = e$

$\Rightarrow b+a-ba = 0 \quad (\text{by } \circledast)$

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

$\Rightarrow b = \frac{-a}{1-a} \quad (\because a \neq 1)$

$= \frac{a}{a-1} \in Q-\{1\}$

$\therefore b*a = \frac{a}{a-1} * a$

$= \frac{a}{a-1} + a - \frac{a}{a-1} \cdot a$

$= \frac{a+a(a-1)-a^2}{a-1} = 0$.

(iv) From the composition table, the rows and columns are interchanged, there is no change in the table if i^{th} row and j^{th} column is a_{ij} then $a_{ij} = a_{ji}$

∴ Commutative property is satisfied.

Problems

→ Show that the fourth roots of unity $G = \{1, -1, i, -i\}$ is an abelian group w.r.t x^n.

Sol^n: $G = \{1, -1, i, -i\}$ and x^n is a b-o on G

Now construct the composition table for G w.r.t x^n.

x	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) Closure prop:
Since all the entries in the composition table are the entries in the set G.
∴ Closure prop. is satisfied.

(ii) Asso. prop:
The elements of G are complex numbers and the multiplication of complex numbers is associative

(iii) Existence of left identity:
From the composition table first row coincides with the top row.
Extremely left column of corresponding row (first element) is the identity element.

i.e, $1(1)=1$, $1(-1)=-1$, $1(i)=i$, $1(-i)=-i$.

i.e, $1 \in G$ and $1a=a$ $\forall a \in G$

$\therefore 1$ is the left identity in G.

(iv) Existence of left inverse:

From the composition table, every row & every column contains the identity element.

i.e, $1 \cdot 1 = 1$, $(-1)(-1)=1$, $i(-i)=1$, $-i(i)=1$

for each $a \in G$ $\exists$ $b \in G$ such that $ba=e$

$\therefore b$ is the left inverse of a in G.

(v) Comm. prop:

From the composition table, the rows & columns are interchanged, there is no change in the table.

$\therefore$ Comm. prop. is satisfied.

$\therefore (G, \cdot)$ is an abelian group. and $o(G)=4$

H.W. → S.T the set $G=\{1, \omega, \omega^2\}$ where ω is imaginary cube root of unity is an abelian group w.r.t x^n $o(G)=3$

HW → S.T (i) $G=\{1,-1\}$ (ii) $G=\{1\}$ are an abelian groups w.r.t x^n.

Note: Every group of order four and less is an abelian.

H.W. → Show that the matrices $A=\begin{bmatrix}1&0\\0&1\end{bmatrix}$ $B=\begin{bmatrix}-1&0\\0&1\end{bmatrix}$ $C=\begin{bmatrix}1&0\\0&-1\end{bmatrix}$, $D=\begin{bmatrix}-1&0\\0&-1\end{bmatrix}$ form an abelian group w.r.t x^n.

→ Show that the set of six transformations $f_1, f_2, f_3, f_4, f_5, f_6$ on the set of complex numbers except 0 and 1 (i.e, $A=C-\{0,1\}$) defined by $f_1(z)=z$, $f_2(z)=\frac{1}{z}$, $f_3(z)=1-z$, $f_4(z)=\frac{z}{z-1}$, $f_5(z)=\frac{1}{1-z}$, $f_6(z)=\frac{z-1}{z}$ forms a finite non-abelian group of order 6 w.r.t the composition known as composite of two functions or product of two functions.

Soln: $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$

Let x^n be the composition of the composite or product of two functions.

Let $f: A \to A$ & $g: A \to A$ then $(gf): A \to A$

such that $(gf)(x) = g(f(x))$ $\forall x \in A$

The function gf is called Composite of the functions g & f

Now we construct the composition table :

	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_6	f_1	f_5	f_4	f_2
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_4	f_2	f_3	f_6	f_1
f_6	f_6	f_3	f_4	f_2	f_1	f_5

$(f_1 f_1)(z) = f_1(f_1(z)) = f_1(z) = z = f_1$

$(f_1 f_2)(z) = f_1(f_2(z)) = f_1\left(\frac{1}{z}\right) = \frac{1}{z} = f_2$

$(f_1 f_3)(z) = f_1(f_3(z)) = f_1(f_3(z)) = f_1(1-z) = 1-z = f_3$

Similarly $f_1 f_4 = f_4$ & $f_1 f_5 = f_5$; $f_2 f_1 = f_2$, $f_3 f_1 = f_3$

$f_4 f_1 = f_4$, $f_5 f_1 = f_5$ & $f_6 f_1 = f_6$

$(f_2 f_2)(z) = f_2(f_2(z)) = f_2\left(\frac{1}{z}\right) = z = f_1$

$(f_2 f_3)(z) = f_2(f_3(z)) = f_2(1-z) = \frac{1}{1-z} = f_5$

$(f_2 f_4)(z) = f_2\left(\frac{z}{z-1}\right) = \frac{z-1}{z} = f_6$

$(f_2 f_5)(z) = f_2\left(\frac{1}{1-z}\right) = 1-\frac{1}{1-z} = f_3$

$(f_2 f_6)(z) = f_2\left(\frac{z-1}{z}\right) = \frac{z}{z-1} = f_4$

$(f_3 f_2)(z) = f_3\left(\frac{1}{z}\right) = 1-\frac{1}{z} = \frac{z-1}{z} = f_6$.

Similarly we can easily find other products

(i) —

(ii) The composite of functions is an asso. composition.

Let $f: A \to A$, $g: A \to A$, $h: A \to A$.

then $h(gf) = (hg)f$.

(iii) —

(iv) —

(v) The composition is not commutative.

Since $f_2 f_3 = f_5$ & $f_3 f_2 = f_6$.

$\therefore f_2 f_3 \neq f_3 f_2$

$\therefore G$ is group but not commutative group w.r.t the composite composition.

$|o(G)| = 6$.

Ex → Show that the bijective transformations f_1, f_2, f_3, f_4 on $A = \mathbb{R} - \{0\}$ given by $f_1(z) = z$, $f_2(z) = \frac{1}{z}$, $f_3(z) = -z$, $f_4(z) = -\frac{1}{z}$ w.r.t the operation composition of mappings is an abelian group.

(1) → Let S be any non-empty set and let $A(S)$ be the set of all one-to-one mappings of the set S onto itself. Then show that $A(S)$ is a group w.r.t composite of mappings as the composition. Is it an abelian group?

Sol^{n}: Let $A(S)$ be the set of all bijections from S to S

Let $f, g \in A(S)$ then f & g are both bijections from $S \to S$.

By the definition of composite of two functions f & g denoted by fg or fg is mapping from S to S given by

$$\therefore (fg)(x) = f(g(x)) \quad \forall x \in S$$

(i) Closure prop:

Let $f, g \in A(S) \Rightarrow fg \in A(S)$

Since f, g are bijections from $S \to S$.

$\therefore$ the composite mapping fg is also bijection from $S \to S$.

$\therefore A(S)$ is closed w.r.t composite composition.

(ii) Asso. prop:

Let $f, g, h \in A(S) \Rightarrow (fg)h = f(gh)$

Since $\forall x \in S$

$$[(fg)h](x) = (fg)[h(x)]$$
$$= f[g(h(x))]$$
$$= f[(gh)(x)]$$
$$= [f(gh)](x).$$

(iii) Existence of left identity:

Let e be the identity mapping from $S \to S$

$\therefore$ for $x \in S$, $e(x) = x$

Also e is bijection.

$\therefore e \in A(S)$

$\therefore f \in A(S) \Rightarrow ef = f$

since $(ef)(x) = e(f(x))$

$= f(x)$

$\therefore ef = f$

$\therefore e$ is the left identity element in $A(S)$.

Existence of left inverse:

Let $f \in A(S) \Rightarrow f: S \to S$ is bijection.

$\therefore f^{-1}: S \to S$ is bijection.

$\therefore f^{-1} \in A(S)$

$\therefore f \in A(S)$ $\exists$ $f^{-1} \in A(S)$ such that $f^{-1}f = e$.

Since $\forall x \in S$

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

$\therefore f^{-1}f = e$

$\therefore A(S)$ is a group w.r.t composite composition.

$S \xrightarrow{f} S$, $x \to y$, $f(x) = y$, $f^{-1}(y) = x$.

- If the set S has only one element then the set $A(S)$ has only one element and every group of order 1 is abelian.
- If the set S has two elements then the set $A(S)$ has also two elements and every group of order 2 is abelian.
- If the set S has more than two elements.

Let x, y, z be three distinct elements in S.

Let $f: S \to S$ & $g: S \to S$

$f(x) = y$, $f(y) = z$, $f(z) = x$

$g(x) = x$, $g(y) = z$, $g(z) = y$

Now $(fg)(x) = f(g(x)) = f(x) = y$.

and $(gf)(x) = g(f(x)) = g(y) = z$

$\therefore (fg)(x) \neq (gf)(x)$.

$\therefore$ Comm. prop. is not satisfied.

$\therefore A(S)$ is non-abelian group.

→ prove that the set of all n^{th} roots of unity forms a finite abelian group of order n w.r.t multiplication.

Sol^n: $1^{1/n} = (1+0i)^{1/n}$

$= (\cos 0 + i\sin 0)^{1/n}$

$= (\cos 2k\pi + i\sin 2k\pi)^{1/n}$

$= \left(\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}\right)$ where $k = 0, 1, 2, \ldots n-1$

$= e^{\frac{2k\pi i}{n}}$ (By DeMoivre's theorem)

Let $G = \left\{ e^{\frac{2k\pi i}{n}} / k = 0, 1, 2, \ldots n-1 \right\}$

(i) Closure prop:

Let $a, b \in G$ where $a = e^{\frac{2r\pi i}{n}}$, $b = e^{\frac{2s\pi i}{n}}$

$0 \le r, s \le n-1$

then $a.b = e^{\frac{2(r+s)\pi i}{n}} \in G$

$(\because 0 \le r+s \le n-1)$

$\therefore G$ is closed under x^n.

(ii) Asso. prop:

The elements of G are all complex numbers and multiplication of complex numbers is associative.

(iii) Existence of left identity:

$\forall a = e^{\frac{2r\pi i}{n}} \in G$ $\exists b = e^{\frac{2(0)\pi i}{n}} = 1 \in G$

$0 \le r \le n-1$

such that $ba = e^{\frac{2(0)\pi i}{n}} \cdot e^{\frac{2r\pi i}{n}}$

$= e^{\frac{2(0+r)\pi i}{n}}$

$= e^{\frac{2r\pi i}{n}}$

$= a$

$\therefore b = 1$ is the left identity element in G.

(iv) Existence of left inverse:

Since $1 \cdot 1 = 1$,
we have left inverse of 1 is 1.

Let $a = e^{\frac{2r\pi i}{n}} \in G$; $1 \le r \le n-1$

$\Rightarrow 1 \le n-r \le n-1$

$\Rightarrow e^{\frac{2(n-r)\pi i}{n}} \in G$

Now $e^{\frac{2(n-r)\pi i}{n}} \cdot e^{\frac{2r\pi i}{n}} = e^{2\pi i}$

$= \cos 2\pi + i \sin 2\pi$

$= 1$

$\therefore e^{\frac{2(n-r)\pi i}{n}}$ is the left inverse of $e^{\frac{2r\pi i}{n}}$ in G.

$\therefore$ Inverse prop is satisfied.

(v) Commutative prop:

The elements of G are all complex numbers and multiplication of complex numbers is commutative.

$\therefore (G, \cdot)$ is a finite abelian group.

Quaternion Group:

Let $T = \{\pm 1, \pm i, \pm j, \pm k\}$ —

Define a multiplicative b-o on T by setting $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$, $jk = -kj = i$ and $ki = -ik = j$.

is non-abelian group of order 8.

(Note: This group is known as Quaternion group of order 8).

Hw: P.T the set G consisting of the following eight matrices $\pm\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\pm\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, $\pm\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$, $\pm\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ forms a Quaternion group under the operation of matrix multiplication.

Set-I

* Groups *

Practice problems

IMS
(INSTITUTE OF MATHEMATICAL SCIENCES)
INSTITUTE FOR IAS/IFoS EXAMINATION
NEW DELHI-110009
Mob: 09999197625

1. Let $(G,*)$ be a group and a be an element of G such that $o(a)=n$. (i) If $a^m = e$ for some positive integer m, then n divides m.

(ii) For every positive integer t,

$$o(a^t) = \frac{n}{\gcd(t,n)}.$$

2. Which of the following groupoids are semigroups? Which are groups?

(i) $(\mathbb{N}, *)$ where $a*b = ab$ for all $a,b \in \mathbb{N}$.

(ii) $(\mathbb{N}, *)$ where $a*b = b$ for all $a,b \in \mathbb{N}$

(iii) $(\mathbb{Z}, *)$ where $a*b = a+b+2$ for all $a,b \in \mathbb{Z}$

(iv) $(\mathbb{Z}, *)$ where $a*b = a-b$ for all $a,b \in \mathbb{Z}$

(v) $(\mathbb{Z}, *)$ where $a*b = a+b+ab$ for all $a,b \in \mathbb{Z}$

(vi) $(\mathbb{R}, *)$ where $a*b = |a|b$ for all $a,b \in \mathbb{R}$.

(vii) $(\mathbb{R}, *)$ where $a*b = 2^a b$ for all $a,b \in \mathbb{R}$

(viii) $(\mathbb{R}\setminus\{-1\}, *)$ where $a*b = a+b+ab$ for all $a,b \in \mathbb{R}\setminus\{-1\}$

3. Write all complex roots of $x^6 = 1$. Show that they form a group under the usual complex multiplication.

4. Let $G = \{a \in \mathbb{R} : -1 < a < 1\}$. Define $*$ on G by $a*b = \frac{a+b}{1+ab}$ for all $a,b \in G$. Show that $*$ is a binary operation on G. Hence prove that $(G,*)$ is a group.

5. Write down the Cayley table for the group operation of the group Z_5.

6. Consider the group Z_{30}. Find the smallest positive integer n such that $n[5]=[0]$ in Z_{30}.

7. Write down all elements of the group U_{10}. Write the Cayley table for this group.

8. Let $G=\left\{\begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix} \mid n\in Z\right\}$. Show that G becomes a group under usual matrix multiplication.

9. Find the order of $[6]$ in the group Z_{14} and the order of $[3]$ in U_{14}.

10. Let $(G,*)$ be a group and $a,b\in G$. Suppose that $a*e$ and $a*b*a=b^7$. Prove that $b^{48}=e$.

11. Which of the following groupoids are semigroups? Which are groups?

(a) $(N,*)$, where $a*b=a+b$ for all $a,b\in N$.

(b) $(N,*)$, where $a*b=a$ for all $a,b\in N$.

(c) $(Z,*)$, where $a*b=a+b+1$ for all $a,b\in Z$.

(d) $(Z,*)$, where $a*b=a+b-1$ for all $a,b\in Z$.

(e) $(Z,*)$, where $a*b=a+2b$ for all $a,b\in Z$.

(f) $(Z,*)$, where $a*b=a+b-ab$ for all $a,b\in Z$.

(g) $(R,*)$, where $a*b=|a|b$ for all $a,b\in R$.

(h) $(R,*)$, where $a*b=a^2b^2$ for all $a,b\in R$.

(i) $(R,*)$, where $a*b=a+b+ab$ for all $a,b\in R$.

(j) $(Q^+,*)$, where $a*b=ab$ for all $a,b\in Q^+$.

(k) $(Q\setminus\{0\},*)$, where $a*b=ab$ for all $a,b\in Q\setminus\{0\}$.

12. Let $P(X)$ be the Power set of a set X. Consider the operation Δ (Symmetric difference) on $P(X)$. Then for all $A, B \in P(X)$,

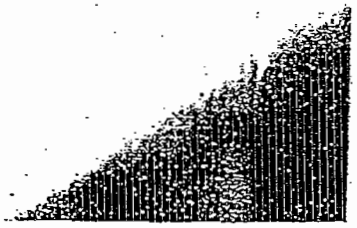
$$A \Delta B = (A \setminus B) \cup (B \setminus A).$$

$(P(X), \Delta)$ is a Commutative group. The empty set ϕ is the identity of $(P(X), \Delta)$ and every element of $P(X)$ is its own inverse. We leave the reader that verification of the associative law is tedious.

13. Let $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a, b, c, d \in R, ad - bc \neq 0 \right\}$, the set of all 2×2 real matrices having a non-zero determinant. Define a binary operation $*$ on G by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} u & v \\ w & s \end{bmatrix} = \begin{bmatrix} au+bw & av+bs \\ cu+dw & cv+ds \end{bmatrix}$$

for all $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} u & v \\ w & s \end{bmatrix} \in G$. This binary operation is the usual matrix multiplication. Since matrix multiplication is associative, we have $*$ is associative. The element $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$ is the identity element for the above operation. Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$. Then $ad - bc \neq 0$. Consider the matrix $\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$. Since



$$\frac{d}{ad-bc}\cdot\frac{a}{ad-bc}-\frac{-b}{ad-bc}\cdot\frac{-c}{ad-bc}=\frac{1}{ad-bc}\neq 0,$$

we have

$$\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix} \in G_1.$$

Now,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and

$$\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix} * \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

thus, $\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$ is the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Hence, G_1 is a group. Now

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in G_1$$

and

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Hence, G_1 is a non commutative group.

This group is known as the general linear group of degree 2 over R and is denoted by $GL(2,R)$.

14. Let R^- denote the set of all negative real numbers. Can you define a binary operation $*$ on R^- so that the system $(R^-, *)$ becomes a group?

15. Write all complex roots of $x^7 = 1$. Show that they form a group under the usual complex multiplication.

16. Show that the set of all complex numbers $a+ib$ such that $a^2+b^2=1$ is a group under the usual multiplication of complex numbers.

17. Let $G_1 = \left\{\begin{bmatrix} a & 0 \\ b & 1 \end{bmatrix} : a, b \in R, a \neq 0\right\}$. Show that G_1 becomes a group under the usual matrix multiplication.

18. Let $G_1 = \left\{\begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in R, a \text{ and } b \text{ not both zero}\right\}$. Show that $(G_1, *)$ is a commutative group, where $*$ denotes the usual matrix multiplication.

19. Consider the group Z_{15}. Find the smallest positive integer n such that $n[5] = [0]$ in Z_{15}.

20. Consider the group Z_{20}. Find the smallest positive integer n such that $n[5] = [0]$ in Z_{20}.

21. Write down all elements of the group U_{10}. Write the Cayley table for this group.

22. Let $(G, *)$ be a group and $a, b, c \in G$. Show that there exists a unique element x in G such that $a * x * b = c$.

23. Let $(G,*)$ be a finite abelian group and $G=\{a_1,a_2,\dots a_n\}$. Let $a_1a_2\dots a_n=x$. Prove that $x*x=e$.

24. Let $(G,*)$ be a group and $a,b\in G$. Suppose that $a*b^3*a^{-1}=b^2$ and $b^{-1}*a^2*b=a^3$. Show that $a=b=e$.

25. Let $(G,*)$ be a group and $a,b\in G$. Suppose that $a^2=e$ and $a*b^4*a=b^7$. Prove that $b^{33}=e$.

26. Let $(G,*)$ be a group and $a,b\in G$. Show that $(a*b*a^{-1})^n=a*b^n*a^{-1}$ for all positive integer n.

27. In a group G, if $a^5=e$ and $a*b*a^{-1}=b^m$ for some positive integer m, and some $a,b\in G$, then Prove that $b^{m^5-1}=e$.

28. In $GL(2,R)$, show that $A=\begin{bmatrix}1 & -1\\ 0 & -1\end{bmatrix}$ and $B=\begin{bmatrix}1 & 1\\ 0 & -1\end{bmatrix}$ are elements of finite order, whereas AB is of infinite order.

29. Let $(G,*)$ be a group. If for $a,b\in G$, $(a*b)^3=a^3*b^3$ and $(a*b)^5=a^5*b^5$, then Prove that $a*b=b*a$.

30. Show that a group $(G,*)$ is Commutative if and only if $(a*b)^5=a^5*b^5$, $(a*b)^6=a^6*b^6$ and $(a*b)^7=a^7*b^7$ for all $a,b\in G$.

31. In the group Z_{15}, find the order of the following elements: $[5]$, $[8]$, and $[10]$.

32. Let G be a group and $a\in G$. If $o(a)=24$, then find $o(a^4)$, $o(a^7)$ and $o(a^{10})$.

33. Let G be a group and $a,b\in G$, such that $ab=ba$ and $o(a)$ and $o(b)$ are relatively Prime. Then Prove that $o(ab)=o(a)o(b)$

34. Find the smallest positive integer n such that $[7]^n = [1]$ in U_{10} and in U_{12}.

35. Find the order of $[6]$ in the group Z_{10} and the order $[3]$ in U_{10}.

36. Show that $\{1, 2, 3\}$ under multiplication modulo 4 is not a group but that $\{1, 2, 3, 4\}$ under multiplication modulo 5 is a group.

37. Find the inverse of the element $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}$ in $GL(2, Z_{11})$.

38. Give an example of group elements a and b with the property that $a^{-1}ba \neq b$.

39. Let p and q be distinct primes. Suppose that H is a proper subset of the integers and H is a group under addition that contains exactly three elements of the set $\{p, p+q, pq, p^q, q^p\}$. Determine which of the following are the three elements in H.

a. pq, p^q, q^p

b. $p+q$, pq, p^q

c. p, $p+q$, pq

d. p, p^q, q^p

e. p, pq, p^q

40. Prove that the set of all 2×2 matrices with entries from $\mathbb{R}$ and determinant $+1$ is a group under matrix multiplication.

41. Let G be a group with the following property: If a, b and c belong to G and $ab = ca$, then $b = c$. Prove that G is Abelian.

42. An Abstract Algebra teacher intended to give a typist a list of nine integers that form a group under multiplication modulo 91. Instead, one of the nine integers was inadvertently left out so that the list appeared as 1, 9, 16, 22, 53, 74, 79, 81. Which integer was left out? (This really happened!).

43. (Law of Exponents for Abelian Groups) Let a and b be elements of an Abelian group and let n be any integer. Show that $(ab)^n = a^n b^n$. Is this also true for non-abelian groups?

44. (Socks-shoes Property) In a group, Prove that $(ab)^{-1} = b^{-1}a^{-1}$. Find an example that shows it is possible to have $(ab)^{-2} \neq b^{-2}a^{-2}$. Find a non-abelian example that shows it is possible to have $(ab)^{-1} = a^{-1}b^{-1}$ for some distinct non identity elements a and b. Draw an analogy between the statement $(ab)^{-1} = b^{-1}a^{-1}$ and the act of putting on and taking off your socks and shoes.

45. Show that the set $\{5, 15, 25, 35\}$ is a group under multiplication modulo 40. What is the identity element of this group? Can you see any relationship between this group and $U(8)$?

46. If $a_1, a_2, \ldots, a_n$ belong to a group, what is the inverse of $a_1 a_2 \cdots a_n$?

47. Suppose the table below is a group table. Fill in the blank entries.

	e	a	b	c	d
e	e	–	–	–	–
a	–	b	–	–	e
b	–	c	d	e	–
c	–	d	–	a	b
d	–	–	–	–	–

48. Prove that if $(ab)^2 = a^2b^2$ in a group G, then $ab = ba$.

49. Let G be a finite group. Show that the number of elements x of G such that $x^3 = e$ is odd. Show that the number of elements x of G such that $x^2 \neq e$ is even.

50. Prove that the set of all 3×3 matrices with real entries of the form

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

is a group.

51. In a finite group, show that the number of non-identity elements that satisfy the equation $x^5 = e$ is a multiple of 4.

52. Let $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} / a \in \mathbb{R}, a \neq 0 \right\}$. Show that G is a group under matrix multiplication.

NOTE: The group $GL(2, \mathbb{R})$ is known as the general linear group of degree 2 over $\mathbb{R}$.

✲ Groups ✲

Answers

11. Ans.

(a) Semi group but not group, (b) Semigroup but not group

(c) Semi group as well as a group (d) Semigroup as well as a group.

(e) not a Semigroup (f) Semi group but not group.

(g) Semigroup but not group (h) Not a semigroup

(i) Semigroup but not group (j) Semigroup as well as a group

(k) Semigroup as well as a group

14. Yes; [Hint: For some $c \in R$; define $a*b = acb$ for all $a, b \in R$]

19. $n = 3$.

20. $n = 4$

21. $U_{10} = \{[1], [3], [7], [9]\}$ and the Cayley table is given by the following.

$*$	[1]	[3]	[7]	[9]
[1]	[1]	[3]	[7]	[9]
[3]	[3]	[9]	[1]	[7]
[7]	[7]	[1]	[9]	[3]
[9]	[9]	[7]	[3]	[1]

31. 3, 15, 8.

32. 6, 24, 12

34. $n = 4$ in U_{10}, $n = 2$ in U_{12}

35. $o([6]) = 5$, $o([3]) = 4$

36. Under modulo 4, 2 does not have an inverse. Under modulo 5, each element has an inverse.

38. $\begin{bmatrix} 4 & 9 \\ 10 & 8 \end{bmatrix}$

39. Ans : (e)

40. Use the fact that $\det(AB) = (\det A)(\det B)$.

42. 29.

43. $(ab)^n$ need not equal $a^n b^n$ in a non-abelian group.

45. The identity is 25

49. If $x^3 = e$ and $x \neq e$, then $(x^{-1})^3 = e$ and $x \neq x^{-1}$. So, nonidentity solutions come in pairs. If $x^r \neq e$, then $x^{-1} \neq x$ and $(x^{-1})^r \neq e$. So solutions to $x^r \neq e$ come in pairs.

52. closure follows from the definition of multiplication. The identity is $\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$. The inverse of $\begin{bmatrix} a & \bar{a} \\ \bar{a} & a \end{bmatrix}$ is $\begin{bmatrix} \frac{1}{4a} & \frac{1}{4\bar{a}} \\ \frac{1}{4\bar{a}} & \frac{1}{4a} \end{bmatrix}$

Let $P(X)$ be the powerset of a set X. Consider operation Δ (symmetric difference) on $P(X)$. Then for all $A, B \in P(X)$, $A \Delta B = (A \setminus B) \cup (B \setminus A)$. Show that $(P(X), \Delta)$ is a commutative group.

Sol': Closure prop:

Let $A, B \in P(X)$

Then $A \subset X$, $B \subset X$.

Now $A \Delta B = (A - B) \cup (B - A)$ ($\Rightarrow$ which is also a subset of X.

$\therefore A \Delta B$ is also a member of $P(X)$

i.e., $A \Delta B \in P(X)$.

$\therefore P(X)$ is closed w.r.t operation Δ.

(∵ difference and union of sets are binary operation on $P(X)$.

because: $A, B \in P(X)$

$\Rightarrow A - B, B - A \in P(X)$

$\Rightarrow (A - B) \cup (B - A) \in P(X)$

i.e., $A \Delta B \in P(X)$]

Associative prop:

The verification of the associative law is tedious. we are enough to show through an example.

Existence of left identity:

The empty set ϕ is a subset of X.

$\therefore \phi$ is a member of $P(X)$.

If A is any member of $P(X)$, we have

$\phi \Delta A = (\phi - A) \cup (A - \phi)$

$= \phi \cup A$

$= A$

$\therefore \phi$ is the left identity.

Existence of left inverse:

Every element of $P(X)$ is its own inverse.

Since $A \Delta A = (A - A) \cup (A - A)$

$= \phi \cup \phi$

$= \phi$

which is a member of $P(X)$

$\therefore (P(X), \Delta)$ is a group.

Commutative prop:

Let $A, B \in P(X)$

$A \Delta B = (A - B) \cup (B - A)$

$= (B - A) \cup (A - B)$

$= B \Delta A$

$\therefore A \Delta B = B \Delta A$.

$\therefore$ commutative prop is satisfied

$\therefore (P(X), \Delta)$ is a commutative group.

* Permutation Groups *

Practice Problems

1. Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 4 & 7 & 5 & 2 & 3 & 1 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 6 & 7 & 3 & 5 & 2 \end{pmatrix}$ be elements of S_7.

(i) write α as a product of disjoint cycles.

(ii) write β as a product of 2 cycles.

(iii) Is β an even permutation?

(iv) Is α^{-1} an even permutation?

2. Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$. Find the smallest positive integer k such that $\alpha^k = e$ in S_4.

3. Compute each of the following and express it in two-row notation in S_7.

(i) $(1\ 3\ 4\ 7)(5\ 4\ 2)$ (ii) $(1\ 2\ 5\ 4)^2 (1\ 2\ 3)(2\ 5)$.

4. Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \in S_4$. Find the smallest positive integer k such that $a^k = e$.

5. Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$ in S_5. Find a permutation γ in S_5 such that $\alpha\gamma = \beta$.

6. If $\beta \in S_7$ and $\beta^4 = (2\ 1\ 4\ 3\ 5\ 6\ 7)$ then find β.

7. If $\beta = (1\ 2\ 3)(1\ 4\ 5)$, write β^{99} in cycle notation.

8. Let $\beta = (1\ 3\ 5\ 7\ 9\ 8\ 6)(2\ 4\ 10)$ in S_{10}. What is the smallest positive integer n for which $\beta^n = \beta^{-5}$?

9. In S_3, find elements α and β s.t. $|\alpha| = 2$, $|\beta| = 2$, and $|\alpha\beta| = 3$.

* Permutation Groups *

Answers

4. $K = 4$

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

6. $\beta = (1\ 3\ 6\ 2\ 4\ 5\ 7)$

7. $\beta^{99} = (1\ 3\ 2\ 5\ 4)$

8. $n = 16.$

Set-III

IIMS
(INSTITUTE OF MATHEMATICAL SCIENCES)
INSTITUTE FOR IAS/IFoS EXAMINATION
NEW DELHI-110009
Mob: 09999197625

* Subgroups *

Practice Problems

1. Let $GL(2,\mathbb{R})$ be the group of all non-singular 2×2 matrices over $\mathbb{R}$. Show that each of the following sets is a subgroup of $GL(2,\mathbb{R})$.

(i) $H=\left\{\begin{bmatrix} a & 0 \\ c & d \end{bmatrix} \in GL(2,\mathbb{R}) \mid ad \neq 0\right\}$

(ii) $H=\left\{\begin{bmatrix} a & b \\ b & a \end{bmatrix} \in GL(2,\mathbb{R}) \text{ either } a \text{ or } b \neq 0\right\}$.

2. Find all subgroups of the group $\mathbb{Z}$ of all integers under usual addition.

3. In each case, determine whether H is a subgroup of the group G under usual operation.

(a) $H=\{3n \mid n\in\mathbb{Z}\}$, $G=\mathbb{Z}$

(b) $H=\{n \mid n\in\mathbb{Z} \text{ and } n\geq 0\}$, $G=\mathbb{Z}$

(c) $H=\{n \mid n\in\mathbb{Z} \text{ and } |n|\geq 1\}$, $G=\mathbb{Z}$

(d) $H=\{(m,n) \mid m,n\in\mathbb{Z} \text{ and } m+n \text{ is even}\}$, $G=\mathbb{Z}\times\mathbb{Z}$

(e) $H=\{1,-1,0\}$, $G=\mathbb{Z}$

(f) $H=\{[0],[2],[4],[6]\}$, $G=\mathbb{Z}_8$

4. In each case, determine whether H is a subgroup of the group $\mathbb{R}^*=(\mathbb{R}\setminus\{0\},\cdot)$.

(a) $H=\{1,-1\}$

(b) $H=$ the set of all positive real numbers.

(c) $H=$ the set of all positive integers.

(d) $H=\{a+b\sqrt{3}\in\mathbb{R}^* \mid a,b\in\mathbb{Q}\}$.

5 Let $GL(2,\mathbb{R})$ denote the group of all nonsingular 2×2 matrices with real entries. In each case, determine whether S is a subgroup of the group $GL(2,\mathbb{R})$.

(a) $S=\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2,\mathbb{R}) \mid ad-bc=1\right\}$.

(b) $S=\left\{\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \in GL(2,\mathbb{R}) \mid n\in\mathbb{Z}\right\}$.

(c) $S=\left\{\begin{bmatrix} 0 & b \\ -b & 0 \end{bmatrix} \in GL(2,\mathbb{R}) \mid b \text{ is nonzero}\right\}$.

(d) $S=\left\{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in GL(2,\mathbb{R}) \mid ad>0\right\}$.

(e) $S=\left\{\begin{bmatrix} a & b \\ b & a \end{bmatrix} \in GL(2,\mathbb{R}) \mid a^2+b^2\neq 0\right\}$

(f) $S=\left\{\begin{bmatrix} a & 0 \\ b & 1 \end{bmatrix} \in GL(2,\mathbb{R}) \mid a\neq 0\right\}$.

6. Show that the set $H=\{a+ib\in\mathbb{C}^* \mid a^2+b^2=1\}$ is a subgroup of $(\mathbb{C}^*,\cdot)$, where $\cdot$ is the usual multiplication of complex numbers.

7. Let G be a group. Prove that a nonempty subset H is a subgroup of G if and only if for $a,b\in H$, ab in H and a^{-1} in H.

8. Let G be a group and $a\in G$. $C(a)=\{x\in G \mid ax=xa\}$. show that $C(a)$ is a subgroup of G and $Z(G)$ is contained in $C(a)$.

9. If G is a commutative group, then prove that $H = \{a^2 / a \in G\}$ is a subgroup of G.

10. If G is a commutative group, then prove that $H = \{a \in G / a^2 = e\}$ is a subgroup of G.

11. Let K be a subgroup of a group G and H be a subgroup of K. Is it true that H is a subgroup of G? Justify.

12. Let G be a group and $a \in G$. Show that $H = \{a^{2n} : n \in Z\}$ is a subgroup of G.

13. In the group S_3, show that the subset $H = \{a \in S_3 / o(a) \text{ divides } 2\}$ is not a subgroup.

14. In the symmetric group S_3, show that $H = \{e, (2\ 3)\}$ and $K = \{e, (1\ 2)\}$ are subgroups but HUK is not a subgroup of S_3.

15. If H and K are subgroups of a group G, then prove that HUK is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$.

16. Let G be a group and H be a nonempty subset of G.
(a) show that if H is a subgroup of G, then $HH = H$.
(b) If H is finite and $HH \subseteq H$, then prove that H is a subgroup of G.
(c) Give an example of a group G and a nonempty subset H such that $HH \subseteq H$, but H is not a subgroup of G.

17. Let G be a commutative group. Prove that the set H of all elements of finite order in G is a subgroup of G.

18. Let G be a commutative group. Prove that the subset $H = \{a \in G \mid o(a) \text{ divides } 10\}$ is a subgroup of G.

19. Let $G = \{(a,b) : a,b \in \mathbb{R} \text{ and } b \neq 0\}$. show that $(G,*)$ is a non commutative group under the binary operation $(a,b) * (c,d) = (ac+bc, bd)$ for all $(a,b), (c,d) \in G$.

(a) show, that $H = \{(a,b) \in G \mid a = 0\}$ is a subgroup of G.

(b) show that $K = \{(a,b) \in G \mid b > 0\}$ is a subgroup of G.

(c) show that $T = \{(a,b) \in G \mid b = 1\}$ is a subgroup of G.

(d) Does G Contain a finite subgroup of order 2?

20. Let $H = \{\beta \in S_5 \mid \beta(1) = 1 \text{ and } \beta(3) = 3\}$. Prove that H is a subgroup of S_5.

21. Let G be a group. Prove or disprove that $H = \{g^2 \mid g \in G\}$ is a subgroup of G.

22. For each divisor k of n, let $U_k(n) = \{x \in U(n) \mid x = 1 \bmod k\}$. For example, $U_3(21) = \{1, 4, 10, 13, 16, 19\}$ and $U_7(21) = \{1, 8\}$. List the elements of $U_4(20)$, $U_5(20)$, $U_5(30)$, and $U_{10}(30)$. Prove that $U_k(n)$ is a subgroup of $U(n)$.

23. Suppose that H is a proper subgroup of $\mathbb{Z}$ under addition and H Contains 18, 30, and 40. Determine H.

24. Let G be a group. Show that $Z(G) = \bigcap_{a \in G} C(a)$. [This means the intersection of all subgroups of the form $C(a)$.]

25. Let G be a group, and let $a \in G$. Prove that $C(a) = C(a^{-1})$.

26. Let $H = \{x \in U(20) \mid x = 1 \bmod 3\}$. Is H a subgroup of $U(20)$?

27. Suppose G_1 is the group defined by the following cayley table.

	1	2	3	4	5	6	4	8
1	1	2	3	4	5	6	7	8
2	2	1	8	7	6	5	4	3
3	3	4	5	6	7	8	1	2
4	4	3	2	1	8	7	6	5
5	5	6	7	8	1	2	3	4
6	6	5	4	3	2	1	8	7
7	7	8	1	2	3	4	5	6
8	8	7	6	5	4	3	2	1

(a) find the Centralizer of each member of G_1.

(b) Find $Z(G)$

(c) Find the order of each element of G_1. How are these orders arithmetically related to the order of the group?

28. Consider the elements $A=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}$ and $B=\begin{bmatrix}0 & 1\\ -1 & -1\end{bmatrix}$ from $SL(2,R)$. Find $|A|$, $|B|$, and $|AB|$. Does your answer suprise you?

29. Consider the element $A=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$ in $SL(2,R)$. What is the order of A? If we view $A=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$ as a member of $SL(2,Z_p)$ (p is a prime), what is the order of A?

30. For any positive integer n and any angle θ, show that in the group $SL(2,R)$,

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^n = \begin{bmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{bmatrix}$$

Use this formula to find the order of

$$\begin{bmatrix} \cos 60^\circ & -\sin 60^\circ \\ \sin 60^\circ & \cos 60^\circ \end{bmatrix} \text{ and } \begin{bmatrix} \cos\sqrt{2}^\circ & -\sin\sqrt{2}^\circ \\ \sin\sqrt{2}^\circ & \cos\sqrt{2}^\circ \end{bmatrix}.$$

31. Compute the orders of the following.

a. $U(3), U(4), U(12)$ b. $U(5), U(7), U(35)$

c. $U(4), U(5), U(20)$ d. $U(3), U(5), U(15)$

32. Let $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$ under addition. Let $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G, \ a+b+c+d = 0 \right\}$. Prove that H is a subgroup of G. What if 0 is replaced by 1?

33. Let $G = GL(2, \mathbb{R})$. Let $H = \{ A \in G \mid \det A \text{ is a power of } 2 \}$. Show that H is a subgroup of G.

34. Let H be a subgroup of $\mathbb{R}$ under addition. Let $K = \{ 2^a \mid a \in H \}$. Prove that K is a subgroup of $\mathbb{R}^*$ under multiplication.

35. Let G be a group of functions from $\mathbb{R}$ to $\mathbb{R}^*$ under multiplication. Let $H = \{ f \in G \mid f(1) = 1 \}$. Prove that H is a subgroup of G.

36. Let $G = GL(2, \mathbb{R})$ and $H = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a \text{ and } b \text{ are non-zero integers} \right\}$. Prove or disprove that H is a subgroup of G.

37. Let $G = GL(2, \mathbb{R})$

(a) Find $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)$ (b). Find $C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)$

(c). Find $Z(G)$.

* Subgroups *

Answers:

3. (a) Yes (b) no (c) no (d) yes (e) no (f) Yes.

4. (a) Yes (b) yes (c) no (d) yes

5. (a) Yes (b) Yes (c) no (d) Yes (e) no (f) Yes.

16. (c) - Consider $G = (Z, +)$ and $H = \{n \in Z \mid n \geq 1\}$.

25. $\langle 2 \rangle$

24. If $x \in Z(G)$, then $x \in C(a)$ for all a, so $x \in \bigcap_{a \in G} C(a)$. If $x \in \bigcap_{a \in G} C(a)$, then $xa = ax$ for all a in G, so $x \in Z(G)$.

26. NO: $7 \in H$ but $7 \cdot 7 \notin H$.

27. a. $C(5) = G$; $C(7) = \{1, 3, 5, 7\}$

b. $Z(G) = \{1, 5\}$

c. $|2| = 2$, $|3| = 4$. They divide order of the group.

29. Note that $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$

32. Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ belong to H. It suffices to show that $a - a' + b - b' + c - c' + d - d' = 0$. this follows from $a + b + c + d = 0 = a' + b' + c' + d'$. If 0 is replaced by 1, H is not a subgroup.

34. If 2^a and $2^b \in K$, then $2^a (2^b)^{-1} = 2^{a-b} \in K$ since $a - b \in H$.

36. $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}^{-1} = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}$ is not in H

37. a $\left\{ \begin{bmatrix} a+b & a \\ a & b \end{bmatrix} / ab + b^2 \neq a^2;\ a, b \in R \right\}$

b. $\left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} / a^2 \neq b^2;\ a, b \in R \right\}$

c. $\left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} / a \neq 0;\ a \in R \right\}$

Set-IV

* Cosets and Lagrange's Theorem *

* Practice Problems *

1. Let H be a subgroup of a group G_1. Then $|L| = |R|$, where L (resp. R) denotes the set of all left (resp. right) cosets of H in G_1.

2. Find all subgroups of S_3. Show that union of any two non-trivial distinct subgroups of S_3 is not a subgroup of S_3.

3. Let H be a subgroup of a group G_1. Denote by L_H, the relation on G_1 defined by $L_H = \{(a, b) \in G_1 \times G_1 : a^{-1}b \in H\}$. Prove that
   (i) L_H is an equivalence relation
   (ii) Every equivalence class is a left coset of H in G_1.
   (iii) Every left coset of H is an equivalence class of the relation L_H.

4. Find all distinct left cosets of the subgroup H in the group G_1.
   (a) $H = \{1, -1\}$, $G_1 = (\mathbb{R} \setminus \{0\}, \cdot)$ (b) $H = 7\mathbb{Z}$, $G_1 = \mathbb{Z}$
   (c) $H = \{e, (2\ 3)\}$, $G_1 = S_3$. (d) $H = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$, $G_1 = S_3$.

5. Show that the set L of all left cosets of $\mathbb{Z}$ in the additive group $(\mathbb{R}, +)$ of all real numbers is given by $L = \{x + 8\mathbb{Z} \mid x = 0, 1, 2, \ldots, 7\}$.

and S_3 itself are the nontrivial subgroups of S_3.

Let H be a subgroup of S_3. Now $|H|$ divides $|G|$. Thus, $|H| = 1, 2, 3$, or 6. If $|H| = 1$, then $H = \{e\}$. If $|H| = 6$, then $H = S_3$. If $|H| = 2$, then H is a cyclic group of order 2. Hence H is one of $\{e, (12)\}, \{e, (13)\}, \{e, (23)\}$. Suppose $|H| = 3$. Then by Lagrange's theorem, H has no subgroup of order 2. Thus, $(12), (13), (23) \notin H$. Hence $e, (123), (132) \in H$. Also $\{e, (123), (132)\}$ is a subgroup and so $H = \{e, (123), (132)\}$. Hence $H_0 = \{e\}$, $H_1 = \{e, (12)\}$, $H_2 = \{e, (13)\}$, $H_3 = \{e, (23)\}$, $H_4 = \{e, (123), (132)\}$ and S_3 are the only subgroups of S_3.

Let H and K be two nontrivial distinct subgroups of S_3. Then $|H| = 2$ or 3 and $|K| = 2$ or 3. Also we note that $H \cap K = \{e\}$. Now $|HK| = 3$ or 4. But there exists only one subgroup of order 3 in S_3 and a subgroup of order 3 cannot contain any subgroup of order 2. Also 4 does not divide $|S_3|$, Hence we find that HK is not a subgroup of S_3.

3. Sol'n: (i) Let $a \in G$. Since $a^{-1}a = e \in H$, we find that $(a, a) \in L_H$ for all $a \in G$. Let $a, b \in G$ such that $(a, b) \in L_H$. Then $a^{-1}b \in H$ and so $b^{-1}a = (a^{-1}b)^{-1} \in H$. Hence $(b, a) \in L_H$. Suppose now $(a, b) \in L_H$ and $(b, c) \in L_H$. Hence $a^{-1}b \in H$ and $b^{-1}c \in H$. Then $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$. Consequently,

Cosets and Lagrange's Theorem

Answers

1. **Proof:** To establish this, we need to show the existence of a bijective function from L onto R. Define $f: L \to R$ by $f(aH) = Ha^{-1}$ for all $aH \in L$. Observe that Ha^{-1} is a right coset of H in G and hence $Ha^{-1} \in R$. Now, we show that $aH = bH$ if and only if $Ha^{-1} = Hb^{-1}$. Suppose $aH = bH$. Then $a^{-1}b \in H$. Hence $b^{-1}(a^{-1})^{-1} \in H$ and so by known theorem [Let H be a subgroup of a group G and let $a, b \in G$, $Ha = Hb$ if and only if $ba^{-1} \in H$] we have $Ha^{-1} = Hb^{-1}$.

Conversely, assume that $Ha^{-1} = Hb^{-1}$. Then by known theorem [Let H be a subgroup of a group G and let $a, b \in G$, $Ha = Hb$ if and only if $ba^{-1} \in H$], $b^{-1}(a^{-1})^{-1} \in H$, i.e., $b^{-1}a \in H$ and so $a^{-1}b = (b^{-1}a)^{-1} \in H$. Then by theorem [Let H be a subgroup of a group G and let $a, b \in G$, $aH = bH$ if and only if $a^{-1}b \in H$], $aH = bH$. Thus we find that f is well-defined and one-one. Since for all $Ha \in R$, $Ha = H(a^{-1})^{-1} = f(a^{-1}H)$ and $a^{-1}H \in L$, f is onto. Thus f is a one-one and onto mapping.

2. **Sol'n:** $S_3 = \{e, (12), (13), (23), (123), (132)\}$, $o(12) = o(13) = o(23) = 2$, $o(123) = o(132) = 3$. Now $\{e\}, \{e, (12)\}, \{e, (13)\}, \{e, (23)\}, \{e, (123), (132)\}$

and S_3 itself are the non-trivial subgroups of S_3.

Let H be a subgroup of S_3. Now $|H|$ divides $|G|$. Thus, $|H| = 1, 2, 3,$ or 6. If $|H| = 1$, then $H = \{e\}$. If $|H| = 6$, then $H = S_3$. If $|H| = 2$, then H is a cyclic group of order 2. Hence H is one of $\{e, (12)\}, \{e, (13)\}, \{e, (23)\}$. Suppose $|H| = 3$. Then by Lagrange's theorem, H has no subgroup of order 2. Thus, $(12), (13), (23) \notin H$. Hence $e, (123), (132) \in H$. Also $\{e, (123), (132)\}$ is a subgroup and so $H = \{e, (123), (132)\}$. Hence $H_0 = \{e\}$, $H_1 = \{e, (12)\}$, $H_2 = \{e, (13)\}$, $H_3 = \{e, (23)\}$, $H_4 = \{e, (123), (132)\}$ and S_3 are the only subgroups of S_3.

Let H and K be two non-trivial distinct subgroups of S_3. Then $|H| = 2$ or 3 and $|K| = 2$ or 3. Also we note that $H \cap K = \{e\}$. Now $|H \cup K| = 3$ or 4. But there exists only one subgroup of order 3 in S_3 and a subgroup of order 3 cannot contain any subgroup of order 2. Also 4 does not divide $|S_3|$, Hence we find that $H \cup K$ is not a subgroup of S_3.

3. Sol^n: (i) Let $a \in G$. Since $a^{-1}a = e \in H$, we find that $(a, a) \in L_H$ for all $a \in G$. Let $a, b \in G$ such that $(a, b) \in L_H$. Then $a^{-1}b \in H$ and so $b^{-1}a = (a^{-1}b)^{-1} \in H$. Hence $(b, a) \in L_H$. Suppose now $(a, b) \in L_H$ and $(b, c) \in L_H$. Hence $a^{-1}b \in H$ and $b^{-1}c \in H$. Then $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$. Consequently,

$(a,c) \in L_H$. So it follows that L_H is an equivalence relation.

(ii) Let $[a]$ be an equivalence class of the relation L_H. Now,

$[a] = \{x \in G \mid (a,x) \in L_H\} = \{x \in G \mid a^{-1}x \in H\} = \{x \in G \mid x \in aH\} \subseteq aH$.

Again for any $ah \in aH$, $a^{-1}(ah) = h \in H$ implies that $(a,ah) \in L_H$. Hence $ah \in [a]$ and then $aH \subseteq [a]$. Consequently $[a] = aH$.

(iii) Let aH be a left coset. proceeding as in (ii), show that $[a] = aH$.

4. Let S be the set of all left cosets of H in G.

(a) $S = \{\{x, -x\} \mid x \in \mathbb{R}^+\}$

(b) $S = \{\{7n \mid n \in \mathbb{Z}\}, \{7n+1 \mid n \in \mathbb{Z}\}, \{7n+2 \mid n \in \mathbb{Z}\}, \{7n+3 \mid n \in \mathbb{Z}\}, \{7n+4 \mid n \in \mathbb{Z}\}, \{7n+5 \mid n \in \mathbb{Z}\}, \{7n+6 \mid n \in \mathbb{Z}\}\}$

(c) $S = \{H, (1\,2)H, (1\,2\,3)H\}, \{(1\,3)H, (1\,3\,2)H\}\}$

(d) $S = \{H, \{(1\,2)H, (2\,3)H, (1\,3)H\}\}$

9. (i) no (ii) no

8. Let $K_4 = \{e, a, b, c\}$; then $\{e\}, \{e,a\}, \{e,b\}, \{e,c\}, K_4$ are the only subgroups of it.

11. $|G| = 315$

14. $H = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$, $\alpha_5 H = \{\alpha_5, \alpha_8, \alpha_6, \alpha_7\}$, $\alpha_9 H = \{\alpha_9, \alpha_{11}, \alpha_{12}, \alpha_{10}\}$

15. H, $(1+H)$, $2+H$

16. $8/2 = 4$ so there are four cosets. Let $H = \{1, H\}$. The cosets are H, $7H$, $13H$, $19H$.

* Cyclic Groups *

Set-V

Practice Problems

1. Show that the 8th roots of unity form a cyclic group. Find all generators of this group.
2. Show that Z_{10}, the additive group of all integers modulo 10 is a cyclic group. Find all generators of Z_{10}.
3. The group $(\mathbb{Q}, +)$ is not cyclic.
4. Prove that any finitely generated subgroup of $(\mathbb{Q}, +)$ is cyclic.
5. Let G be a group of order 28. Show that G has a nontrivial subgroup.
6. If $G = \langle a \rangle$ is a cyclic group of order 30, then find all distinct elements of the subgroups (i) $\langle a^5 \rangle$ (ii) $\langle a^6 \rangle$.
7. Show that the 7th roots of unity form a cyclic group. Find all generators of this group.
8. Show that the cyclic group $(Z, +)$ has only two generators.
9. Is the group $(Z_{10}, +)$ a cyclic group? If so, find all generators of this group and also find all its subgroups.
10. Show that for every positive integer n, the nth roots of unity form a cyclic group.
11. Show that $(\mathbb{Q}^+, \cdot), (\mathbb{Q}^*, \cdot), (\mathbb{R}^+, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$ are not cyclic groups.
12. If a group G has only two subgroups, then prove that G is a cyclic group.

13. Let G be a cyclic group of order 42. Find the number of elements of order 6 and the number of elements of order 7 in G.

14. Let $G = \langle a \rangle$ be a cyclic group of order 20. Find all distinct elements of the subgroups (i) $\langle a^4 \rangle$ (ii) $\langle a^7 \rangle$.

15. Prove that every noncommutative group has a nontrivial cyclic group.

16. Let $G = \{a, b, c, d, e\}$ be a group. Complete the following Cayley table for this group.

$*$	e	a	b	c	d
e	e	a	b	c	d
a	a				
b	b		c	d	
c	c				
d	d				

17. Prove that any finite subgroup of the group of non-zero complex numbers is a cyclic group.

18. Let $G \neq \{e\}$ be a group of order p^n, p is a prime. Show that G contains an element of order p.

19. Prove that every proper subgroup of S_3 is cyclic.

20. Find all generators of Z_6, Z_8 and Z_{10}.

21. Suppose that $\langle a \rangle$, $\langle b \rangle$ and $\langle c \rangle$ are cyclic groups of order 6, 8 and 20 respectively. Find all generators of $\langle a \rangle$, $\langle b \rangle$ and $\langle c \rangle$.

22. List the elements of the subgroups $\langle 20\rangle$ and $\langle 10\rangle$ in Z_{30}.

23. List the elements of the subgroups $\langle 3\rangle$ and $\langle 15\rangle$ in Z_{18}.

24. List the elements of the subgroups $\langle 3\rangle$ and $\langle 7\rangle$ in $U(20)$.

25. List the cyclic subgroups of $U(30)$.

26. Let Z denote the group of integers under addition. Is every subgroup of Z cyclic? why? Describe all the subgroups of Z.

27. Find all generators of Z.

28. List all the elements of order 8 in $Z_{8000000}$. How do you know your list is complete.

29. Consider the set $\{4,8,12,16\}$. show that this set is a group under multiplication modulo 20 by constructing its Cayley table. what is the identity element? Is the group cyclic? If so, find all of its generators.

30. List all the elements of Z_{40} that have order 10.

31. Let $|x|=40$. List all the elements of $\langle x\rangle$ that have order 10.

32. Let a and b belong to a group. If $|a|=24$ and $|b|=10$, what are the possibilities for $|\langle a\rangle \cap \langle b\rangle|$?

33. Prove that $H=\left\{\begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix} / n\in Z\right\}$ is a cyclic subgroup of $GL(2,R)$.

34. Let a and b belong to a group. If $|a|=12$, $|b|=22$, and $\langle a\rangle \cap \langle b\rangle \neq \{e\}$, Prove that $a^6=b^{11}$.

Answers.

(1) sol'n: The 8th roots of unity are

$$\alpha_K = \cos\frac{2K\pi}{8} + i\sin\frac{2K\pi}{8}, \quad K = 0, 1, 2, \cdots 7$$

Let $G_1 = \{\alpha_0, \alpha_1, \cdots \alpha_7\}$.

Here we can easily show that G_1 is a group of order 8.

Now

$$\alpha_K = \cos\frac{2K\pi}{8} + i\sin\frac{2K\pi}{8}$$

$$= \left(\cos\frac{2\pi}{8} + i\sin\frac{2\pi}{8}\right)^K = \alpha_1^K \text{ for } K = 0, 1, 2, \cdots 7$$

Hence we find that $G_1 = \langle\alpha_1\rangle$ and so, G_1 is a cyclic group of order 8. Now for any integer $1 \le t < 8$, α_1^t is a generator of G_1 if and only if $\gcd(t, 8) = 1$. Hence α_1^1, α_1^3, α_1^5 and α_1^7 are generators of this cyclic group.

2. The group Z_{10} consists of all the following 10 distinct elements, viz., $[0], [1], [2], \cdots [9]$. Since $[m] = m[1]$ for $m = 0, 1, \cdots 9$, it follows that Z_{10} is generated by $[1]$. Hence Z_{10} is a cyclic group. Now an element $m[1]$, $(m = 1, 2, \cdots 9)$ is a generator of Z_{10} if and only if $\gcd(m, 10) = 1$. Hence $1[1]$, $3[1]$, $7[1]$, and $9[1]$ are the generators of Z_{10}, i.e., $[1]$, $[3]$, $[7]$ and $[9]$ are the generators of Z_{10}.

3. Sol'n: Suppose $(Q, +)$ is cyclic. Then $Q = \langle x \rangle$ for some $x \in Q$. Clearly $x \neq 0$. Hence $x = \frac{p}{q}$, where p and q are integers prime to each other and $q \neq 0$. Since $\frac{p}{2q} \in Q$, there exists $n \in Z$, $n \neq 0$ such that $\frac{p}{2q} = n\frac{p}{q}$. This implies that $\frac{1}{2} = n \in Z$, which is a contradiction. Hence $(Q, +)$ is not cyclic.

4. Let H be any finitely generated subgroup of $(Q, +)$ and suppose $H = \left\langle \left\{ \frac{p_1}{q_1}, \frac{p_2}{q_2}, \cdots, \frac{p_n}{q_n} \right\} \right\rangle$. Let $x \in H$. Then $x = k_1\frac{p_1}{q_1} + k_2\frac{p_2}{q_2} + \cdots + k_n\frac{p_n}{q_n}$ for some $k_1, k_2 \cdots k_n \in Z$. Now,

$$x = \frac{\sum_{i=1}^{n} k_i p_i \bar{q}_i}{q_1 q_2 \cdots q_n} \quad \text{where } \bar{q}_i = \prod_{\substack{j=1 \\ j \neq i}}^{n} q_j.$$

Then it is easy to see that $x \in \left\langle \frac{1}{q_1 q_2 \cdots q_n} \right\rangle$ since $\sum_{i=1}^{n} k_i p_i \bar{q}_i \in Z$.

Thus $H \subseteq \left\langle \frac{1}{q_1 q_2 \cdots q_n} \right\rangle$, hence H become a subgroup of a cyclic group $\left\langle \frac{1}{q_1 q_2 \cdots q_n} \right\rangle$ and consequently H is cyclic. Hence the result.

5. Sol'n: First suppose that G is cyclic. Then by theorem

[Let $G = \langle a \rangle$ be a cyclic group of order n.
(i) If H is a subgroup of G, then $|H|$ divides $|G|$.
(ii) If m is a positive integer such that m divides n, then there exists a unique subgroup of G of order m,]

for every positive divisor m of $|G|$, G has a subgroup of order m. Now 4 is a divisor of 28. So G has a subgroup of order 4. Hence there is a nontrivial subgroup of G. Now suppose that G is not cyclic. Let $e \neq a \in G$ and let H be the subgroup $\langle a \rangle$ generated by a. Then $H \neq \{e\}$. Also $G \neq H = \langle a \rangle$, as otherwise G becomes cyclic. Hence H is a proper subgroup of G.

6. Sol'n: (i) Here $\langle a^5 \rangle = \{(a^5)^n / n \in \mathbb{Z}\}$. Now $o(a) = |\langle a \rangle| = |G| = 30$. Hence $a^{30} = e$. Then $(a^5)^6 = e$ implies that $o(a^5) = 6$. Observe that the divisors of 6 are 1, 2, 3 and 6. Since $(a^5)^1 \neq e$, $(a^5)^2 \neq e$, $(a^5)^3 \neq e$ it follows that $o(a^5) = 6$. Hence,

$$\langle a^5 \rangle = \{(a^5)^0, (a^5)^1, (a^5)^2, (a^5)^3, (a^5)^4, (a^5)^5\}$$
$$= \{e, a^5, a^{10}, a^{15}, a^{20}, a^{25}\}$$

(ii) The order of a^6 is 5. Hence,

$$\langle a^6 \rangle = \{(a^6)^0, (a^6)^1, (a^6)^2, (a^6)^3, (a^6)^4\}$$
$$= \{e, a^6, a^{12}, a^{18}, a^{24}\}.$$

7. All non-identity elements.

12. Yes ; $[1], [3], [7], [9]$ are the generators $\{[0]\}, \{[0],[5]\}$, $\{[0],[2],[4],[6],[8]\}$ and Z_{10} are the only subgroups of Z_{10}.

13. 2 and 6

14. (i) $\{e, a^4, a^8, a^{12}, a^{16}\}$

(ii) G_1.

16.

*	e	a	b	c	d
e	e	a	b	c	d
a	a	d	e	b	c
b	b	e	c	d	a
c	c	b	d	a	e
d	d	c	a	e	b

17. Soln: Let H be a finite subgroup of $C^* = C \setminus \{0\}$. Let $|H| = n$ and $a \in H$. Then by the Knocon theorem [Let G be a group of finite order n and $a^n = e$], $a^n = 1$. Hence any element of H is a root of $x^n = 1$. On the other hand, $x^n = 1$ has only n distinct roots, so it follows that $H = \{w \in C^* : w \text{ is a root of } x^n = 1\}$. We know that the set of n^{th} roots of unity forms a cyclic group. Hence H is a cyclic subgroup of C^*.

18. Soln: Let $a \in G_1$, $a \neq e$. Then $H = \langle a \rangle$ is a cyclic subgroup of G_1. Now $|H|$ divides $|G_1| = p^n$ and so $|H| = p^m$ for some $m \in Z$, $0 < m \leq n$. Now in a cyclic group of order p^m, for every

divisor d of p^m, there exists a subgroup of order d. Since p divides $|\langle a\rangle|$, there exists a subgroup T of H such that $|T| = p$. Let $T = \langle b\rangle$. Then $o(b) = p$. Hence the result.

20. For Z_6, generators are 1 and 5; for Z_8, generators are 1, 3, 5 and 7; for Z_{20}, generators are 1, 3, 7, 9, 11, 13, 17 and 19.

22. $\langle 20\rangle = \{20, 10, 0\}$
$\langle 10\rangle = \{10, 20, 0\}$

24. $\langle 3\rangle = \{3, 9, 7, 1\}$, $\langle 7\rangle = \langle 7, 9, 3, 1\rangle$

25. $\langle 1\rangle, \langle 7\rangle, \langle 11\rangle, \langle 17\rangle, \langle 19\rangle, \langle 29\rangle$.

26. Yes, by the known theorem [Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a\rangle| = n$, then the order of any subgroup of $\langle a\rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a\rangle$ has exactly one subgroup of order k - namely, $\langle a^{n/k}\rangle$]. The subgroups of Z are of the form $\{0, \pm n, \pm 2n, \pm 3n, \cdots\}$ where n is any integer.

28. 1000000, 3000000, 5000000, 7000000
by the known theorem [Every subgroup of a cyclic group is a cyclic. Moreover, if $|\langle a\rangle| = n$, then the order of any subgroup of $\langle a\rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a\rangle$ has exactly one subgroup of order k - namely, $\langle a^{n/k}\rangle$], $\langle 1000000\rangle$ is the unique subgroup of order 8 and only those on the list are generators.

30. 4, 3·4, 7·4, 9·4.

32. 1 and 2.

34. Use the fact the a cyclic group of even order has a unique element of order 2.

Set-VI Practice Problems

* Normal Subgroups *

(1) Let H be a proper subgroup of a group G such that for all $x, y \in G \setminus H$, $xy \in H$. Prove that H is a normal subgroup of G.

(2) (a) Let H be a subgroup of a group G. Show that for any $g \in G$, $K = gHg^{-1} = \{ ghg^{-1} \mid h \in H \}$ is a subgroup of G and $|K| = |H|$.

(b) If H is the only subgroup of order n in a group G, then prove that H is a normal subgroup.

(3) Show that $K = \{ e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3) \}$ is a normal subgroup of A_4.

(4) Let $GL(2, \mathbb{R})$ denote the set of all non singular 2×2 matrices with real entries. Show that $SL(2, \mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, \mathbb{R}) : ad - bc = 1 \right\}$ is a normal subgroup of the group $GL(2, \mathbb{R})$.

(5) Let T denote the group of all non singular upper triangular 2×2 matrices with real entries, i.e, the matrices of the form, $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ where $a, b, c \in \mathbb{R}$ and $ac \neq 0$. Show that $H = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \right\}$ is a normal subgroup of T.

(6) In the Symmetric group S_3, show that $H = \{ e, (2\,3) \}$ is a subgroup but not a normal subgroup.

(7) Show that $H = \{ e, (1\,2)(3\,4) \}$ is not a normal subgroup of A_4.

(8) In A_4, find subgroups H and K such that H is normal in K and K is normal in A_4, but H is not normal in A_4.

(9) Show that A_3 is a normal subgroup of S_3.

(10) Let G be a group and H a subgroup of G. If for all $a, b \in G$, $ab \in H$ implies $ba \in H$, then Prove that H is a normal subgroup of G.

(11) Show that $12\mathbb{Z}$ is a normal subgroup of the group $(3\mathbb{Z}, +)$. write the Cayley table for the factor group $3\mathbb{Z}/12\mathbb{Z}$.

(12) write down the Cayley table for the quotient group $\mathbb{Z}/15\mathbb{Z}$

(13) Let $G = \langle a \rangle$ be the cyclic group such that $o(a) = 12$. Let $H = \langle a^4 \rangle$. Find the order of a^3H in G/H.

(14) write down the Cayley table for the quotient group A_4/K, where $K = \{e, (1\,2)(3\,4), (1\,4)(3\,2), (1\,3)(2\,4)\}$. Is the group A_4/K a Commutative group?

(15) Let $\mathbb{R}^*$ be the group of all non-zero real numbers under usual multiplication. show that the set $\mathbb{R}^+$ of all positive real numbers is a subgroup of $\mathbb{R}^*$. What is the index of $\mathbb{R}^+$ in $\mathbb{R}^*$?

(16) Let G be a group and $a \in Z(G)$. Prove that $H = \langle a \rangle$ is a normal subgroup.

(17) Let H be a normal subgroup of a group G. Prove that
(i) if G is Commutative, then so is the quotient group G/H.
(ii) if G is cyclic, then so is G/H.

(18) Let G be a group. Let H be a subgroup of G such that $H \subseteq Z(G)$. show that if G/H is cyclic, then $G = Z(G)$, i.e, G is abelian.

(19). Let K be a normal subgroup of a group G such that $[G:K]=m$. If n is +ve integer such that $\gcd(m,n)=1$, then show that $K \supseteq \{g \in G \mid o(g)=n\}$

(20). Let K be a normal subgroup of a finite group. If G/K has an element of order n, then show that G has an element of order n.

(21) Let H be a subset of a group G and let the set N(H), called the normalizer of H in G, be defined by $N(H)=\{a \in G \mid aHa^{-1}=H\}$. Prove that N(H) is a subgroup of G. If in addition H be a subgroup of G, then Prove that

(a) H is normal in N(H)

(b) N is normal in G if and only if $N(H)=G$.

(c) N(H) is the largest subgroup of G in which H is normal, i.e, if H is normal in a subgroup K of G, then $K \subseteq N(H)$.

(22). Let G be a group. Let H be a normal subgroup of G. Define the relation ρ_H on G by, for all $a,b \in G$, $a \rho_H b$ if and only if $ab^{-1} \in H$. Prove that (i) ρ_H is an equivalence relation on G.

[Note: An equivalence relation ρ on a group G is called a congruence relation if for all $a,b,c \in G$, $a \rho b$ implies that $ca \rho cb$ and $ac \rho bc$]

(ii) the ρ_H class $a\rho_H = \{b \in G \mid a \rho_H b\}$ is the left coset aH.

(iii) $H = e\rho_H$

(22) Let H be a subgroup of a group G. Define a relation in G by $\rho_H = \{(a,b) \in G \times G \mid a^{-1}b \in H\}$. show that if ρ_H is a congruence relation, then H is a normal subgroup of G.

(23) Let ρ be a congruence relation on a group G. show that there exists a normal subgroup H of G such that $\rho = \{(a,b) \in G \times G \mid a^{-1}b \in H\}$

(25) Prove that a non-empty subset H of a group G is normal subgroup of $G \Leftrightarrow$ for all $x, y \in H$, $g \in G$, $(gx)(gy)^{-1} \in H$.

(26) If G is the union of proper normal subgroups such that any two of them have only e in common, then G is Abelian.

(27) show that a subgroup N of G is normal iff $xy \in N \Rightarrow yx \in N$.

(28) Let H be a subgroup of G and let $N = \bigcap_{x \in G} xHx^{-1}$ then show that N is a normal subgroup of G.

(29) Let H be a subset of a group G. Let $N(H) = \{x \in G \mid Hx = xH\}$ be the normalizer of H in G.

(i) If H is a subgroup of G then $N(H)$ is the largest subgroup of G in which H is normal.

(ii) If H is a subgroup of G then H is normal in G iff $N(H) = G$.

(iii) show by an example, the converse of (ii) fails (if H is only a subset of G)

(iv) If H is a subgroup of G and K is a subgroup of $N(H)$ then H is normal subgroup of HK

(30) Let H be normal in G such that $o(H)$ and $\frac{o(G)}{o(H)}$ are co-prime. Show that H is unique subgroup of G of given order.

(31)

(32) Let $\langle Z, + \rangle$ be the group of integers and let $N = \{3n \mid n \in Z\}$ then N is a normal subgroup of Z.

(33) Let N be a normal subgroup of a group G. Show that $o(Na) \mid o(a)$ for any $a \in G$.

(34). If G is a group such that $\frac{G}{Z(G)}$ is cyclic, where $Z(G)$ is centre of G then show that G is abelian.

(35) Give an example of an infinite group in which every element is of finite order.

Answers

(1) Let $x \in G/H$. Then $x^{-1} \in G \setminus H$. Let $y \in H$. Then $xy \in G \setminus H$, (for otherwise, $x = xyy^{-1} \in H$). Thus $xy, x^{-1} \in G \setminus H$. Hence $xyx^{-1} \in H$. Also for any $x \in H$, we have $xyx^{-1} \in H$. Thus H is normal subgroup of G.

(2) Let $a = ghg^{-1}$ and $b = gh_1g^{-1}$ be two elements of K. Then

$$ab^{-1} = ghg^{-1}(gh_1g^{-1})^{-1}$$
$$= ghg^{-1}((g^{-1})^{-1}h_1^{-1}g^{-1})$$
$$= ghg^{-1}gh_1^{-1}g^{-1}$$
$$= ghh_1^{-1}g^{-1} \quad \text{---(*)}$$

Now, $h, h_1 \in H$ and H is a subgroup of G. Hence $hh_1^{-1} \in H$. Then from (*) above,

$$ab^{-1} = g(hh_1^{-1})g^{-1} \in gHg^{-1}$$

Hence K is a subgroup of G.

To show that $|K| = |H|$, we Prove that there exists a bijective function from H onto gHg^{-1}. Define $f: H \to gHg^{-1}$ by $f(h) = ghg^{-1}$ for all $h \in H$. Let h_1 and $h_2 \in H$, such that $f(h_1) = f(h_2)$. Then $gh_1g^{-1} = gh_2g^{-1}$. By Cancellation, we obtain $h_1 = h_2$. Hence f is injective. Let $a \in gHg^{-1}$. Then $a = ghg^{-1}$ for some $h \in H$ and $f(h) = ghg^{-1} = a$. this implies f is surjective and so $|H| = |K|$.

(b) Let $g \in G$. from the above Problem, gHg^{-1} is a subgroup of G and $|H| = |gHg^{-1}|$.

Hence $|gHg^{-1}| = n$ and so by the given condition $gHg^{-1} = H$. This is

true for all $g \in G$. thus we find that H is a normal subgroup of G.

(3). A_4 has 12 elements. These elements are $e, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (14)(23)$. Hence A_4 has no element of order 4. the only elements of order 2 are $a = (12)(34)$, $b = (13)(24)$, $c = (14)(23)$. Now $a^2 = b^2 = e$ and $ab = ba = c$. Hence $K = \{e, a, b, ab = c\}$ is a subgroup of order 4 and this is the only subgroup of order 4 in G.

∴ we conclude that K is a normal subgroup of G.

(∵ we know that if H is the only subgroup of order n in a group G, then prove that H is a normal subgroup.)

(25) Sol'n: Let H be normal subgroup of G.

Let $x, y \in H$, $g \in G$ be any elements;

then $(gx)(gy)^{-1} = (gx)(y^{-1}g^{-1}) = g(xy^{-1})g^{-1} \in H$

as $xy^{-1} \in H$, $g \in G$, H is normal in G.

Conversely, we show H is normal subgroup of G.

Let $x, y \in H$ be any elements,

then $xy^{-1} = exy^{-1}e = (ex)(ey)^{-1} \in H$ as $e \in G$

i.e., H is a subgroup of G.

Again let $h \in H$, $g \in G$ be any elements

then as $(gh)(ge)^{-1} \in H$

we get $(gh)(eg^{-1}) \in H$

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

$\Rightarrow$ H is normal.

(26) Sol'n: Let $G = H_1 \cup H_2 \cup \cdots \cup H_k$

Let $x, y \in G$ be any elements, then $x \in H_i$, $y \in H_j$ for some i, j

Case(i): If $i \neq j$ then $xy = yx$

Case(ii): $i = j$, then $x, y \in H_i$.

Now, since H_i is a proper subgroup of G, $\exists$ some $g \in G$ such that, $g \notin H_i$ (and $g \in H_t$ for some $t \neq i$)

We know that g commutes with both x and y.

i.e. $xg = gx$ and $yg = gy$

Now $g \notin H_i \Rightarrow gx \notin H_i$

$\therefore gx$ also commutes with x, y and $xy \in H_i$

Also $(xy)g = g(xy)$

$= (gx)y$

$= y(gx)$

$= (yx)g$

$\Rightarrow xy = yx$ (Cancellation)

Hence G is abelian.

(27) Let N be normal in G and let $xy \in N$

Since $yx = y(xy)y^{-1}$

and $xy \in N$, $y \in G$, N is normal in G we find

$y(xy)y^{-1} \in N \Rightarrow yx \in N$

Conversely, let $n \in N$, $g \in G$ be any elements

then $n \in N \Rightarrow (ng)g^{-1} \in N$

$\Rightarrow g^{-1}(ng) \in N$ (given condition)

$\Rightarrow$ N is normal in G.

(28) Sol'n: we know that intersection of subgroups is a subgroup and also subsets of the type xHx^{-1} are subgroups.

Hence $\bigcap_{x \in G} xHx^{-1}$ is a subgroup of G.

Let $g \in G$ be any element, then

$gNg^{-1} = g(\bigcap_{x} xHx^{-1})g^{-1} = \bigcap (gxHx^{-1}g^{-1}) = \bigcap (yHy^{-1}) = N$.

showing thereby that N is normal.

we have used above the result $g(H \cap K) = gH \cap gK$ for subgroups H, K and $g \in G$, It is true as:

$x \in g(H \cap K) \Rightarrow x = ga, a \in H \cap K$

$a \in H \Rightarrow ga \in gH \Rightarrow x \in gH \Rightarrow x \in gH \cap gK$

$a \in K \Rightarrow ga \in gK \Rightarrow x \in gK$

Also $y \in gH \cap gK \Rightarrow y \in gH, y \in gK$

$\Rightarrow y = gh, y = gk \quad h \in H, k \in K$

$\Rightarrow gh = gk$

$\Rightarrow h = k \Rightarrow h, k \in H \cap K$.

$\therefore y = gh \in g(H \cap K)$ proving the result.

(29) Sol'n: (i) we show H is normal in N(H)

Since $Hh = hH$ for all $h \in H$, we find

$h \in N(H)$ for all $h \in H$

thus $H \leq N(H)$.

Again by definition of N(H), $Hx = xH$ for all $x \in N(H)$

$\Rightarrow$ H is normal in N(H)

To show that N(H) is the largest subgroup of G in which H is normal suppose K is any subgroup of G such that H is normal in K.

then $k^{-1}Hk = H$ for all $k \in K$

$\Rightarrow Hk = kH$ for all $k \in K$

$\Rightarrow k \in N(H)$ for all $k \in K$

$\Rightarrow K \subseteq N(H)$

(ii) Let H be a normal subgroup of G

then $N(H) \subseteq G$ (by definition)

Let $x \in G$ be any element,

then $xH = Hx$ as H normal in G.

$\Rightarrow x \in N(H) \Rightarrow G \subseteq N(H)$

hence $G = N(H)$

Conversely, let $G = N(H)$

H is a subgroup of G (given)

Let $h \in H$, $g \in G$ be any elements

then $g \in N(H)$ as $N(H) = G$

$\Rightarrow gH = Hg$

$\Rightarrow H$ is normal in G.

(iii) Consider $G = \langle a \rangle = \{e, a, a^2, a^3\}$

G is abelian being cyclic is abelian group.

Take $H = \{a\}$

Then H is a subset and not a subgroup of G ($e \notin H$)

Also $N(H) = G$ as G is abelian.

(iv) Let K be a subgroup of $N(H)$.

then $k \in K \Rightarrow k \in N(H) \Rightarrow Hk = kH$

i.e. $Hk = kH$ for all $k \in K$

$\Rightarrow HK = KH$

$\Rightarrow HK$ is subgroup of $N(H)$

Note, $\cdot\ h \in H \Rightarrow Hh = hH\ (=H)$

$\Rightarrow H \subseteq N(H)$ Also $K \subseteq N(H)$

Again $H \subseteq HK \subseteq N(H)$

hence H is a subgroup of HK

$\Rightarrow H$ is a subgroup of HK

$[a \in HK \Rightarrow a \in N(H) \Rightarrow Ha = aH]$

(30) Soln: Let $o(H) = m$, $\frac{o(G)}{o(H)} = n$. Suppose K is a subgroup of G of order m.

Then $o(HK) = \frac{m \cdot m}{d}$, where $d = o(H \cap K)$

Since H is normal, $HK \leq G$.

Thus $o(HK) \mid o(G)$

$\Rightarrow m \cdot \frac{m}{d} \mid m \cdot n \Rightarrow \frac{m}{d} \mid n$

$\Rightarrow d \frac{m}{d} \mid dn \Rightarrow m \mid dn$

$\Rightarrow m \mid d$ as $(m, n) = 1$

But $d \mid m$ as $H \cap K \leq H$,

Thus $d = m$ and hence

$o(H \cap K) = o(H) = o(K)$

$\Rightarrow H = K$

(31) Let G be the set of 2×2 matrices over reals of the type $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ where $ad \neq 0$. Then it is easy to see that G will form a group under matrix multiplication. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ will be identity, $\begin{bmatrix} 1/a & -b/ad \\ 0 & 1/d \end{bmatrix}$ will be inverse of any element $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$. Also G is not abelian.

Let N be the subset containing members of the type $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$. Then N is a subgroup of G. (Prove!) Also it is normal as the product of the type.

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \frac{1}{a} & \frac{-b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix} = \begin{bmatrix} 1 & akd + bd - b/d \\ 0 & 1 \end{bmatrix} \in N.$$

So we get the quotient group $\frac{G}{N}$. we show $\frac{G}{N}$ is abelian.

Let $Nx, Ny \in \frac{G}{N}$ be any elements, then $x, y \in G$

Let $x = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, $y = \begin{bmatrix} c & e \\ 0 & f \end{bmatrix}$

$\frac{G}{N}$ will be abelian iff $NxNy = NyNx$

$\Leftrightarrow Nxy = Nyx$

$\Leftrightarrow xy(yx)^{-1} \in N$

$\Leftrightarrow xyx^{-1}y^{-1} \in N$

All we need check now is that the product

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} c & e \\ 0 & f \end{bmatrix}\begin{bmatrix} \frac{1}{a} & \frac{-b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix}\begin{bmatrix} \frac{e}{cf} \\ 0 & \frac{1}{f} \end{bmatrix}$$ is a matrix of the type $\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$.

Thus we can have an abelian quotient group, without the 'parent' group being abelian

→ (32) Sol'n $\frac{Z}{N}$ will consist of members of the type $N+a, a \in Z$.

we show $\frac{Z}{N}$ contains only three elements. Let $a \in Z$ be any element where $a \neq 0, 1, 2$ then we can write, by division algorithm.

$a = 3q + r$ where $0 \leq r \leq 2$.

$\Rightarrow N+a = N + (3q+r) = (N+3q) + r = N + r$ as $3q \in N$.

but r can take values $0, 1, 2$.

Hence $N+a$ will be one of

$N, N+1, N+2$

or that $\frac{Z}{N}$ contains only these three members.

Remarks: (i) This example also tells us that in case of cosets, $Ha=Hb$ may not necessarily mean $a=b$.

(ii) This serves as an example of an infinite group which has a subgroup N having finite index in G.

→(33) Sol^n Let $o(a)=n$

then n is the least +ve integer such that $a^n=e$.

This gives $Na^n=Ne$

$\Rightarrow Na\cdot a \cdots a = N$ (n times) $\Rightarrow a=N$

$\Rightarrow Na\cdot Na \cdots Na = N$ (n times) $\Rightarrow Na=N$

$\Rightarrow (Na)^n = N$; $Na \in \frac{G}{N}$ and N is identity of $\frac{G}{N}$

$\Rightarrow o(Na) \mid n$ or $o(Na) \mid o(a)$

→(34). Sol^n: Let us write $Z(G)=N$. Then $\frac{G}{N}$ is cyclic, suppose it is generated by Ng.

Let $a, b \in G$ be any two elements.

then $Na, Nb \in \frac{G}{N}$

$\Rightarrow Na=(Ng)^n$, $Nb=(Ng)^m$ for some n, m

$\Rightarrow Na = Ng\cdot Ng \cdots Ng = Ng^n$

$Nb = Ng^m$

$\Rightarrow ag^{-n} \in N$, $bg^m \in N$

$\Rightarrow ag^{-n}=x$, $bg^m=y$ for some $x, y \in N$

$\Rightarrow a=xg^n$, $b=yg^m$

$\Rightarrow ab = (xg^n)(yg^m) = x(g^n y)g^m$

$= x(yg^n)g^m$ as $y \in N = Z(G)$

$= xyg^n g^m$

$= xyg^{n+m}$

similarly $ba = (yg^m)(xg^n) = y(g^m x)g^n = y(xg^m)g^n$

$= (yx)g^{m+n}$

$\Rightarrow ab = ba$ as $xy = yx$ as $x, y \in Z(G)$

showing that G is abelian.

Remarks (i): (i) We are talking about $\frac{G}{Z(G)}$ assuming, therefore, that $Z(G)$ is a normal subgroup of G.

(ii) One can, moving on same lines as in the above solution prove that if G/H is cyclic, where H is a subgroup of $Z(G)$ then G is abelian

(iii) If G is a non abelian group then $G/Z(G)$ is not cyclic.

→(35) sol'n: Let $\langle Z, + \rangle$ be the group of integers under addition.

Let $G = \left\{ Z + \frac{m}{p^n} \;\middle|\; m, n \text{ are integers}, n \geq 0, p = \text{fixed prime} \right\}$

Then G is a subgroup of $\frac{Q}{Z}$ where $\langle Q, + \rangle$ is the group of rationals under addition.

$0_G = Z + \frac{0}{p^0} = Z + 0 = Z = \text{zero of } G$

$\Rightarrow$ order of $Z + \frac{m}{p^n}$ divides p^n.

$\Rightarrow$ order of $Z + \frac{m}{p^n}$ is p^r, $r \leq n$.

$\Rightarrow$ order of every element in G is finite.

Here G is an infinite group.

In fact, one can also show that every subgroup $H \neq G$ is of finite order. So, this also gives an example of an infinite group in which every proper subgroup is of finite order.

→ we construct some finite groups whose elements, called permutations, act on finite sets.

- These groups will provide us with examples of finite non-abelian groups.

- The notion of a permutation of a set as a rearrangement of the elements of the set.

Now for the set $\{1,2,3,4,5\}$.

a rearrangement of the elements could be given below schematically as:

(i)	(ii)
$1 \to 4$	$1 \to 3$
$2 \to 2$	$2 \to 2$
$3 \to 5$	$3 \to 4$
$4 \to 3$	$4 \to 5$
$5 \to 1$	$5 \to 3$

Let us think of the diagram (i) as a function mapping of each element listed in the left column in a single (not necessarily different) element from the same set listed at the right.

Furthermore, to be a permutation of the set, this mapping must be such that each element appearing in the right column once and only once.

The diagram in fig (ii) doesnot give a permutation, for 3 appears twice while 1 doesnot appear at all in the right column.

We now define a permutation to be such a mapping:

Defn: A permutation of a set A is a function $\phi: A \to A$ that is both one-one and onto.

(or)

Suppose A is a finite set having 'n' distinct elements. Then a 1-1 mapping of A onto itself is called a permutation of degree 'n'.

→ The number of elements in the finite set A is known as the degree of permutation.

[redacted]

I. Let $\phi(a_1) = b_1$, $\phi(a_2) = b_2 \ldots\ldots \phi(a_n) = b_n$

where $\{b_1, b_2, \ldots\ldots b_n\} = \{a_1, a_2, \ldots\ldots a_n\}$.

i.e, $b_1, b_2, \ldots\ldots b_n$ is some arrangement of n elements $a_1, a_2, \ldots\ldots a_n$.

II. We can introduce a two-line notation.

i.e, $\phi = \begin{pmatrix} a_1 & a_2 & \ldots\ldots & a_n \\ b_1 & b_2 & \ldots\ldots & b_n \end{pmatrix}$

i.e, each element in the second row is the ϕ image of the element the first row lying directly above it.

Ex: Let $A = \{1, 2, 3, 4\}$

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

Here the elements 1, 2, 3, 4 have been replaced by 2, 4, 1, 3 respectively.

$\phi(1) = 2$; $\phi(2) = 4$, $\phi(3) = 1$ & $\phi(4) = 3$

Equality of two permutations:

Two permutations f and g of degree 'n' are said to be equal if $f(a) = g(a)$ $\forall a \in S$, where S is a finite set of 'n' distinct elements.

Ex: If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 3 & 1 & 4 & 2 \end{pmatrix}$

Here $f = g$

(∵ in both cases 1 is replaced by 2, 2 by 3, 3 by 4 and 4 by 1)

Note: The interchange of columns does not change the permutation.

Ex: If $f = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix}$

then $f = \begin{pmatrix} a_2 & a_1 & a_3 \\ b_2 & b_1 & b_3 \end{pmatrix} = \begin{pmatrix} a_1 & a_3 & a_2 \\ b_1 & b_3 & b_2 \end{pmatrix}$ etc.

~~Total no of distinct permutations of degree~~

~~If S is a finite set having n distinct~~

~~then we have n! distinct arrangements~~

~~of n elements. Therefore there will be n! distinct permutations~~

~~of degree n.~~

~~If P_n be the set consisting of all permutations~~

~~of degree n, then the P_n is set will have n! distinct~~

~~elements.~~

This set P_n is called the symmetric set of permutations of degree 'n'.

Sometimes it is denoted by S_n.

i.e $P_n = \{f : f$ is a permutation of degree $n\}$.

Ex: The set P_3 of all permutations of degree 3 will have 3! (i.e, 6) elements.

i.e, $P_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$.

Identity permutation:

Identity permutation on $S = \{a_1, a_2, \ldots a_n\}$ in S_n is denoted by I.

where $I = \begin{pmatrix} a_1 & a_2 \ldots a_n \\ a_1 & a_2 \ldots a_n \end{pmatrix}$ or $\begin{pmatrix} b_1 & b_2 \ldots b_n \\ b_1 & b_2 \ldots b_n \end{pmatrix}$.

$b_1, b_2, \ldots b_n$ are nothing but the elements $a_1, a_2, \ldots a_n$ of S in some order.

If $S = \{1,2,3,4,5\}$ then Identity permutation on S is $I = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 4 & 3 & 1 & 5 & 2 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$ etc.

Product of permutations (or) multiplication of permutations (or) Composition of permutations in S_n.

Let S_n be the set of all permutations of degree n.

Let $f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$ and $g = \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ c_1 & c_2 & \cdots & c_n \end{pmatrix}$ be any two permutations of S_n;

Here $b_1, b_2, \ldots, b_n$ or $c_1, c_2, \ldots, c_n$ are not the elements $a_1, a_2, \ldots, a_n$ of S in some order.

Now $f(a_1) = b_1$, $g(b_1) = c_1$, $f(a_2) = b_2$, $g(b_2) = c_2$ etc.

By defn we have

$$c_1 = g(b_1) = g(f(a_1)) = (gf)(a_1)$$

i.e., $(gf)(a_1) = c_1$

Similarly $(gf)(a_2) = c_2$, $\ldots$ $(gf)(a_n) = c_n$.

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

$\therefore gf$ is also a permutation of degree 'n' on S and hence $gf \in S_n$ for $g, f \in S_n$.

Ex: If $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ then $AB = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$(\because (AB)(1) = A(B(1)) = A(3) = 1$ etc.

and $BA = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $(\because (BA)(1) = B(A(1)) = B(2) = 1$ etc.

→ If $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$

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

$\therefore fg \neq gf$.

$\therefore$ Multiplication of permutations is not commutative

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

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

Similarly $If = f$.

Note: Some times we may have $fg = gf$.

If $f = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$, $g = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$

then $fg = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix} = gf$.

Multiplication of permutations is associative

If $f = \begin{pmatrix}1&2&3&4&5\\3&1&4&5&2\end{pmatrix}$, $g = \begin{pmatrix}1&2&3&4&5\\1&3&4&5&2\end{pmatrix}$ and $h = \begin{pmatrix}1&2&3&4&5\\4&3&2&5&1\end{pmatrix}$

then $(fg)h = f(gh)$.

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

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

Inverse of a permutation:

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

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

Also $f^{-1}f = \begin{pmatrix}b_1&b_2&\cdots&b_n\\a_1&a_2&\cdots&a_n\end{pmatrix}\begin{pmatrix}a_1&a_2&\cdots&a_n\\b_1&b_2&\cdots&b_n\end{pmatrix}$

$= \begin{pmatrix}a_1&a_2&\cdots&a_n\\a_1&a_2&\cdots&a_n\end{pmatrix} = I$

Similarly $ff^{-1} = I$.

Note: [1]. The set S_n of all permutations on n symbols is a finite group of order $n!$ w.r.t multiplication of permutations.

for $n \leq 2$, the group is abelian and for $n \geq 3$ the group is non-abelian.

[2]. To write the inverse of a permutation, write the 2nd row as 1st row and 1st row as 2nd row.

[3]. The group S_n of all permutations of degree 'n' is called the symmetric group of degree 'n' or the symmetric group of order $n!$.

Problem → Show that the set P_3 of all permutations on three symbols 1, 2, 3 is a finite non-abelian group of order 6 w.r.t permutation multiplication as composition.

Soln: we have

$$P_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$$

where

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ and } f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Now Construct the composition table:

	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_6	f_1	f_5	f_4	f_2
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_4	f_2	f_3	f_6	f_1
f_6	f_6	f_3	f_4	f_2	f_1	f_5

$f_1 f_1 = f_1$, $f_2 f_2 = f_2 f_1 = f_1$, $f_1 f_3 = f_3 f_1 = f_3$,
$f_1 f_4 = f_4 f_1 = f_4$, $f_1 f_5 = f_5 f_1 = f_5$, $f_1 f_6 = f_6 f_1 = f_6$.

$f_2f_2 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = f_1$

$f_2f_3 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = f_5$

$f_2f_4 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = f_6$

$f_2f_5 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = f_3$

$f_2f_6 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = f_4$.

$f_3f_2 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = f_6$

$f_3f_3 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = f_1$.

$f_3f_4 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = f_5$

$f_3f_5 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = f_4$

$f_3f_6 = f_2$.

$f_4f_2 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = f_5$

$f_4f_3 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = f_6$

$f_4f_4 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = f_1$

$f_4f_5 = f_2$ and $f_4f_6 = f_3$.

$f_5f_2 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = f_4$ and so on.

(i) Since all the entries in the composition table are elements of P_3.

$\therefore P_3$ is closed w.r.t multiplication of permutations.

(ii) multiplication of permutations is an associative

(iii) From the composition table the first row coincides with the top row.

Here identity permutation f_1 is the identity element.

Since $f_1f_1 = f_1$, $f_1f_2 = f_2$, $f_1f_3 = f_3$, $f_1f_4 = f_4 = f_2f_1$, $f_1f_5 = f_5 = f_3f_1$ and so on.

(iv) In the composition table, every row and every column contains the identity element.

Here $f_1f_1 = f_1$, $f_2f_2 = f_1$, $f_3f_3 = f_1$, $f_4f_4 = f_1$, $f_5f_6 = 1 = f_6f_5$.

(v) The composition is not commutative.

Since $f_4 f_2 = f_5$ & $f_2 f_4 = f_6$.

$\therefore f_4 f_2 \neq f_2 f_4$.

$\therefore P_3$ is a finite non-abelian group of order 6 w.r.t permutation multiplication.

Orbit of an element under a permutation

Defn: Let S be a non-empty set, $a \in S$ and f a permutation on S. If for $a \in S$, there exists a smallest positive integer i depending on a such that $f^i(a) = a$ then the set $\{a, f^1(a), f^2(a), \ldots, f^{i-1}(a)\}$ is called the orbit of a for the permutation f.

The ordered set $\{a, f^1(a), f^2(a), \ldots, f^{i-1}(a)\}$ is called a cycle of f.

Ex: Consider $S = \{1,2,3,4,5,6\}$ and a permutation on S be $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$.

Now we have $f^1(1) = 2$, $f^2(1) = f(2) = 1$.

$\therefore$ orbit of 1 under $f = \{1, f(1)\} = \{1,2\}$

we have $f^1(2) = 1$, $f^2(2) = f(1) = 2$.

$\therefore$ orbit of 2 under $f = \{2, f(2)\} = \{2,1\}$

we have $f(3) = 3$

$\therefore$ Orbit of 3 under $f = \{3\}$

we have $f^1(4) = 5$, $f^2(4) = f(5) = 6$, $f^3(4) = f(6) = 4$.

$\therefore$ orbit of 4 under $f = \{4,5,6\}$

we have $f(5) = 6$, $f^2(5) = f(6) = 4$, $f^3(5) = f(4) = 5$.

$\therefore$ Orbit of 5 under $f = \{5,6,4\}$.

we have $f^1(6) = 4$, $f^2(6) = 5$, $f^3(6) = 6$.

$\therefore$ Orbit of 6 under $f = \{6,4,5\}$

Hence the cycles of f are $(1,2)$, (3), $(4,5,6)$

Cyclic permutations:

Def: Consider a set $S = \{a_1, a_2, \ldots, a_n\}$ and a permutation $f = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_k & a_{k+1} & \cdots & a_n \\ a_2 & a_3 & a_4 & \cdots & a_{k+1} & a_1 & \cdots & a_n \end{pmatrix}$ on S.

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

This type of permutation f is called a cyclic permutation of length k or f is represented by $(a_1, a_2, \ldots, a_k)$ or $(a_2, a_3, \ldots, a_k, a_1)$ which is a cycle of length k or k-cycle.

→ Also we can write the cycle $(a_1, a_2, \ldots, a_k)$ as $(a_2, a_3, \ldots, a_k, a_1)$ or $(a_3, a_4, \ldots, a_k, a_1, a_2)$ etc.

Ex:

① $S = \{1, 2, 3, 4, 5, 6\}$ then a permutation of f on S is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 6 & 5 & 2 \end{pmatrix}$

It can be written as $(1\ 3\ 4\ 6\ 2)$

Since $f(1) = 3$, $f(3) = 4$, $f(4) = 6$, $f(6) = 2$, $f(2) = 1$ and $f(5) = 5$.

f is a cycle of length 5.

f can also be written as $(3\ 4\ 6\ 2\ 1)$ or $(4\ 6\ 2\ 1\ 3)$ etc. following the cycle order.

Ex ② If $S = \{1, 2, 3, 4, 5, 6, 7\}$ then a permutation f on S is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 7 & 6 & 1 \end{pmatrix}$. It can be written as $(1\ 3\ 5\ 7)$

f is cycle of length 4.

f can be written as $(3\ 5\ 7\ 1)$ or $(5\ 7\ 1\ 3)$ or $(7\ 1\ 3\ 5)$

Ex ③ If $S = \{1, 2, 3, 4, 5, 6\}$ then the permutation f on S is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 1 & 2 & 6 \end{pmatrix}$.

f is a cyclic permutation

Since $f(1) = 4$, $f(4) = 1$, $f(2) = 3$, $f(3) = 5$, $f(5) = 2$, $f(6) = 6$

Note: [1]. A cyclic permutation doesnot change by changing the places of its elements provided their cyclic order is not changed.

[2]. A cycle of length 1 is the identity permutation since $f(a_1) = a_1$, $f(a_2) = a_2$, ---- $f(a_n) = a_n$.

Transposition

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

Ex: If $S = \{1, 2, 3, 4, 5\}$ and a permutation f on S is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$ then $f = (2,3)$ is a cycle of length 2 and degree 5.

Observe that $f(1) = 3$, $f(3) = 2$ and the image of each element is itself (i.e., the remaining elements are left unchanged).

Here $f^{-1} = (3,2) = (2\ 3)$

i.e., $f^{-1} = f$.

i.e., the transposition is itself.

Disjoint cycles:

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

Ex: Let $S = \{1, 2, 3, 4, 5, 6, 7\}$

(i) If $f = (1\ 3\ 7)$ and $g = (2\ 4\ 5)$ then f, g are disjoint cycles.

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

→ Product of two cycles over the same set $S = \{1, 2, 3, 4, 5, 6\}$.

Ex: $f = (1\ 4\ 3)$, $g = (2\ 5)$

Now we find products gf, fg.

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

Also $gf = (2\,5)(1\,4\,3)$

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

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

$\therefore fg = gf$.

Note [1]. If f & g are two disjoint cycles then $fg = gf$.
i.e, the product of disjoint cycles is commutative.

[2]. we leave identity permutation (s) while writing the product of cycles.

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

$= (1\,5\,2)(3\,4)(6)$

$= (1\,5\,2)(3\,4)$ ($\because$ (6) is the identity permutation and it need not be shown).

$= (3\,4)(1\,5\,2)$

Observe that $(3\,4)$, $(1\,5\,2)$ are disjoint cycles.

Ex: $f = (2\,3\,6)$, $g = (1\,4\,6)$.

Now we find products fg, gf.

$\therefore fg = (2\,3\,6)(1\,4\,6)$

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

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

and $gf = (1\,4\,6)(2\,3\,6)$

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

Observe that f, g are not disjoint and $fg \neq gf$.

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

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

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

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

Ex: $(3\ 4)(3\ 5)(3\ 6) = (3\ 4)(3\ 6\ 5)$
$= (3\ 6\ 5\ 4)$

and $(3\ 4)(3\ 5)(3\ 6) = (3\ 5\ 4)(3\ 6)$
$= (3\ 6\ 5\ 4)$

Ex: If $f = (1\ 3\ 4)$, $g = (2\ 3)$, $h = (5\ 4\ 2)$
then we have $(fg)h = f(gh)$.

Inverse of a cyclic permutation:

Ex: 1) If $f = (2\ 3\ 4\ 1)$ of degree 5, then $f^{-1} = (1\ 4\ 3\ 2)$

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

2) If $f = (1\ 3\ 4\ 6)$ is a cyclic permutation on 6 symbols, its inverse $f^{-1} = (6\ 4\ 3\ 1)$
$= (4\ 3\ 1\ 6)$ etc.

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

Now $fg = (1\ 2\ 3\ 4\ 5\ 8\ 7\ 6)(4\ 1\ 5\ 6\ 7\ 3\ 2\ 8)$

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

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

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

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

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

$\therefore (fg)^{-1} = g^{-1}f^{-1}$

(4) If $f=(1\,3\,4)$, $g=(2\,3)$, $h=(5\,4\,2)$ then we have (i) $(fg)^{-1}=g^{-1}f^{-1}$ and (ii) $(fgh)^{-1}=h^{-1}g^{-1}f^{-1}$.

Order of a cyclic permutation:

Ex: If $A=\{1,2,3,4\}$ and $f=(2\,1\,3)$ then

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

i.e, $(2\,1\,3)(2\,1\,3)=(2\,3\,1)$

Now $f^3=f^2f$

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

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

∴ If f is a cycle of length 3 and degree 4 then $f^3=I$ and hence the order of f is 3.

Q: If $f=(1\,2\,3\,4\,5)$ then $f^2=(1\,3\,5\,2\,4)$

$f^3=f\cdot f^2=(1\,4\,2\,5\,3)$

$f^4=(1\,5\,4\,3\,2)$ and $f^5=I$.

∴ If f is a cycle of length 5 and degree 5 then $f^5=I$, and hence the order of f is 5.

→ Every permutation can be expressed as a product of disjoint cycles.

Ex: Let $f=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&1&4&8&6&9&7&5\end{pmatrix}$ be a permutation of degree 9 on the set $\{1,2,3,\ldots\ldots 9\}$.

we have $f=(1\,2\,3)(4)(5\,8\,7\,9)(6)$.

$=(1\,2\,3)(5\,8\,7\,9)$.

Q: Write down the following products as disjoint cycles.

(i) $(1\,3\,2)(5\,6\,7)(2\,6\,1)(4\,5)$

(ii) $(1\,3\,6)(1\,3\,5\,7)(6\,7)(1\,2\,3\,4)$.

Soln (i) $(1\,3\,2)(5\,6\,7)(2\,6\,1)(4\,5)$

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

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

Since 7 is the maximum in any cycle, we take every cycle as a permutation of a degree 7.

→ Express the product $(4\,5)(1\,2\,3)(3\,2\,1)(5\,4)(2\,6)(1\,4)$ on 6 symbols as the product of disjoint cycles.

Soln: $(4\,5)(1\,2\,3)(3\,2\,1)(5\,4)(2\,6)(1\,4)$

$= (4\,5)(5\,4)(2\,6)(1\,4)$

$(\because (3\,2\,1)^{-1} = (1\,2\,3)$ and $(2\,1)^{-1}(3\,2\,1) = I$

$= (2\,6)(1\,4)$ $(\because (5\,4)^{-1} = (4\,5))$

→ Every cycle can be expressed as a product of transpositions.

Ex: Let $f = (2\,4\,3)$ of degree 4.

Then $f = (2\,3)(2\,4)$ $\left(\because \begin{pmatrix} 1&2&3&4 \\ 1&3&2&4 \end{pmatrix}\begin{pmatrix} 1&2&3&4 \\ 1&4&3&2 \end{pmatrix} = \begin{pmatrix} 1&2&3&4 \\ 1&4&2&3 \end{pmatrix} = (2\,4\,3)\right)$

Also we have

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

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

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

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

∴ we can have

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

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

∴ Every cycle can be expressed as a product of transpositions in many ways.

Ex: Let $f = (1\,2\,3\,4)$

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

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

we have $f = (2\,1)(2\,4)(2\,3)$ etc.

Ex: Let $f = (a_1 a_2 \cdots a_n)$

we can have

$$f = (a_1 a_n)(a_1 a_{n-1}) \cdots (a_1 a_3)(a_1 a_2).$$

i.e, a cycle of length 'n' may be expressed as a product of $(n-1)$ transpositions.

Note:

In the case of any cycle the number of transpositions is either always odd or always even.

→ Every permutation can be expressed as a product of transpositions in many ways.

Even and odd permutation

A permutation is said to be an even (odd) permutation if it can be expressed as a product of an even (odd) number of transpositions.

Note: If f is expressed as a product of 'n' transpositions then n is even or 'n' is odd but not both and it is unique.

In other words, a permutation can be expressed as a product of an even number of transpositions or an odd number of transpositions. Hence the permutation group S_n on 'n' symbols can be split up into two disjoint sets, namely, the set of even permutations and the set of odd permutations.

→ Every transposition is an odd permutation.

– Identity permutation I is always an even permutation.

Since I can be expressed as a product of two transpositions.

Ex: $I = (12)(21)$

$= (12)(21)(13)(31)$ etc.

→ A cycle of length 'n' can be expressed as a product of $(n-1)$ transpositions.

– If 'n' is odd, then the cycle can be expressed as a product of even number of transpositions.

– If 'n' is even, then the cycle can be expressed as a product of odd number of transpositions.

→ The product of two odd permutations is an even permutation.

Proof: Let f, g be two odd permutations;

Let f can be expressed as a product of r (odd) transpositions and g can be expressed as a product of s (odd) transpositions.

$\therefore gf$ can be expressed as $r+s$ i.e, even number of transpositions.

$\therefore gf$ is even.

Note:

1. The product of two even permutations is an even permutation.
2. The product of an odd permutation and an even permutation is an odd permutation.

→ The inverse of an odd permutation is an odd permutation.

Proof: Let f be an odd permutation and I be the identity permutation.

$\therefore f^{-1}$ is also a permutation and $f^{-1}f = ff^{-1} = I$.

Since I is even permutation and f is odd permutation.

$\therefore f^{-1}$ is must be an odd permutation.

Note: The inverse of an even permutation is an even permutation.

→ Let S_n be the permutation group on 'n' symbols. Then of the n! permutations (elements) in S_n, $\frac{1}{2}n!$ are even permutations and $\frac{1}{2}n!$ are odd permutations.

Proof: Let $S_n = \{e_1, e_2, \ldots e_p, o_1, o_2, \ldots o_q\}$ be the permutation group on 'n' symbols where $e_1, e_2, \ldots e_p$ are even permutations and $o_1, o_2, \ldots o_q$ are odd permutations.

(∵ any permutation can be either even or odd but not both).

$\therefore p+q = n!$

Let $t \in S_n$ and t be a transposition.

Since permutation multiplication follows Closure law in S_n.

we have

$te_1, te_2, \ldots te_p, to_1, to_2, \ldots to_q$ as elements of S_n.

Since t is an odd permutation.

$\therefore te_1, te_2, \ldots te_p$ are all odd and $to_1, to_2, \ldots to_q$ are all even.

Here no two of the permutations $te_1, te_2, \ldots te_p$ are equal.

Because $te_i = te_j$ for $i \le p, j \le p$.

Since S_n is a group,
by LCL $e_i = e_j$ which is absurd.

$\therefore te_i \neq te_j$ for $i \leq p$, $j \leq s$ and hence the 'p' permutations $te_1, te_2, \ldots te_p$ are all distinct odd permutations in S_n.

But S_n contains exactly 'q' odd permutations.

$\therefore p \leq q$ —— (1)

Similarly we can show that q even permutations $to_1, to_2, \ldots to_q$ are all distinct even permutations in S_n.

$\therefore q \leq p$ —— (2)

from (1) & (2) we have

$$p = q = \frac{n!}{2} \quad (\because p + q = n!)$$

$\therefore$ Number of even permutations in S_n
= Number of odd permutations in S_n
$= \frac{n!}{2}$

Defn: Let S_n be the permutation group on 'n' symbols. The set of all $\frac{n!}{2}$ even permutations of S_n denoted by A_n, is called the alternating set of permutations of degree 'n'.

Theorem: The set A_n of all even permutations of degree 'n' forms a group of order $\frac{n!}{2}$ w.r.t permutation multiplication.

Proof: (i) Closure: Let $f, g \in A_n$:
then f, g are even permutations.
$\therefore gf$ is an even permutation.
$\therefore gf \in A_n$.

(ii) Associativity: Since a permutation is a bijection,

multiplication of permutations (composition of mappings) is associative.

(iii) Existence of left identity:

Let $f \in A_n$.

Let I be the identity permutation on the 'n' symbols then $I \in A_n$.

Since I is an even permutation.

$\therefore If = f$ for $f \in A_n$.

$\therefore$ Identity exists in A_n and I is the identity in A_n.

(iv) Existence of left inverse:

Let $f \in A_n$

Since f is even permutation.

$\therefore f^{-1}$ is also even permutation on 'n' symbols

$\therefore f^{-1}f = I$ for $f \in A_n$.

$\therefore$ Every element of A_n is invertible and inverse of f is f^{-1}.

$\therefore A_n$ forms a group of order $\frac{n!}{2}$.

($\because$ the number of permutations on 'n' symbols is $\frac{n!}{2}$)

Note: [1]. The group A_n is called an alternating group (or) alternating group of degree 'n' and the number of elements in A_n is $\frac{n!}{2}$

[2]. The product of two odd permutations is an even permutation and hence the set of odd permutations w.r.t permutation multiplication is not a group.

Ex: Examine whether the following permutations are even or odd.

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 5 & 6 & 7 & 1 \end{pmatrix}$. (ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 1 & 8 & 5 & 6 & 2 & 4 \end{pmatrix}$

(iii) $(1\ 2\ 3\ 4\ 5)(1\ 2\ 3)(4\ 5)$.

Sol^{n} (i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 5 & 6 & 7 & 1 \end{pmatrix} = (1\ 3\ 4\ 5\ 6\ 7)(2)$

$= (1\ 7)(1\ 6)(1\ 5)(1\ 4)(1\ 3)$

(product of 5 transpositions)

∴ The permutation is odd.

→ Express $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}$ as a product of transpositions.

→ Write down the inverses of the following permutations.

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$ (ii) $\begin{pmatrix} 4 & 2 & 3 & 1 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ (iii) $(2\ 5\ 1\ 6)(3\ 7)$

Ans: $(6\ 1\ 5\ 2)(7\ 3)$

→ Write down the following permutations as products of disjoint cycles.

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 1 & 4 & 8 & 2 & 6 & 5 \end{pmatrix}$ (ii) $(1\ 3\ 2\ 5)(1\ 4\ 3)(2\ 5\ 1)$

(iii) $(4\ 3\ 1\ 2\ 5)(1\ 4\ 5\ 2)$

→ Express $(1\ 2\ 3)(4\ 5\ 6)(1\ 6\ 7\ 8\ 9)$ as a product of disjoint cycles. Find its inverse.

→ Write down all the permutations on four symbols 1, 2, 3, 4 which of these permutations are even?

Sol^{n}: Let $S = \{1, 2, 3, 4\}$

There will be 4!

i.e, 24 permutations of degree 4.

If P_4 is the set of all permutations then

$P_4 = \{(1), (1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)$
$(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3)$
$(2\ 3\ 4), (2\ 4\ 3), (1\ 2)(3\ 4), (2\ 3)(1\ 4)$
$(3\ 1)(2\ 4), (1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4)$
$(1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)\}$

If A_4 is the set of all even permutations of degree 4 then A_4 will have $\frac{4!}{2}$ i.e, 12 elements.

i.e, $A_4 = \{ (1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (23)(14), (31)(24) \}$.

→ Show that the four permutations I, (ab), (cd), (ab)(cd) on four symbols a, b, c, d form a finite abelian group w.r.t the permutation multiplication.

Soln: Let $I = f_1$, $(ab) = f_2$, $(cd) = f_3$ and $(ab)(cd) = f_4$.

Let $G = \{f_1, f_2, f_3, f_4\}$.

Now construct the composition table

→ Show that the eight permutations (a), (abcd), (ac)(bd), (adcb), (ab)(cd), (bc)(ad), (bd), (ac) on four symbols a, b, c, d form a finite non-abelian group w.r.t permutation multiplication.

→ Show that the set G of four permutations I, (12)(34), (13)(24) and (14)(23) on four symbols 1, 2, 3, 4 is abelian group w.r.t the permutation multiplication.

(This group is known as the Klein-4-group)

→ prove that the set A_3 of three permutations (a), (abc), (acb) on three symbols a, b, c forms a finite abelian group w.r.t the permutation multiplication

Order of a cycle

Let $f = (1\ 2\ 3 \ldots n)$ be a cycle of length n

f moves every symbol two places along

f moves every symbol three places along

f moves every symbol n places along

i.e, $f^n = (1)(2) \ldots (n)$

i.e, identity permutation.

∴ Order of f is n.

In particular

If $f = (1\,2\,3\,4\,5)$ then $f^2 = (1\,3\,5\,2\,4)$, $f^3 = (1\,4\,2\,5\,3)$

$f^4 = (1\,5\,4\,3\,2)$, $f^5 = (1)(2)(3)(4)(5)$ = Identity permutation

$\therefore f^5 = I$

$\therefore o(f) = 5$.

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

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

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

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

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

$= (1\,4\,2\,5\,3)$

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

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

$= (1\,5\,4\,3\,2)$

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

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

- **Order of the product of the disjoint cycles of lengths $m_1, m_2, \ldots, m_k$:**

Suppose a permutation f is the product of disjoint cycles of lengths $m_1, m_2, \ldots, m_k$. The order of f will be the L.C.M. (least common multiple) of the integers $m_1, m_2, \ldots, m_k$.

Eg: Find the order of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$.

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

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

$\therefore o(f)$ = L.C.M of 1, 3

$= 3$.

→ If $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$, $\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}$, then find σ^{100} and μ^{100}.

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

$= (1\,5)(3\,4)(2)(6)$

$O(\mu) = \text{LCM}[\text{lengths of } (1\,5), (3\,4), (2), (6)]$

$= \text{LCM}\{2, 2, 1, 1\} = 2$

$\therefore O(\mu) = 2$

$\mu^2 = I$ (By defn of an order of element)

Thus $(\mu^2)^{50} = I^{50}$

$= I$

$\therefore \mu^{100} = I$

PT 2007 Let $\sigma = (1\,3\,5\,7\,11)(2\,4\,6) \in S_{11}$. What is the smallest +ve integer 'n' such that $\sigma^n = \sigma^{37}$.

(a) 3 (b) 5 (c) 7 (d) 11.

Soln: $O(\sigma) = \text{LCM of } 5 \text{ \& } 3$

$= 15$

$\therefore \sigma^{15} = I$

$\therefore \sigma^{37} = (\sigma^{15})^2 \cdot \sigma^7$

$= I \cdot \sigma^7 = \sigma^7$

$\sigma^n = \sigma^{37} = \sigma^7$

$\Rightarrow \boxed{n = 7}$

PT 2006 Consider the permutation $\alpha = (1\,2\,3)(1\,4\,5)$ on the set $\{1, 2, 3, 4, 5\}$. What is the permutation α^{99}

(a) $(5\,4\,1)(3\,2\,1)$ (b) $(5\,4\,1)(1\,2\,3)$ (c) $(3\,2\,1)(5\,4\,1)$ (d) $(1\,3\,2)(1\,5\,4)$

Soln: $\alpha = (1\,2\,3)(1\,4\,5)$

$= (1\,3)(1\,2)(1\,5)(1\,4) = (1\,4\,5\,2\,3)$

$\alpha^5 = I \Rightarrow \alpha^{99} = (\alpha^5)^{20} \alpha^{-1}$

$= I(3\,2\,5\,4\,1)$

$= (3\,2\,5\,4\,1) = (5\,4\,1)(3\,2\,1)$

2005 What is the number of distinct cycles of length ≥ 1 in the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 7 & 6 & 3 & 4 & 1 \end{pmatrix}$?

(a) 2 (b) 3 (c) 4 (d) 5

Soln: $\sigma = \begin{pmatrix} 1 & 5 & 3 & 7 & 2 & 4 & 6 \\ 5 & 3 & 7 & 1 & 2 & 6 & 4 \end{pmatrix} = (1\,5\,3\,7)(2)(4\,6)$

Addition Modulo m:-

Let $a, b \in \mathbb{Z}$ and m be a fixed +ve integer. If the remainder r ($0 \le r < m$) when $a+b$ is divided by m, we define $a +_m b = r$.

Ex: (1) $20 +_6 5 = 1$.

Since $20+5 = 25$
$= 4(6)+1$

$\therefore$ 1 is the remainder when $20+5$ is divided by 6.

(2) $24 +_5 4 = 3$

(3) $2 +_7 3 = 5$

(4) $-32 +_4 5 = 1$ $\quad (\because -32+5 = -27 = (-7)(4)+1)$

(5) $-9 +_2 (-18) = 1$ $\quad (\because -9-18 = -27 = (-14)(2)+1)$

(6) $0 +_5 (-3) = 2$ $\quad (\because 0-3 = -3 = (-1)(5)+2)$

Note: $a +_m b = b +_m a$.

Congruences:-

Let $a, b \in \mathbb{Z}$ and m be any fixed +ve integer. If $a-b$ is divisible (devided) by m, we say that a is congruent to b modulo m and we write it as $a \equiv b \pmod m$.

The relation between integers a & b is called congruence modulo m.

i.e. $a \equiv b \pmod m \Leftrightarrow m \mid a-b$

(or) $m \mid b-a$ (or) $\frac{a-b}{m} = q$ (i.e. $a-b = mq$) for $q \in \mathbb{Z}$

and $a \not\equiv b \pmod m \Leftrightarrow m \nmid (a-b)$ or $a-b \neq km$ for $k \in \mathbb{Z}$.

Note:

[1]. If $a \equiv b \pmod m$ then we get the same remainder if a & b are separately divided by m.

Ex(1) If $22 \equiv 13 \pmod 3$

then 1 is the remainder when 22 & 13 are seperately divided by 3.

(2) If $-7 \equiv 17 \pmod 6$

then 5 is the remainder when -7 & 17 are seperately divided by 6.

[2]. $a +_m b \equiv a+b \pmod m$.

Ex: i) $9 +_4 5 = 2$ and $9+5 = 14$

Now $14 \equiv 2 \pmod 4$

ii) $12 +_4 7 = 3$ and $12+7 = 19$

Now $3 \equiv 19 \pmod 4$

→ If $a \equiv b \pmod m$, then $a +_m c = b +_m c$.

Sol^n: for $a \equiv b \pmod m \Rightarrow m \mid a-b$

$\Rightarrow m \mid (a+c)-(b+c)$ for $c \in \mathbb{Z}$

$\Rightarrow a+c \equiv b+c \pmod m$

$\Rightarrow a +_m c = b +_m c$.

Equivalence Classes (or) Equivalence sets

Let A be a non-empty set and let R be an equivalence relation in A.

$I_2 = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$

$I_3 = \{\ldots -7, -2, 3, 8, 13, \ldots\}$

$I_4 = \{\ldots -6, -1, 4, 9, 14, \ldots\}$

we observe that

(i) the sets I_0, I_1, I_2, I_3 & I_4 are non-empty.

(ii) the sets I_0, I_1, I_2, I_3 & I_4 are pair wise disjoint

(iii) $I = I_0 \cup I_1 \cup I_2 \cup I_3 \cup I_4$.

$\therefore \{I_0, I_1, I_2, I_3, I_4\}$ is a partition of I.

→ The operation congruence modulo 'm' is an equivalence relation in the set of integers. So the operation congruence modulo 'm' partitions $\mathbb{Z}$ into disjoint equivalence classes called residue classes or congruence modulo 'm'.

→ $\{0, 1, 2, 3, \ldots (m-1)\}$ is called the complete set of least positive residues modulo 'm' or simply set of residues modulo 'm'.

→ Let $m \in \mathbb{N}$ and $r \in \mathbb{Z}$. Let $\bar{r} = \{x / x \in \mathbb{Z}, x \equiv r \pmod m\}$

Then the set $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \ldots (\overline{m-1})\}$ is called the complete set of least +ve residue classes modulo 'm'. (or) simply set of residue classes modulo 'm'.

Addition of residue classes:

For $\bar{a}, \bar{b} \in \mathbb{Z}_m$, we define addition of residue classes, denoted by $+$, as $\bar{a} + \bar{b} = \overline{a+b}$

Note: [1] $+$ on the RHS is ordinary addition.

[2] if r is the remainder $(0 \le r < m)$ when

$a+b$ is divided by m then $\overline{a+b} = \overline{r}$

i.e, $\bar{a} +_5 \bar{b} = \bar{r}$

3. The set $G = \{0, 1, 2, \ldots, (m-1)\}$ of first m non-negative integers is an abelian group w.r.t addition modulo 'm'.

Problems:

→ P.T the set $G = \{0, 1, 2, 3, 4\}$ is an abelian group of order 5 w.r.t addition modulo 5.

Sol: Construct composition table

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Now we can easily prove all the axioms of abelian group.

$\therefore (G, +_5)$ is an abelian group.

→ P.T the set $G = \{0, 1, 2, 3, 4, 5\}$ is an abelian group w.r.t $+_6$:

Note: The set of residue classes modulo 'm' is abelian group of order 'm' w.r.t addition of residue classes

Multiplication modulo p:

If a and b are integers and p is a positive integers if ab is divided by p such that r is the remainder $(0 \le r < p)$, we define $a \times_p b = r$.

Further let 'a' be an arbitrary element of A. The elements $x \in A$ satisfying xRa constitute a subset A_a of A, called an equivalence class of 'a' w.r.t R. We shall denote the equivalence class by A_a or by $[a]$ or by $\bar{a}$.

i.e., A_a or $[a]$ or $\bar{a} = \{x / x \in A \text{ and } (x, a) \in R \text{ i.e. } xRa\}$

Ex: Let us determine the equivalence classes in the set I of all integers w.r.t the equivalence relation congruence modulo 5.

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

$x \in I$ is congruent to $0 \in I \pmod 5$ form an equivalence class I_0.

Here $x \equiv 0 \pmod 5$

$\Rightarrow 0 \equiv 0 \pmod 5$

$5 \equiv 0 \pmod 5$

$10 \equiv 0 \pmod 5$

$15 \equiv 0 \pmod 5$ etc.

$\therefore I_0 = \{\ldots\ldots -10, -5, 0, 5, 10, \ldots\ldots\}$

$= \{5k / k \in I\}$

$= 5I$.

The integers $(x \in I)$ congruent to 1 modulo 5 form another equivalence class I_1.

Here $x \equiv 1$ (modulo 5).

$\Rightarrow 1 \equiv 1 \pmod 5$, $6 \equiv 1 \pmod 5$, $11 \equiv 1 \pmod 5$

$16 \equiv 1 \pmod 5$ etc.

$\therefore I_1 = \{\ldots\ldots -9, -4, 1, 6, 11, 16, \ldots\ldots\}$

$= \{5k+1 / k \in I\}$

Similarly $I_2 = \{5k+2 / k \in I\}$

$= \{\ldots\ldots -8, -3, +2, 7, 12, \ldots\ldots\}$

$I_3 = \{ 5k+3 / k \in I \}$

$= \{ \cdots\cdots -7, -2, 3, 8, 13, \cdots\cdots \}$

and $I_4 = \{ 5k+4 / k \in I \}$

$= \{ \cdots\cdots -6, -1, 4, 9, 14, \cdots\cdots \}$

These classes have the following properties.

(i) The set I is the union of these five non-empty classes

(ii) Integers in each class have a relation of congruence modulo 5 with one another.

(iii) Integers in different classes donot have a relation of congruence modulo 5 with one another.

(iv) The classes are mutually disjoint.
i.e, no two of them have any elements in common.

Partition of a set:

Let S be a non-empty set. A set $P = \{A, B, C, \cdots\}$ of non-empty subsets of S will be called a partition of S if

(i) $A \cup B \cup C \cup \cdots\cdots = S$

(ii) the intersection of every pair of distinct subsets of $S \in P$ is the null set.
i.e, if $A, B \in P$ then $A \cap B = \phi$.

Ex: Let I be the set of all integers and $x \equiv y \pmod 5$ is an equivalence relation in I. Consider the set of five equivalence classes I_0, I_1, I_2, I_3 & I_4

where $I_0 = \{ \cdots\cdots -10, -5, 0, 5, 10, \cdots\cdots \}$

$I_1 = \{ \cdots\cdots -9, -4, 1, 6, 11, \cdots\cdots \}$

Ex: (1) $20 \times_6 5 = 4$

Since $20 \times 5 = 100$

$= 16(6) + 4$

i.e, 4 is the remainder when 20×5 is divided by

(2) $24 \times_5 4 = 1$

(3) $3 \times_7 -3 = 2$

(4) $(-32) \times_4 5 = 0$

Since $-32 \times 5 = -160$

$= (-40)(4) + 0$

(5) $0 \times_5 (-3) = 0$

$(\because 0 \times (-3) = 0$

$= 0(5) + 0)$

Note: 1) $a \times_p b \equiv ab \pmod p$

Ex: $7 \times_5 3 \equiv 21 \pmod 5$

$(\because 7 \times_5 3 = 1$ and $1 - 21 = (-4)5$

2) $a \times_m b = b \times_m a$

Ex: $3 \times_7 6 = 6 \times_7 3$

3) If $a \equiv b \pmod p$, then $a \times_p c = b \times_p c$

Ex: If $3 \equiv 23 \pmod 5$

then $3 \times_5 4 = 23 \times_5 4$

$(\because 3 \times_5 4 = 2$ & $23 \times_5 4 = 2)$

Prime Integer:

→ An integer p is said to be a prime integer if $p \neq 0$, $p \neq \pm 1$ and the only divisors of p are $\pm 1, \pm p$.

Ex: $\pm 2, \pm 3, \pm 5, \pm 7, \ldots$ are prime integers.

Note: 1. If p is a prime integer and $a, b \in I$ such that $p \mid ab$ then $p \mid a$ or $p \mid b$.

Multiplicative group of integers mod ab p ideas

P is prime:

The set $G = \{1, 2, 3, \ldots p-1\}$ where p is prime,

form a finite abelian group of order $p-1$ w.r.t multiplication modulo p.

Note: [1]. Suppose in the set G, p is not prime but p is composite.

Then $\exists$ two integers a and b such that $1 < a \leq p-1$, $1 < b \leq p-1$ and $ab = p$

$\therefore a \times_p b = 0$ and $0 \notin G$.

$\therefore G$ is not closed w.r.t composition multiplication modulo p.

$\therefore G$ is not group.

[2]. If we include 0 in the set G then for this composition G is not a group. (∵ inverse of 0 is not exist)

[3]. Multiplicative group of non-zero residue classes modulo a prime integer p:

→ The set of non-zero residue classes modulo a prime integer p forms an abelian group of order $(p-1)$ w.r.t multiplication of residue classes.

Problems:

→ P.T the set $G = \{1, 2, 3, 4, 5, 6\}$ is a finite abelian group order 6 w.r.t $\times_7$.

→ P.T $G = \{1, 2, 3, 4\}$ is abelian group of order 4 w.r.t $\times_5$.

→ P.T $G = \{1, 3, 5, 7\}$ is an abelian group of order 4 w.r.t $\times_8$.

→ Show that the set of integers $\{1, 5, 7, 11\}$ forms an abelian group w.r.t $\times_{12}$.

Law of Integral exponents:

Let $(G, \cdot)$ be a group. Let $a \in G$. Then by closure law $a, aa, aaa, \ldots$ are all elements of G.

Since the composition in G obeys general associative law. $a \cdot a \cdot a \cdots a$ (n times) is independent of the manner in which the elements are grouped.

For any integer 'n', we define a^n as follows:

(i) $a^0 = e$ is the identity element.

(ii) $a^1 = a$

(iii) for $n \geq 1$, $a^{n+1} = a^n \cdot a$

(iv) for $n > 0$, $a^{-n} = (a^{-1})^n$

Ex: $a^2 = a^1 \cdot a = a \cdot a$

$a^3 = a^2 \cdot a = (a \cdot a) a$ etc.

$a^{-4} = (a^{-1})^4 = (a^{-1})^3 (a^{-1})^1$

$= \left[(a^{-1})^2 (a^{-1})^1\right] a^{-1}$

$= \left[(a^{-1})^1 (a^{-1})^1\right] a^{-1} \cdot a^{-1}$

$= a^{-1} a^{-1} a^{-1} a^{-1}$ etc.

Note:

(i) $a^n = a \cdot a \cdots a$ (n times) and $a^n \in G$

(ii) $a^{-n} = (a^{-1})(a^{-1})(a^{-1}) \cdots (a^{-1})$ (n times). and $a^{-n} \in G$.

(iii) If additive operation $+$ is taken as the operation, then a^n in multiplication notation becomes na in additive notation.

Identity element $= 0$

and inverse of a is $-a$.

$na = a + a + \cdots + a$ (n times) and

$-na = (-a) + (-a) + \cdots + (-a)$ (n times)

when n is +ve integer.

Also $na \in G$ & $-na \in G$.

→ In a group $(G,\cdot)$, for $a \in G$, a is idempotent $\Leftrightarrow a = e$

Sol: $(G,\cdot)$ is a group.

Let $a \in G$, a is idempotent.

$\Leftrightarrow a \cdot a = a$

$\Leftrightarrow a \cdot a = ae$.

$\Leftrightarrow a = e$. (By LCL)

Note: If a is an element in a group $(G,\cdot)$ such that $a \cdot a = a$ then a is called an idempotent element.

→ If a, b are any two elements of a group $(G,\cdot)$ which commute. Show that (i) a^{-1} and b commute (ii) b^{-1} and a commute and (iii) a^{-1} and b^{-1} commute.

Sol^n: Given that $(G,\cdot)$ is a group such that

$ab = ba \quad \forall a, b \in G$ ... (1)

(i) we have

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

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

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

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

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

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

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

$\Rightarrow \boxed{ba^{-1} = a^{-1}b}$

$\therefore a^{-1}$ & b commute.

Similarly (ii) can be proved.

(iii) we have $ab = ba$

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

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

$\Rightarrow a^{-1}$ & b^{-1} commute.

→ In a group $(G,\cdot)$, for $a \in G$, a is idempotent $(?$
$\Leftrightarrow a = e$

Soln: $(G,\cdot)$ is a group.

Let $a \in G$, a is idempotent

$\Leftrightarrow a \cdot a = a$

$\Leftrightarrow a \cdot a = ae$.

$\Leftrightarrow a = e$. (By LCL)

Note: If a is an element in a group $(G,\cdot)$ such that $a \cdot a = a$ then a is called an idempotent element.

→ If a, b are any two elements of a group $(G,\cdot)$ which commute. Show that (i) $\bar{a}^1$ and b commute (ii) $\bar{b}^1$ and a commute and (iii) $\bar{a}^1$ and $\bar{b}^1$ commute.

Soln: Given that $(G,\cdot)$ is a group such that

$ab = ba \quad \forall a, b \in G$

(i) we have

$ab = ba \Rightarrow \bar{a}^1(ab) = \bar{a}^1(ba)$

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

$\Rightarrow eb = \bar{a}^1(ba)$

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

$\Rightarrow b\bar{a}^1 = [(\bar{a}^1 b) a]\bar{a}^1$

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

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

$\Rightarrow \boxed{b\bar{a}^1 = \bar{a}^1 b}$

$\therefore \bar{a}^1$ & b commute.

Similarly (ii) can be proved.

(iii) we have $ab = ba$

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

$\Rightarrow \bar{b}^1\bar{a}^1 = \bar{a}^1\bar{b}^1$

$\Rightarrow \bar{a}^1$ & $\bar{b}^1$ Commute.

$= a e \bar{a}^1$ (by (2))

$= a \bar{a}^1 = e$

Similarly $\bar{a}^{(k+1)} \cdot a^{k+1} = e$

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

$\therefore S(k+1)$ is true.

By Induction $S(n)$ is true for every +ve integer n.

Note: If $n \in N$, $(a^n)^{-1} = \bar{a}^n$ and $(\bar{a}^n)^{-1} = a^n$.

Let G be a group. Let $a, b \in G$ then

(i) $a^m a^n = a^{m+n}$ for $m, n \in N$

(ii) $(a^m)^n = a^{mn}$ for $m, n \in N$

(iii) $(ab)^n = a^n b^n$ when G is abelian and $n \in N$.

(iv) $e^n = e$ for $n \in N$

Soln: we prove the statements by using the principle of mathematical Induction.

(i) Let $S(n)$ be $a^m \cdot a^n = a^{m+n}$ for $m, n \in N$.

Put $n = 1$

$\therefore a^m \cdot a^1 = a^{m+1}$ (by defn)

$\therefore S(1)$ is true.

Let $S(k)$ be true.

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

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

$= (a^m \cdot a^k) a$

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

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

$\therefore S(k+1)$ is true.

$\therefore$ By Induction, $S(n)$ is true for $n \in N$.

Note: $a^m a^n = a^n a^m$.

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

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

→ Let G be a group and $a \in G$. If n is any +ve integer, then (i) $a \cdot a^n = a^n \cdot a$ and

(ii) $a^n, \bar{a}^n$ are inverse elements to one another.

Soln: We prove the statements by using mathematical induction.

(i) Let $S(n)$ be $a \cdot a^n = a^n \cdot a$ for $n \in \mathbb{Z}^+$

put $n=1$

$\therefore a a^1 = a \cdot a = a^1 \cdot a$

$\therefore S(1)$ is true.

Suppose for $n=k$ $S(k)$ is true.

$\therefore a a^k = a^k \cdot a$ —— (1)

Now $a a^{k+1} = a(a^k a)$

$= (a a^k) a$ (by asso.)

$= (a^k \cdot a) \cdot a$ (by (1))

$= a^{k+1} \cdot a$

$\therefore S(k+1)$ is true

$\therefore$ By induction $S(n)$ is true for every +ve integer 'n'.

(ii) Let $S(n)$ be that a^n and $\bar{a}^n$ are inverse to one another.

Let e be the identity element in G.

Since $a\bar{a}^1 = e = \bar{a}^1 a$.

$\Rightarrow a^1 \bar{a}^1 = e = \bar{a}^1 a^1$

$\Rightarrow S(1)$ is true.

Let $S(k)$ be true

$\therefore a^k \bar{a}^k = e = \bar{a}^k a^k$ —— (2)

Now $a^{k+1} \cdot \bar{a}^{(k+1)} = a^{k+1} (\bar{a}^1)^{k+1}$

$= a^k \cdot a (\bar{a}^1)^k \bar{a}^1$

$= a \cdot a^k \cdot \bar{a}^k \cdot \bar{a}^1$ (by (1))

$= a(a^k \bar{a}^k) \bar{a}^1$ (by asso.)

$\therefore S(k+1)$ is true

$\therefore$ By the induction $S(n)$ is true for $n \in N$

(iv) Let $S(n)$ be $e^n = e$ for $n \in N$

Put $n=1$, $\therefore e^1 = e$

$\therefore S(1)$ is true

Let $S(k)$ be true for some $k \in N$.

$\therefore e^k = e$ ——— (1)

Now $e^{k+1} = e^k e$

$= e \cdot e = e$.

$\therefore S(k+1)$ is true.

$\therefore$ By induction method $S(n)$ is true for $n \in N$.

Note: If G is an additive group, the above properties can be stated as

(i) $-(na) = (-n)a$ for $n \in Z$.

(ii) $ma + na = (m+n)a$

$= (n+m)a = na + ma$ for $m, n \in Z$

(iii) $n(ma) = (nm)a$

$= (mn)a = m(na)$ for $m, n \in Z$

(iv) $m(a+b) = ma + mb$ for $m \in Z$.

→ In a group G for every $a \in G$, $a^2 = e$. prove that G is an abelian group.

Soln: Let $(G, \cdot)$ be the given group.

$\forall a, b \in G \Rightarrow ab \in G$

since $a \in G$, $a^2 = e$

we have $(ab)^2 = e$

$\Rightarrow (ab)(ab) = e$

$\Rightarrow$ inverse of ab is ab.

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

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

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

(ii) Let $S(n)$ be

$(a^m)^n = a^{mn}$ for $m, n \in N$.

Put $n = 1$

$\therefore (a^m)^1 = a^m = a^{m \cdot 1}$ (by defn)

$\therefore S(1)$ is true.

Let $S(k)$ be true.

$\therefore (a^m)^k = a^{mk}$ —(1)

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

$= a^{mk} \cdot a^m$ (by (1))

$= a^{mk+m}$

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

$\therefore S(k+1)$ is true.

$\therefore$ By Induction, $S(n)$ is true for $n \in N$.

Note: $(a^m)^n = (a^n)^m$

Since $(a^m)^n = a^{mn} = (a^n)^m$ for $m, n \in N$.

(iii) Let $S(n)$ be

$(ab)^n = a^n b^n$ for $n \in N$

and G is abelian.

Put $n = 1$

$\therefore (ab)^1 = ab = a^1 b^1$

$\therefore S(1)$ is true.

Let $S(k)$ be true for some $k \in N$

$\therefore (ab)^k = a^k b^k$. —(1)

Now $(ab)^{k+1} = (ab)^k (ab)$

$= (a^k b^k)(ab)$ (by (1))

$= (a^k b^k)(ba)$ ($\because$ G is abelian i.e., $ab = ba$)

$= a^k (b^k b) a$

$= a^k (b^{k+1}) a$

$= a^k (b^{k+1} a)$

$= a^k (a \cdot b^{k+1})$

$= (a^k \cdot a) b^{k+1}$

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

since the number of elements in G is even (Given)

∴ there is atleast one more element of G which is its own inverse.

∴ In G, there is an element $a \neq e$ such that

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

→ If G is a group such that $(ab)^m = a^m b^m$ for three consecutive integers m for all $a, b \in G$, show that G is abelian.

Sol^n: Let $a, b \in G$

Let $m, m+1, m+2$ be three consecutive integers

By hypothesis, $(ab)^m = a^m b^m$ —①

$$(ab)^{m+1} = a^{m+1} b^{m+1} \text{ —②}$$

and $(ab)^{m+2} = a^{m+2} b^{m+2}$ —③

Now $(ab)^{m+2} = (ab)^{m+1}(ab)$ (by defn)

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

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

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

$\Rightarrow (ab)^{m+1} = (ab)^m ba$

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

$\Rightarrow ab = ba$

$\Rightarrow$ G is abelian

Order of an element of a group

Let $(G, \cdot)$ be a group, $a \in G$. Then the order of the element a is defined as the least +ve integer n such that $a^n = e$.

But $a^2 = e \Rightarrow aa = e$

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

Similarly $b^2 = e \Rightarrow b^{-1} = b$

(1) $\equiv ab = ba$

$\therefore G$ is abelian

→ Show that in a group G, $\forall a, b \in G$, $(ab)^2 = a^2b^2 \Leftrightarrow G$ is abelian.

Sol^n:

Part 1:

Let $(G, \cdot)$ be the given group.

$\forall a, b \in G$ and $(ab)^2 = a^2b^2$

To prove that G is abelian.

NOW $\forall a, b \in G$

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

$\Rightarrow (ab)(ab) = aabb$

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

$\Rightarrow ba = ab$ (By LCL & RCL)

$\Rightarrow G$ is abelian.

Let G be abelian.

To prove that $(ab)^2 = a^2b^2$

Now we have

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

$= a(ba)b$

$= a(ab)b$ ($\because G$ is abelian)

$= (aa)(bb)$

$= a^2b^2$

$\therefore (ab)^2 = a^2b^2$

→ If G is a group of even order, prove that it has an element $a \neq e$ satisfying $a^2 = e$.

Sol^n: In a group every element possesses its inverse and the identity element e is its own inverse.

since $3 \in G$ and $3^m \neq 1$ for any +ve integer m.

(5) $G = \{0, 1, 2, 3, 4, 5\}$ is a group w.r.t $+_6$

$1(0) = 0$ $\quad 1(1) = 1$

$0(0) = 1$ $\quad 2(1) = 2 = 1 +_6 1 = 2$

$3(1) = 3 = 1 +_6 1 +_6 1 = 3$

$4(1) = 4 = 1 +_6 1 +_6 1 +_6 1 = 4$

$5(1) = 5 = 1 +_6 1 +_6 1 +_6 1 +_6 1 = 5$

$6(1) = 6 = 1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 = 0$

$\therefore o(1) = 6$

Similarly we can easily see

$o(2) = 3$, $o(3) = 2$, $o(4) = 3$, $o(5) = 6$.

(6) $G = (I, +)$ is a group.

$1(0) = 0$

$\therefore o(0) = 1$

If $a (\neq 0) \in Z$ then there exists no +ve integer $n \in I^+$ such that $na = e$

$\therefore o(a) = \infty$ or 0.

Note: [1] The order of an identity element is 1

[2] If $a^m = e$ in group G where m is a +ve integer then the order of a is finite.

Also $o(a) \leq m$

Observe that, by definition $o(a) \neq m$.

→ The order of every element of a finite group is finite and is less than or equal to the order of the group.

Proof: Let $(G, \cdot)$ be the given finite group.

Let $a \in G$

— If there exist no +ve integer n such that $a^n = e$ then we say that a is of infinite order or zero order and the order of a is denoted by $o(a)$.

Note: If $(G, +)$ is a group then $na = e$ where n is the least +ve integer and $a \in G$

Examples:

(1) $G = \{1, -1, i, -i\}$ is a multiplicative group.

Now $1^1 = 1 = 1^2 = 1^3 = 1^4 = \cdots$

$\therefore o(1) = 1$

$(-1)^1 = -1$; $(-1)^2 = 1 = (-1)^4 = (-1)^6 = \cdots$

$\therefore o(-1) = 2$

$(i)^1 = i$; $(i)^2 = -1$, $(i)^3 = -i$, $(i)^4 = 1 = (i)^8 = (i)^{12} = \cdots$

$\therefore o(i) = 4$

and $(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$, $(-i)^4 = 1 = (-i)^8 = \cdots$

$\therefore o(-i) = 4$

(2) $G = \{1, \omega, \omega^2\}$.

$1^1 = 1$ $\quad \omega^1 = \omega$ $\quad (\omega^2)^1 = \omega^2$

$\therefore o(1) = 1$ $\quad \omega^2 = \omega^2$ $\quad (\omega^2)^2 = \omega$

$\omega^3 = 1$ $\quad (\omega^2)^3 = 1$

$\therefore o(\omega) = 3$ $\quad \therefore o(\omega^2) = 3$.

(3) $G = \{1, 3, 5, 7\}$ is a group w.r.t $\times_8$.

$1^1 = 1$ $\quad 3^1 = 3$ $\quad 5^1 = 5$ and $7^1 = 7$.

$o(1) = 1$ $\quad 3^2 = 3 \times_8 3 = 1$ $\quad 5^2 = 5 \times_8 5 = 1$ $\quad 7^2 = 7 \times_8 7 = 1$

$\therefore o(3) = 2$ $\quad \therefore o(5) = 2$ $\quad \therefore o(7) = 2$

(4) $G = (\mathbb{Z} - \{0\}, \cdot)$ is a group.

$1^1 = 1$ $\quad (-1)^1 = -1$

$o(1) = 1$ $\quad (-1)^2 = 1$

$o(-1) = 2$

The order of every other element of G is infinite.

→ In a group G, if $a \in G$ then $o(a) = o(a^{-1})$.

Proof: Let $o(a) = n$ & $o(a^{-1}) = m$

Since $o(a) = n \Rightarrow a^n = e$

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

$\Rightarrow a^{-n} = e$

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

$\Rightarrow o(a^{-1}) \leq n$

$\Rightarrow m \leq n$ ——— (1)

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

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

$\Rightarrow a^{-m} = e$

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

$\Rightarrow a^m = e$

$\Rightarrow o(a) \leq m$

$\Rightarrow n \leq m$ ——— (2)

from (1) & (2) we have $n = m$

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

→ The order of any +ve integral power of an element 'a' in a group G cannot exceed the order of an element 'a'.

i.e, $o(a^r) \leq o(a)$ for $a \in G$ and $r \in N$

Proof: Let $o(a^r) = m$ & $o(a) = n$

Since $o(a^r) = m$

i.e, m is the least +ve integer such that $(a^r)^m = e$

Since $o(a) = n$

i.e, n is the least +ve integer such that $a^n = e$

Now $o(a) = n \Rightarrow a^n = e$

$\Rightarrow (a^n)^r = e^r$; $r \in N$

$\Rightarrow (a^r)^n = e$

$\Rightarrow o(a^r) \leq n$

$\Rightarrow m \leq n$.

i.e, $o(a^r) \leq o(a)$

By Closure property

$a \cdot a = a^2 \in G$

$a \in G,\ a^2 \in G \Rightarrow a \cdot a^2 = a^3 \in G$ etc.

$\therefore a, a^2, a^3, \ldots \in G$

Since G is finite, all these elements cannot be different.

Let $a^r = a^s$ where $r, s \in N$ and $r > s$

Now $a^r a^{-s} = a^s a^{-s}$ $\quad (\because a^s \in G \Rightarrow a^{-s} \in G)$

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

$\Rightarrow a^{r-s} = a^0 = e$

$\Rightarrow a^m = e$ where $r - s = m > 0$ $\quad (\because r > s \Rightarrow r - s > 0)$

$\therefore \exists$ a +ve integer m such that $a^m = e$.

$\therefore$ Every collection of +ve integers has least element say 'n'.

$\therefore \exists$ a least +ve integer 'n' such that $a^n = e$

$\therefore o(a) = n$

$\therefore$ order of 'a' is finite.

Now to prove that $o(a) \leq o(G)$

If possible let $o(a) > o(G)$.

Let $o(a) = n$ i.e $a^n = e$

By closure property,

we have $a^1, a^2, a^3, \ldots a^n \in G$.

No two of these elements are equal.

If possible, let $a^r = a^s$, $1 \leq s < r \leq n$

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

Since $0 < r - s < n$

$\therefore a^{r-s} = e \Rightarrow o(a) \leq r - s < n \Rightarrow o(a) < n$ which is contradiction

$\therefore$ The n elements $a^1, a^2, \ldots a^n$ are distinct elements of G.

$\therefore o(a) > o(G)$ is wrong.

$\therefore o(a) \leq o(G)$

→ The order of ab is same as that of ba where a, b are elements of a group G.

proof: W.K.T $o(a) = o(b^{-1}ab)$

we have

$$o(ba) = o(b^{-1}(ba)b)$$

$$\Rightarrow o(ba) = o((b^{-1}b)ab)$$

$$= o(eab)$$

$$= o(ab)$$

$\therefore o(ba) = o(ab)$

$\therefore$ The orders of ab & ba are same.

→ If a is an element of order n (i.e $o(a) = n$) and p is prime to n then a^p is also of order n.

proof: Let $o(a^p) = m$.

i.e, m is the least +ve integer such that $(a^p)^m = e$

Since $o(a) = n$

i.e, n is the least +ve integer such that $a^n = e$

$$\Rightarrow (a^n)^p = e^p$$

$$\Rightarrow (a^p)^n = e$$

$$\Rightarrow o(a^p) \leq n$$

$$\Rightarrow m \leq n \quad \text{---} (1)$$

Since p is prime to n.

i.e, p, n are relatively prime.

$\therefore \exists$ two integers x & y such that

$$px + ny = 1$$

Now $a = a^1$

$$= a^{px+ny}$$

$$= a^{px} \cdot a^{ny}$$

$$= (a^p)^x (a^n)^y$$

$$= (a^p)^x e^y$$

$$= (a^p)^x e$$

$$a = (a^p)^x.$$

$\Rightarrow a = [(a^p)^m]^x$

$= [(a^p)^m]^x$

$= e^x$

$= e$

$\therefore o(a) \leq m$

$\Rightarrow n \leq m$ ——— (2)

from (1) & (2) we have $m = n$

i.e., $o(a^p) = o(a)$

→ In a group, if $ba = a^m b^n$, prove that the elements $a^m b^{n-2}$, $a^{m-2} b^n$, ab^{-1} have the same order.

Soln: we have

$a^m b^{n-2} = a^m b^n b^{-2}$

$= bab$ $(\because ba = a^m b^n)$

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

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

W.K.T $o(a) = o(b^{-1}ab)$ ——— (1)

where $a, b \in G$

$\therefore o(a^m b^{n-2}) = o((b^{-1})^{-1}(ab^{-1})b^{-1})$

$\therefore o(a^m b^{n-2}) = o(ab^{-1})$ ——— (2) (by (1))

Now we have

$a^{m-2} b^n = a^{-2} a^m b^n$

$= a^{-2} ba$

$= a^{-2} ba^{-1} a^2$

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

$\therefore o(a^{m-2} b^n) = o[(a^2)^{-1} (ba^{-1}) a^2]$

$= o(ba^{-1})$ (by (1))

$= o[(ba^{-1})^{-1}]$ $(\because o(a) = o(a^{-1}))$

$= o(ab^{-1})$ ——— (3)

from (2) & (3)

$o(a^m b^{n-2}) = o(ab^{-1}) = o(a^{m-2} b^n)$

→ If in the group G, $a^5 = e$, $aba^{-1} = b^2$ for $a, b \in G$ find $o(b)$

Sol^n: We have

$$(aba^{-1})^2 = (aba^{-1})aba^{-1}$$
$$= ab(a^{-1}a)ba^{-1}$$
$$= abeba^{-1}$$
$$= ab^2a^{-1}$$
$$= aababa^{-1}a^{-1} \quad (\because aba^{-1} = b^2)$$
$$= a^2ba^{-2}$$

Now $(aba^{-1})^4 = \{(aba^{-1})^2\}^2$
$$= (a^2ba^{-2})^2$$
$$= a^2ba^{-2} \cdot a^2ba^{-2}$$
$$= a^2b(a^{-2}a^2)ba^{-2}$$
$$= a^2beba^{-2}$$
$$= a^2b^2a^{-2}$$
$$= a^2aba^{-1}a^{-2}$$
$$= a^3ba^{-3}$$

Now $(aba^{-1})^8 = \{(aba^{-1})^4\}^2$
$$= (a^3ba^{-3})^2$$
$$= a^3ba^{-3} \cdot a^3ba^{-3}$$
$$= a^3b(a^{-3}a^3)ba^{-3}$$
$$= a^3b^2a^{-3}$$
$$= a^3aba^{-1}a^{-3}$$
$$= a^4ba^{-4}$$

Now $(aba^{-1})^{16} = \{(aba^{-1})^8\}^2$
$$= (a^4ba^{-4})^2$$
$$= a^4ba^{-4} \cdot a^4ba^{-4}$$
$$= a^4b(a^{-4}a^4)ba^{-4}$$
$$= a^4b^2a^{-4}$$
$$= a^4aba^{-1}a^{-4}$$
$$= a^5ba^{-5}$$

→ The orders of a & $b^{-1}ab$ are same, whose symbol

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

proof: Let $o(a) = m$ & $o(b^{-1}ab) = n$

Since $o(a) = m$

i.e, m is the least +ve integer such that $a^m = e$

Since $o(b^{-1}ab) = n$.

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

Now we have

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

$(b^{-1}ab)^2 = (b^{-1}ab)(b^{-1}ab)$

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

$= b^{-1}aeab$ (by inverse)

$= b^{-1}aab$ (by identity)

$= b^{-1}a^2b$

In general, we get

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

$= b^{-1}eb$ $(\because a^m = e)$

$= b^{-1}b$

$= e$

$\therefore o(b^{-1}ab) \leq m$

$\Rightarrow n \leq m$ —(1)

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

$e = b^{-1}a^nb$ $\left(\because (b^{-1}ab)^n = e\right)$

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

$\Rightarrow e = a^n$ (by LCL & RCL)

$\Rightarrow a^n = e$

$\Rightarrow o(a) \leq n$

$\Rightarrow m \leq n$ —(2).

from (1) & (2) we have

$o(a) \leq o(b^{-1}ab)$

(i) If n is the least +ve integer such that $a^n = e$

Let m be the +ve integer such that $a^m = e$

then we have to prove that n/m.

Since $a^m = e$

where m is the +ve integer such that

$o(a) \leq m$

$\Rightarrow n \leq m$

Case(i): If $n = m$ then n/m

Case(ii): If $n < m$ (i.e., $n \neq m$) then by division algorithm $\exists$ two integers q & r such that $m = nq + r$ where $0 \leq r < n$

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

$= a^{nq} a^r$

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

$= e^q \cdot a^r \quad (\because a^n = e)$

$= a^r$

$\therefore a^m = a^r$.

$\Rightarrow a^m = a^r$

$\Rightarrow a^r = e \quad (\because a^m = e)$

Since $0 \leq r < n$

$\therefore a^r = e$

$\Rightarrow r$ must be equal to '0'

because otherwise $o(a) \neq n$.

if $o(a) = n$ then $\exists$ no +ve integer $r < n$ such that $a^r = e$

$\therefore m = nq + 0$

$\Rightarrow m = nq$

$\Rightarrow \frac{m}{n} = q$

$\Rightarrow n/m$.

Conversely suppose that n/m then we prove that $a^m = e$.

$= ebe \quad (\because a^2 = e)$

$= be$

$= b$

$\therefore (ab\bar{a}^{-1})^{16} = b$

$\Rightarrow (b^2)^{16} = b \quad (\because ab\bar{a}^{-1} = b^2)$

$\Rightarrow b^{32} = b$

$\Rightarrow b^{32} = b$

$\Rightarrow b^{31} = e.$

Since $b^m = e \Rightarrow o(b) / m$ i.e $31/m$

$\therefore o(b) / 31$

But 31 is prime integer

$\therefore o(b) = 1$ or 31

if $b = e$ then $o(b) = 1$

if $b \neq e$ then $o(b) = 31$

Division algorithm: Let $a, b \in I$ with $b \neq 0$ then we can divide a by b to get a non negative remainder r which is smaller than b.

In other words if $a, b(\neq 0) \in I$ then there exists integers q, r such that $a = bq + r$ where $0 \leq r < |b|$

Ex: Let $-15, -9 \in I$

then $-15 = 2(-9) + 3$

Here $0 < 3 < |-9|$

→ If a is an element of a group G such that $o(a) = n$ then $a^m = e$ iff n/m (i.e, n is a divisor of m).

Proof: Given that a is an element of a group G such that $o(a) = n$.

$= a^{pn}(b^n)^p$

$= a^{pn} e$

$= a^{pn}$

$\therefore a^{pn} = e \quad (\because (ab)^{pn} = e)$

$\Rightarrow o(a) / pn$

i.e, m / pn.

Since $(m, n) = 1$

$\Rightarrow m / p$. ——— (2)

Similarly we can prove n/p ——— (3)

from (2) & (3) and $(m, n) = 1$

we have mn / p ——— (4)

$\therefore$ from (1) & (4)

we have $mn = p$

$\therefore o(ab) = p = mn$

$= o(a) \cdot o(b)$.

→ Given $a x a = b$ in G, find x.

Soln: we have $axa = b$

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

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

$\Rightarrow exa = \bar{a}^1 b$

$\Rightarrow xa\bar{a}^1 = \bar{a}^1 b\bar{a}^1$

$\Rightarrow xe = \bar{a}^1 b\bar{a}^1$

$\Rightarrow \boxed{x = \bar{a}^1 b \bar{a}^1}$

→ Find the solution of the equation $abxax = cbx$ in a group G, where $a, b, c \in G$

Soln: we have $abxax = cbx$

$\Rightarrow \bar{a}^1 abxax = \bar{a}^1 cbx$

$\Rightarrow bxax = \bar{a}^1 cbx$

$\Rightarrow xax = b^{-1}\bar{a}^1 cbx$

$\Rightarrow xa = b^{-1}\bar{a}^1 cb$

$\Rightarrow x = b^{-1}\bar{a}^1 cb\bar{a}^1$

Since n/m

i.e, n is divisor of m $\exists$ an integer q such that $m = nq$.

Now $a^m = a^{nq}$

$= (a^n)^q$

$= e^q$ $(\because a^n = e)$

$= e$

$\therefore a^m = e$

→ G is an abelian group. If $a, b \in G$ such that $o(a) = m$, $o(b) = n$ and $(m, n) = 1$ then $o(ab) = mn$

Proof: Given that G is an abelian group and $a, b \in G$ such that $o(a) = m$ & $o(b) = n$

Since $o(a) = m$;

i.e, m is the least +ve integer such that $a^m = e$.

and $o(b) = n$

i.e, n is the least +ve integer such that $a^n = e$

Also $a, b \in G \Rightarrow ab \in G$

Let $o(ab) = p$

Now $(ab)^{mn} = a^{mn} b^{mn}$ $(\because G$ is abelian$)$

$= (a^m)^n (b^n)^m$

$= e^n e^m$

$= e$

$\therefore (ab)^{mn} = e$

$\Rightarrow o(ab) / mn$

i.e, p / mn ——— (1)

Also $(ab)^{pn} = [(ab)^p]^n$

$= e^n$

$= e$

and $(ab)^{pn} = a^{pn} b^{pn}$

→ Prove that a group G is abelian if every element of G except the identity element is of order two.

Sol^n: W.K.T the order of an identity element 'e' is 1. i.e, $o(e)=1$

and given that the order of every element of the group G is 2 except the identity element.

$\therefore o(a)=2 \quad \forall a\in G \ \& \ a\neq e.$

$\Rightarrow a^2=e$

Let $a,b\in G \Rightarrow ab\in G$

$\therefore (ab)^2=e \ ; \ ab\neq e$

$\Rightarrow (ab)(ab)=e$

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

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

$\Rightarrow ba=ab \quad (\because a^2=e \Rightarrow aa=e \Rightarrow a^{-1}=a)$

$\therefore G$ is abelian

→ If every element of a group G is its own inverse, then G is abelian.

Sol^n: Let a & b be two elements of the group G

then $ab\in G$

Given that every element of G is its own inverse

$\therefore a^{-1}=a, \ b^{-1}=b \ \& \ (ab)^{-1}=ab.$

Now we have

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

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

$\Rightarrow ba=ab.$

$\therefore G$ is abelian.

Note [1] All groups of order 4 and less are commutative.

[2] If a group G is of order 4 and every element of G is its own inverse then it is known as Klein-4-group

→ If a and b are any elements of a group G, then $(bab^{-1})^n = ba^nb^{-1}$ for any integer n.

Sol^n: (i) $n=0$

we have $(bab^{-1})^0 = e$ (by defn)

Also $ba^0b^{-1} = beb^{-1}$

$= bb^{-1}$

$= e$

$\therefore (bab^{-1})^0 = ba^0b^{-1}$

(ii) $n>0$.

we have $(bab^{-1})^1 = bab^{-1}$

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

$\therefore$ The result is true for $n=1$

Let us suppose that the result is true for $n=k$

then $(bab^{-1})^k = ba^kb^{-1}$

Now $(bab^{-1})^{k+1} = (bab^{-1})^k (bab^{-1})$

$= (ba^kb^{-1})(bab^{-1})$

$= ba^kb^{-1}bab^{-1}$

$= ba^keab^{-1}$

$= ba^kab^{-1}$

$= ba^{k+1}b^{-1}$

$\therefore$ The result is true for $n=k+1$

$\therefore$ By the mathematical induction the result is true for $n>0$.

(iii) $n<0$

Let $n=-m$ where $m>0$

then $(bab^{-1})^n = (bab^{-1})^{-m}$

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

$= (ba^mb^{-1})^{-1}$

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

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

$= ba^nb^{-1}$

$\therefore$ each of $a_1, a_2, \ldots a_n$ is the inverse of exactly one of them.

So associate each of $a_1, a_2, \ldots a_n$ with its inverse.

$\Rightarrow (a_1 a_2 \cdots a_n)^2 = (a_1 a_1^{-1})(a_2 a_2^{-1}) \cdots (a_n a_n^{-1})$

$= ee \cdots$ upto n times

$= e$

→ The equation $x^2ax = a^{-1}$ is solvable for 'x' in a group G iff 'a' is the cube of some element in G.

Sol^n: Suppose $x^2ax = a^{-1}$ is solvable for 'x' in G

Then $\exists\, c \in G$ such that $c^2ac = a^{-1}$

Now $c^2ac = a^{-1}$

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

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

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

$\Rightarrow c(ca)(ca) = e$

$\Rightarrow (ca)(ca) = c^{-1}$

$\Rightarrow (ca)(ca)c = c^{-1}c$

$\Rightarrow (ca)(ca)(ca) = a$

$\Rightarrow a = (ca)^3$

$\therefore a$ is the cube of some element ca in G.

conversely suppose that $a = b^3$ for some $b \in G$

Let $x = b^{-2}$ be the solution of the equation $x^2ax = a^{-1}$.

for if $x = b^{-2}$ and $a = b^3$ then

$x^2ax = (b^{-2})^2 b^3 b^{-2}$

$= b^{-4} b^3 b^{-2}$

$= b^{-3}$

$= (b^3)^{-1}$

$= a^{-1}$ $(\because b^3 = a)$

$\therefore x = b^{-2}$ is a solution of $x^2ax = a^{-1}$

→ If a is an element of a group G such that $O(a) = n$ then the set $H = \{a^1, a^2, a^3, \ldots a^n = e\}$ forms a group w.r.t the composition in G.

Soln: Let $a \in G$ such that $O(a) = n$
$\Rightarrow a^n = e$
where n is the least +ve integer & e is the identity element in G.

(i) Let $a^p, a^q \in H$
$\Rightarrow a^p \cdot a^q = a^{p+q}$
$= a^r \in H$
when $p+q \equiv r \pmod n$ as $a^n = e$.
$\therefore$ Multiplication is closed in H.

(ii) Let $a^p, a^q, a^r \in H$
$\Rightarrow (a^p \cdot a^q)\, a^r = (a^{p+q})\, a^r$
$= a^{(p+q)+r}$
$= a^{p+(q+r)}$
$= a^p \cdot a^{q+r}$
$= a^p (a^q a^r)$
$\therefore x^n$ is asso. in H.

(iii) $\forall\, a \in H \;\exists\; a^n = e \in H$ such that $ae = ea = a$
$\therefore a^n = e = a^0$ is an identity element in H.

(iv) Let $a^p \in H$. $\exists\; a^{n-p} \in H$ such that
$a^p \cdot a^{n-p} = a^{n-p} a^p = a^n = e$.
$\therefore a^{n-p}$ is the inverse of a^p in H.
$\therefore$ every element of H is invertible.
$\therefore H = \{e = a^0, a^1, a^2, \ldots a^{n-1}\}$ is a group w.r.t composition in G.

→ If G is a finite abelian group with elements $a_1, a_2, \ldots a_n$, PT $a_1 a_2 a_3 \ldots a_n$ is an element whose square is the identity.

Soln: we have $(a_1 a_2 \ldots a_n)^2 = (a_1 a_2 \ldots a_n)(a_1 a_2 \ldots a_n)$
Now each element in the group is unique inverse.

from (3) & (4), we have

$$(xy)^2 = (yx)^3$$
$$= (yx)^2 \cdot (yx)$$
$$= (xy)^3 (yx)$$

$\therefore e = (xy)(yx)$ ($\because$ by cancelling $(xy)^2$ both sides)

$\Rightarrow e = xy^2x$

$\Rightarrow x^{-2} = y^2$ ——— (5)

Now $xy^2 = y^2x$

$\Rightarrow x(x^{-2}) = y(x^{-2})x$

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

$\Rightarrow \boxed{e = y}$

Again $yx^2 = x^3y$

$ex^2 = x^3$

$\Rightarrow \boxed{e = x}$

$\therefore x = y = e$.

(A) Let G be a group and let $a \in G$ be of finite order 'n' (i.e., $O(a) = n$). Then for any integer k we have $O(a^k) = \frac{n}{(n,k)}$ where (n,k) denotes the H.C.F of n and k.

Soln: Let $(n,k) = m$ then we have

$n = pm$, $k = qm$ for some integers p and q such that $(p,q) = 1$

Let $O(a^k) = l$

then $(a^k)^l = e$.

where l is the least +ve integer & e is the identity in G.

$\Rightarrow a^{kl} = e$.

$\Rightarrow O(a) \mid kl$.

→ If in a group G, $xy = yx$ and $yx = xy$ then $x = y = e$ where e is the identity element of G

Soln: we have $xy^2 = y^3x$

$\Rightarrow x(xy^2) = x(y^3x)$

$\Rightarrow x^2y^2 = xy^3x$

$\Rightarrow (x^2y^2)y^{-1} = xy^3xy^{-1}$

$\Rightarrow x^2y^2y^{-1} = xy^3xy^{-1}$

$\Rightarrow x^2y = xy^2yxy^{-1}$

$\Rightarrow x^2y = y^3xyxy^{-1}$ $(\because xy^2 = y^3x)$ ——— (1)

Again $yx^2 = x^3y$

$\Rightarrow yx^2 = x \cdot x^2y$

$= x(y^3xyxy^{-1})$ (by (1))

$\therefore yx^2 = xy^3xyxy^{-1}$

$\Rightarrow x^2 = y^{-1}xy^3xyxy^{-1}$

$\Rightarrow x^2y = y^{-1}xy^3xyx$ ——— (2)

from (1) & (2) we have

$y^3xyxy^{-1} = y^{-1}xy^3xyx$.

$\Rightarrow y^4xyxy^{-1} = xy^3xyx$

$\Rightarrow y^4xyx = xy^3xyxy$

$= xy^2yxyxy$

$= y^3xyxyxy$ $(\because xy^2 = y^3x)$

$\Rightarrow yxyx = xyxyxy$ (∵ by cancellation laws)

$(yx)^2 = (xy)^3$ ——— (3)

Since the given relations $x^2y = y^3x$ & $y^2x = x^3y$ are symmetrical in x & y.

∴ Interchanging x & y in (3) we get $(xy)^2 = (yx)^3$ ——— (4)

$\Rightarrow n/kl \quad (\because o(a) = n)$

$\Rightarrow pm/qml$

$\Rightarrow p/q l \cdot \left(i.e., \frac{ql}{p}\right)$

$\Rightarrow p/l$ ——— (1) ($\because$ p and q are relatively prime)

Again $(a^k)^p = (a^{qm})^p$

$= a^{qmp}$

$= a^{qn}$

$= (a^n)^q$

$= e^q$

$= e$

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

$\Rightarrow o(a^k)/p$

$\Rightarrow l/p$ ——— (2)

From (1) & (2) we have

$l = p.$

$\Rightarrow o(a^k) = p$

$= \frac{n}{m} \quad (\because n = pm)$

$= \frac{n}{(n,k)}$

Subgroups

Complex:

Any non-empty subset of a group G is called complex of G.

Ex: (1) The set of integers is a complex of a group $(\mathbb{R}, +)$.

(2) I_E is a complex of the group $(\mathbb{Z}, +)$

(3) I_O is a complex of the group $(\mathbb{R}, +)$

Multiplication of two complexes:

If M and N are any two complexes of a group G then $MN = \{mn \in G / m \in M, n \in N\}$.

Clearly $MN \subseteq G$ and MN is called the product of the complexes M, N of G.

→ The multiplication of complexes of a group G is associative.

Soln: Let M, N, P be any three complexes in a group G.

Let $m \in M, n \in N, p \in P \Rightarrow m, n, p \in G$

We have $MN = \{mn \in G / m \in M, n \in N\}$

$\therefore (MN)P = \{(mn)p \in G / m \in M, n \in N, p \in P\}$

$= \{m(np) \in G / m \in M, n \in N, p \in P\}$

$= M(NP)$.

Defn: If M is a complex in a group G then we define $M^{-1} = \{m^{-1} \in G / m \in M\}$.

i.e., M^{-1} is the set of all inverses of the elements of M. Clearly $M^{-1} \subseteq G$.

→ If M, N are any two complexes in a group G then $(MN)^{-1} = N^{-1}M^{-1}$.

Soln: we have

$$MN = \{mn \in G / m \in M, n \in N\}$$

$$\text{Now } (MN)^{-1} = \{(mn)^{-1} \in G / m \in M, n \in N\}$$

$$= \{n^{-1}m^{-1} \in G / m \in M, n \in N\}$$

$$= N^{-1}M^{-1}.$$

Subgroups:-

Let G be a group and H be a non-empty subset of G. Then H is called a subgroup of G if H is a group w.r.t the b-o defined in G.

Ex: (1) $G = (I, +)$

$H_1 = (2I, +)$ & $H_2 = (3I, +)$

$\therefore H_1$ & H_2 are subgroups of G.

(2) $G = (\mathbb{R}, +)$

$H_1 = (\mathbb{Q}, +)$, $H_2 = (I, +)$.

$\therefore H_1$ & H_2 are subgroups of G.

(3) $G = (\mathbb{R} - \{0\}, \cdot)$

$H_1 = (\mathbb{Q} - \{0\}, \cdot)$, $H_2 = (\{1, -1\}, \cdot)$,

$H_3 = (\{1\}, \cdot)$, $H_4 = (\{2^n / n \in I\}, \cdot)$

$H_5 = (\mathbb{Q}^+, \cdot)$, $H_6 = (\mathbb{R}^+, \cdot)$ & $H_7 = (\{3^n / n \in I\}, \cdot)$.

$\therefore H_1, H_2, H_3, H_4, H_5, H_6$ & H_7 are subgroups of G.

(4) $= (\{0, 1, 2, 3, 4, 5\}, +_6)$.

$H_1 = (\{0\}, +_6)$, $H_2 = (\{0,3\}, +_6)$, $H_3 = (\{0,2,4\}, +_6)$

$\therefore H_1, H_2$ & H_3 are subgroups of G.

(5) $G = (\mathbb{Z}, +)$

$H_1 = \{3^n, n \in N\}$. is not a subgroup of G.

Note: Every subgroup of G is complex of G but every complex is not always a subgroup.

Defn: For any group G, $G \subseteq G$ & $\{e\} \subseteq G$.

therefore G & $\{e\}$ are subgroups of G.

These two are called trivial or improper subgroups of G.

Other than these two are called proper or non-trivial subgroups of G.

Note:

1. The identity of a subgroup H is the same as that of the group.
2. The inverse of any element of a subgroup is the same as the inverse of that element regarded as an element of the group.
3. The order of every element of a subgroup is the same as the order of element regarded as a member of the group.

Theorem: If H is any subgroup of a group G then $H^{-1} = H$.

Proof: Let $h^{-1} \in H^{-1}$ by definition of H^{-1}, $h \in H$.

Since H is a subgroup of G.

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

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

$\therefore H^{-1} \subseteq H$ —— (1)

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

$\Rightarrow (h^{-1})^{-1} \in H^{-1}$ (by defn)

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

$\therefore H \subseteq H^{-1}$ —— (2)

from (1) & (2) we have

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

Note: The converse of the above need not be true i.e, if $H^{-1} = H$ then H need not be a subgroup of G.

Eg: $H = \{-1\}$ is a complex of multiplicative group $G = \{1, -1\}$

Since inverse of -1 is -1.

$\therefore H^{-1} = \{-1\}$.

But $H = \{-1\}$ is not a group under multiplication. ($\because (-1)(-1) = 1 \notin H$ closure is not true)

$\therefore H$ is not a subgroup of G.

→ If H is any subgroup of G then $HH = H$.

Proof: Let $x \in HH$

but $x = h_1 h_2$ where $h_1 \in H$ & $h_2 \in H$.

Since H is a subgroup of G.

$h_1 h_2 \in H$

$\Rightarrow x \in H$

$\Rightarrow HH \subseteq H$ —— (1)

Let $h_3 \in H$ and e be the identity element in H.

$\therefore h_3 = h_3 e \in HH$.

$\Rightarrow h_3 \in HH$

$\Rightarrow H \subseteq HH$ —— (2)

from (1) & (2) we have $HH = H$.

→ G is a group and $H \subseteq G$; H is a subgroup of G iff (i) $a, b \in H \Rightarrow ab \in H$ (ii) $a \in H \Rightarrow a^{-1} \in H$.

Proof: Let H be a subgroup of G.

∴ By defn H is a group w.r.t the b-o defined in G.

By Closure axiom (i) $a, b \in H \Rightarrow ab \in H$

by inverse axiom (ii) $a \in H \Rightarrow a^{-1} \in H$

Conversely suppose that $H \subseteq G$ and

(i) $a, b \in H \Rightarrow ab \in H$;

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

To prove that H is a subgroup of G.

(1) Since $a, b \in H \subseteq G \Rightarrow ab \in H$ by (i)

∴ H is closed.

(2) Let $a, b, c \in H \subseteq G \Rightarrow (ab)c = a(bc)$ (by asso. prop in G)

∴ Asso-prop in H is satisfied.

(3) $\forall a \in H \subseteq G \Rightarrow a^{-1} \in H \subseteq G$ (by (ii))

∴ $a \in H, a^{-1} \in H \Rightarrow a a^{-1} \in H \subseteq G$ (by (i))

$\Rightarrow e \in H$ (by inverse axiom of G)

∴ $\exists\, e \in H$ such that $ea = ae = a$ $\forall a \in H$ (by identity of G)

∴ Identity axiom in H is satisfied.

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

∴ Each element of H possesses inverse in H

∴ H itself is a group for the composition in G.

∴ H is a subgroup of G.

Hence the theorem.

Note: If the operation in G is $+$, then the conditions in the above theorem can be stated as follows:

(i) $a, b \in H \Rightarrow a + b \in H$. (ii) $a \in H \Rightarrow -a \in H$

Theorem → G is a group and H is a non-empty subset of G (i.e, $H \subseteq G$). H is a subgroup of G iff

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

Proof

N.C:

Let H be a subgroup of G.

Then by definition H is a group of G w.r.t b-o defined in G.

By inverse axiom $b \in H \Rightarrow b^{-1} \in H$

By closure axiom $a \in H, b^{-1} \in H \Rightarrow a b^{-1} \in H$.

S.C: Given that $a \in H, b \in H \Rightarrow a b^{-1} \in H$

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

Existence of identity:

$a \in H, a \in H \Rightarrow a a^{-1} \in H \subseteq G$ (by hyp)

$\Rightarrow e \in H$ (by inverse axiom of G)

$\therefore \exists e \in H$ such that $ae = ea = a \quad \forall a \in H$

$\therefore$ Identity prop. is satisfied

and 'e' is the identity element in H.

Existence of inverse:

$a = e \in H, b = a \in H \Rightarrow e a^{-1} \in H \subseteq G$ (by hyp)

$\Rightarrow a^{-1} \in H$ (by identity in G)

$\therefore \exists a^{-1} \in H$ such that $a a^{-1} = a^{-1} a = e$.

$\therefore$ Inverse axiom is satisfied and

a^{-1} is the inverse of a in H.

Closure prop:

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

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

$\Rightarrow ab \in H \quad (\because (b^{-1})^{-1} = b)$

Closure axiom in H is satisfied.

Asso. prop:

Let $a, b, c \in H \subseteq G$

then $(ab)c = a(bc)$ (By asso. prop in G)

$\therefore$ Asso. prop in H is satisfied.

$\therefore$ H itself is a group for the composition in G.

$\therefore$ H is a subgroup of G.

Note: If the operation in G is + then condition in the above theorem can be stated as follows:

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

Theorem: A necessary and sufficient condition for a non-empty subset H of a group G to be a subgroup of G is that $HH^{-1} \subseteq H$

proof:

N.C:

Let H be a subgroup of G

TO P.T $HH^{-1} \subseteq H$

Let $ab^{-1} \in HH^{-1}$ (by defn)

then $a \in H, b \in H$

Since H is a group

$\forall a \in H, b \in H$

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

$\Rightarrow ab^{-1} \in H$ (by closure axiom)

$\therefore HH^{-1} \subseteq H$.

S.C:

Let $HH^{-1} \subseteq H$

Let $a, b \in H \Rightarrow ab^{-1} \in HH^{-1}$ (by defn)

Since $HH^{-1} \subseteq H$

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

$\therefore$ H is a subgroup of G.

Theorem: A N.C and S.C for a non-empty subset H of a group G to be a subgroup of G is that $HH^{-1} = H$.

Proof: N.C: Let H be a subgroup of G.

Then we have $HH^{-1} \subseteq H$ —— ①

Let e be the identity element in G

$\therefore e \in H$

Let $h \in H$

$\therefore h = he$

$= he^{-1} \in HH^{-1}$

$\therefore H \subseteq HH^{-1}$ —— ②

$\therefore$ from ① & ② we have $HH^{-1} = H$

S.C: Let $HH^{-1} = H$

$\Rightarrow HH^{-1} \subseteq H$

$\therefore H$ is a subgroup of G.

Theorem: G is a group and H is a finite subset of G (i.e., $H \subseteq G$).

H is a subgroup of G iff $a, b \in H \Rightarrow ab \in H$

Proof: N.C

Let H be a subgroup of G

then by defn H is a group w.r.t $\circ$ defined in G.

$\therefore$ By closure axiom $a, b \in H \Rightarrow ab \in H$.

S.C: Given that $a, b \in H \subseteq G \Rightarrow ab \in H \subseteq G$

we have to prove H is a subgroup of G.

(i) Since $a, b \in H \Rightarrow ab \in H$ (by hyp)

$\therefore H$ is closed

(ii) Let $a, b, c \in H \subseteq G$

$(ab)c = a(bc)$ (By asso. prop of G)

$\therefore$ Asso prop. is satisfied in H.

(iii) $a \in H,\ a \in H \Rightarrow aa \in H$ (by hyp)

$\Rightarrow a^2 \in H$

$a \in H,\ a^2 \in H \Rightarrow aa^2 \in H$

$\Rightarrow a^3 \in H$

proceeding in this way

we get, $a^n \in H$ where 'n' is +ve integer

$\therefore a, a^2, a^3, \ldots\ldots a^n, \ldots\ldots \in H$ and they are all infinite in number

But H is finite subset of G.

Therefore there must be repetition in this collection of elements.

if they are all distinct then H will not be a finite set.

Let $a^r = a^s$ for some r & s are +ve integers where $r > s$

$\Rightarrow a^r \cdot \bar{a}^s = a^s \cdot \bar{a}^s$ ($\because a^s \in G \Rightarrow \bar{a}^s \in G$)

$\Rightarrow a^{r-s} = a^0$

$\Rightarrow a^{r-s} = e$ where e is the identity element of G

Since $r-s$ is +ve integer

$\therefore a^{r-s} \in H$

$\Rightarrow e \in H$

$\therefore e = a^0 \in H$

$\therefore \exists\ e \in H$ such that $ae = ea = a\ \ \forall a \in H$

$\therefore$ e is the identity.

(iv) NOW $r > s \Rightarrow r - s \geq 1$

$\Rightarrow r - s - 1 \geq 0$

$\therefore a^{r-s-1} \in H$.

NOW we have

$a \cdot a^{r-s-1} = a^{r-s} = e = a^{r-s} \cdot \bar{a}$.

$\therefore$ Inverse of a is a^{r-s-1} in H.

$\therefore$ H itself is a group.

$\therefore$ H is a subgroup of G.

Theorem →

If H & K are two subgroups of a group G then HK is a subgroup of G iff HK = KH.

proof: Let H & K be any two subgroups of G.

1st part:

Let HK = KH

then we have to prove that HK is a subgroup of G.

For this we are enough to prove that

$$(HK)(HK)^{-1} = HK.$$

Now we have

$$(HK)(HK)^{-1} = HK(K^{-1}H^{-1})$$
$$= H(KK^{-1})H^{-1} \quad (\because \text{complex multiplication is also.})$$
$$= H(K)H^{-1}$$
$$= (HK)H^{-1}$$
$$= (KH)H^{-1} \quad (\text{by hyp})$$
$$= K(HH^{-1})$$
$$= KH \quad (\because H \text{ is a subgroup of } G \Rightarrow HH^{-1} = H)$$
$$= HK \quad (\text{by hyp})$$

$\therefore$ HK is a subgroup of G.

2nd part:

Let HK be a subgroup of G.

$\therefore (HK)^{-1} = HK$

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

$\Rightarrow KH = HK \quad (\because H \text{ & } K \text{ are subgroups} \therefore H^{-1} = H \text{ & } K^{-1} = K)$

Theorem:

The intersection of two subgroups is also a subgroup.

proof: Let H_1 & H_2 be two subgroups of G.

To prove that $H_1 \cap H_2$ is a subgroup of G.

Let $H = H_1 \cap H_2$.

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

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

Since H_1 & H_2 are subgroups of G.

$\therefore ab^{-1} \in H_1$ and $ab^{-1} \in H_2$

$\Rightarrow ab^{-1} \in H_1 \cap H_2$

$\therefore H_1 \cap H_2$ is a subgroup of G.

Theorem Intersection of an arbitrary family of subgroups of a group is a subgroup of the group.

Proof Let $H_1, H_2, H_3 \ldots\ldots$ be arbitrary family of subgroups of G.

To prove that $H_1 \cap H_2 \cap H_3 \cap \ldots\ldots$ is a subgroup of G.

Let $H = H_1 \cap H_2 \cap \ldots\ldots$

$= \bigcap_{i \in N} H_i$.

Let $a, b \in H$

$\Rightarrow a, b \in \bigcap_{i \in N} H_i$

$\Rightarrow a, b \in H_i \quad \forall i \in N$

$\Rightarrow ab^{-1} \in H_i \quad \forall i \in N \quad (\because H_i$ is a subgroup of $G)$

$\Rightarrow ab^{-1} \in \bigcap_{i \in N} H_i$

$\therefore \bigcap_{i \in N} H_i$ is a subgroup of G.

→ The union of two subgroups of a group need not be a subgroup of the group.

Soln: for example

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

is a group w.r.t $+$.

Let $H_1 = \{2n / n \in I\}$

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

and $H_2 = \{3n / n \in I\}$

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

are two subgroups of G w.r.t $+^n$.

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

$2, 3 \in H_1 \cup H_2$

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

$H_1 \cup H_2$ is not closed.

$\therefore H_1 \cup H_2$ is not a group.

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

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

proof: Let H_1 & H_2 be two subgroups of G.

Let $H_1 \subset H_2$ or $H_2 \subset H_1$.

To P.T $H_1 \cup H_2$ is a subgroup of G.

Since $H_1 \subset H_2 \Rightarrow H_1 \cup H_2 = H_2$ is a subgroup.

Since $H_2 \subset H_1 \Rightarrow H_2 \cup H_1 = H_1$ is a subgroup

$\therefore H_1 \cup H_2$ is a subgroup.

Conversely Suppose that $H_1 \cup H_2$ is a subgroup

To P.T $H_1 \subset H_2$ or $H_2 \subset H_1$

If possible suppose that $H_1 \not\subset H_2$ or $H_2 \not\subset H_1$

Since $H_1 \not\subset H_2 \Rightarrow \exists\ a \in H_1$ and $a \notin H_2$ — ①

Again $H_2 \not\subset H_1 \Rightarrow \exists\ b \in H_2$ and $b \notin H_1$ — ②

From ① & ② we have

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

$\Rightarrow a+b \in H_1 \cup H_2$

Since $H_1 \cup H_2$ is a subgroup of G.

$\therefore ab \in H_1 \cup H_2$

$\Rightarrow ab \in H_1$ or $ab \in H_2$

Let $ab \in H_1$.

let $a \in H_1 \Rightarrow a^{-1} \in H_1$ ($\because H_1$ is subgroup)

$\therefore a^{-1} \in H_1$, $ab \in H_1$

$\Rightarrow a^{-1}(ab) \in H_1$ (by closure axiom of H

$\Rightarrow (a^{-1}a)b \in H_1$ (by asso.)

$\Rightarrow eb \in H_1$ (by inverse)

$\Rightarrow b \in H_1$ (by identity)

which is contradiction to $b \notin H_1$

Let $ab \in H_2$

let $b \in H_2 \Rightarrow b^{-1} \in H_2$

$\therefore b^{-1} \in H_2$, $ab \in H_2$

$(ab)b^{-1} \in H_2$ by closure

$a(bb^{-1}) \in H_2$

$ae \in H_2$

$\Rightarrow a \in H_2$

which is contradiction to $a \notin H_2$

$\therefore$ our assumption that $H_1 \not\subset H_2$ or $H_2 \not\subset H_1$ is wrong.

$\therefore$ either $H_1 \subset H_2$ or $H_2 \subset H_1$

Problems

→ Let G be the additive group of integers. Then prove that the set of all multiples of integers by fixed integer 'm' is a subgroup of G.

Sol^n: Let $G = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ be the additive group of integers.

Let m be the fixed integer

Let $H = \{\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\}$

$= \{3m / m \in I\} \subseteq G$

Let $a, b \in H$ Choosing $a = rm$, $b = sm$ where $r, s \in I$.

The inverse of sm in H is $(-s)m$

i.e, $b = (-s)m$.

Now we have

$a - b = rm + (-s)m$

$= (r-s)m$

$\in H$ $(\because r, s \in I \Rightarrow r-s \in I)$

$\therefore$ H is a subgroup of G.

→ Let 'a' be an element of a group G. The set $H = \{a^n : n \in I\}$ of all integral powers of 'a' is a subgroup of G.

Sol^n: Let $a \in G$

To P.T $H = \{a^n / n \in I\}$

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

is a subgroup of G.

Let $a = a^r$, $b = a^s \in H$; $r, s \in I$

The inverse of a^s in H is a^{-s}.

Now we have

$ab^{-1} = a^r (a^s)^{-1}$

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

$= a^{r-s} \in H$. $(\because r, s \in I \Rightarrow r-s \in I)$

$\therefore$ H is a subgroup of G

Note: If G is a group and $a \in G$ then the subgroup $H = \{a^n / n \in I\}$ of G is called the subgroup of G generated by 'a'.

Ex: Let G be the multiplicative group of the rational numbers.

we have $3 \in G$

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

is a subgroup of G.

Let G be the set of all ordered pairs (a,b) of real numbers for which $a \neq 0$

i.e., $G = \{(a,b) / a \neq 0, b \in \mathbb{R}\}$

Let a binary operation $*$ on G be defined by the formula

$$(a,b) * (c,d) = (ac, bc+d)$$

Show that $(G, *)$ is not an abelian group.

Does the subset H of all these elements of G which are of the form $(1,b)$ form a subgroup of G?

Sol^n: Let $G = \{(a,b) / a \neq 0, b \in \mathbb{R}\}$ and the binary operation $*$ on G is defined by the formula

$$(a,b) * (c,d) = (ac, bc+d)$$

(i) Closure prop:

Let $x, y \in G$ Choosing $x = (a,b)$, $y = (c,d)$ where $a, b, c, d \in \mathbb{R}$ & $a \neq 0$, $c \neq 0$.

Now $x * y = (a,b) * (c,d)$

$= (ac, bc+d) \in G$ ($\because ac \neq 0$, $bc+d \in \mathbb{R}$)

$\therefore$ closure prop is satisfied.

(ii) Asso. prop:

Let $(a,b), (c,d), (e,f) \in G$; where $a, b, c, d, e, f \in \mathbb{R}$. & $a \neq 0$, $c \neq 0$, $e \neq 0$.

Now we have

$$[(a,b)\times(c,d)]\times(e,f) = (ab, bc+d)\times(e,f) \quad \text{(by hyp.)}$$
$$= (abe, (bc+d)e+f)$$
$$= (abe, bce+de+f)$$

and similarly we can easily find

$$(a,b)\times[(c,d)\times(e,f)] = (abe, bce+de+f)$$

$\therefore$ LHS = RHS.

$\therefore$ Asso. prop. is satisfied.

(iii) Existence of left Identity:

Let $(a,b)\in G$ $\quad \exists\ (c,d)\in G$
$a\neq 0, b\in\mathbb{R}$ $\quad c\neq 0, d\in\mathbb{R}$

such that $(c,d)\times(a,b) = (a,b)$

$\Rightarrow (ca, da+b) = (a,b)$

$\Rightarrow ca = a$, & $da+b = b$

$\Rightarrow c = 1$ & $da = 0 \Rightarrow d = 0$ $(\because a\neq 0)$

$\therefore (c,d) = (1,0)\in G$.

$\therefore \forall (a,b)\in G$, $a\neq 0, b\in\mathbb{R}$, $\exists\ (1,0)\in G$ such that $(1,0)\times(a,b) = (a,b)$

$\therefore (1,0)$ is an identity element in G.

(iv) Existence left inverse:

Let $(a,b)\in G$ $\quad \exists\ (c,d)\in G$ $\quad c\neq 0, d\in\mathbb{R}$
$a\neq 0, b\in\mathbb{R}$

such that $(c,d)\times(a,b) = (1,0)$

$\Rightarrow (ca, da+b) = (1,0)$

$\Rightarrow ca = 1$, $da+b = 0$

$\Rightarrow c = \frac{1}{a}$, $d = \frac{-b}{a}$ $(\because a\neq 0)$

$\therefore (c,d) = \left(\frac{1}{a}, \frac{-b}{a}\right)\in G$ $a\neq 0, b\in\mathbb{R}$

such that $\left(\frac{1}{a}, \frac{-b}{a}\right)\times(a,b) = (1,0)$

$\therefore \left(\frac{1}{a}, \frac{-b}{a}\right)$ is the inverse of (a,b).

$\therefore (G,\times)$ is a group.

(v) Comm. prop:

$\forall (a,b), (c,d) \in G$
$a, b, c, d \in \mathbb{R}$ & $a \neq 0, c \neq 0$

$\therefore (a,b) \times (c,d) = (ac, bc+d)$

& $(c,d) \times (a,b) = (ca, da+b)$

$\therefore (a,b) \times (c,d) \neq (c,d) \times (a,b)$

$\therefore$ Comm. prop. is not satisfied.

$\therefore (G, \times)$ is not comm. group.

Now let
$H = \{ (1,b) / b \in \mathbb{R} \} \subset G$

Let $x, y \in H$ Choosing $x = (1,b)$ & $y = (1,c)$
where $b, c \in \mathbb{R}$.

The inverse of $y = (1,c)$ in G is

$y^{-1} = \left(\frac{1}{1}, -\frac{c}{1}\right)$
$= (1, -c)$

Now we have

$x \times y^{-1} = (1,b) \times (1,c)^{-1}$
$= (1,b) \times (1,-c)$
$= (1 \cdot 1,\ b \cdot 1 + (-c))$
$= (1, b-c) \in H$
$\because (\because b, c \in \mathbb{R} \Rightarrow b-c \in \mathbb{R})$

$\therefore H$ is a subgroup of G.

→ Show that $H = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} / a \neq 0;\ a, b \in \mathbb{R} \right\}$ is subgroup of the multiplicative group of 2×2 non-singular matrices over $\mathbb{R}$.

Sol^n: Let $X = \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} \in H$, $Y = \begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix} \in H$
where $a_1 \neq 0, b_1$; $a_2 \neq 0, b \in \mathbb{R}$

The inverse of Y in H is Y^{-1}

Now $Y^{-1} = \frac{adj.Y}{|Y|} = \frac{1}{a_2}\begin{pmatrix} 1 & -b_2 \\ 0 & a_2 \end{pmatrix}$

$$= \begin{pmatrix} \frac{1}{a_2} & -\frac{b_2}{a_2} \\ 0 & 1 \end{pmatrix}$$

and $XY^{-1} = \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix}^{-1}$

$$= \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \frac{1}{a_2} & -\frac{b_2}{a_2} \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} \frac{a_1}{a_2} & -\frac{a_1 b_2}{a_2} + b_1 \\ 0 & 1 \end{pmatrix} \quad \left(\because \frac{a_1}{a_2} \neq 0,\ -\frac{a_1 b_2}{a_2} + b_1 \in R\right)$$

$\therefore H$ is a subgroup of G.

If G is a group and $N(a) = \{x \in G : xa = ax\}$ for $a \in G$ then p.t. $N(a)$ is a subgroup of G.

Sol": Since $ea = ae$.

$\therefore e \in N(a)$

$\therefore N(a)$ is non-empty set.

i.e., $N(a) \neq \emptyset$.

Let $x, y \in N(a)$ then $xa = ax$ & $ya = ay$.

Now we shall show that $y^{-1} \in N(a)$.

we have $ya = ay$

$\Rightarrow (ya)^{-1} = (ay)^{-1}$

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

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

$\Rightarrow (aa^{-1})y^{-1} = (ay^{-1})a^{-1}$ (by assoc. in G)

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

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

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

$\Rightarrow y^{-1}a = (ay^{-1})e$

$\Rightarrow y^{-1}a = ay^{-1}$.

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

Now we shall show that $xy^{-1} \in N(a)$ ... (1)

Since $y^{-1}a = ay^{-1}$

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

$\Rightarrow (xy^{-1})a = (xa)y^{-1}$

$= (ax)y^{-1}$ $(\because xa = ax)$

$= a(xy^{-1})$ (by also $xy^{-1} \in G$)

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

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

$\therefore N(a)$ is a subgroup of G.

Normalizer of an element of a group:

If 'a' is an element of a group G then the normalizer on 'a' in G is the set of all those elements of G which commute with a. The normalizer of 'a' in G is denoted by $N(a)$.

Where $N(a) = \{x \in G / xa = ax\}$

Note: The Normalizer $N(a)$ is a subgroup of G.

Self-conjugate element of a group:

$(G, \cdot)$ is a group and $a \in G$ such that $a = x^{-1}ax \ \forall x \in G$. Then 'a' is called self conjugate element of G.

A self conjugate element is some times called an invariant element.

Here $a = x^{-1}ax$

$\Rightarrow xa = ax \ \forall x \in G$

The centre of a group:

The set Z of all self-conjugate elements of a group G is called the centre of the group G.

i.e, $Z = \{z \in G / zx = xz \ \forall x \in G\}$.

Note: If G is abelian group then centre of G is G

→ G is a group then $Z = \{z \in G / zx = xz \ \forall x \in G\}$ is a subgroup of G.

Soln Since $ex = xe \ \forall x \in G$

$\therefore e \in Z$

$\therefore Z \neq \phi$

Let $a, b \in Z$

then $ax = xa$ & $bx = xb \ \forall x \in G$

We shall show that $b^{-1} \in Z$

Now we have

$bx = xb \ \forall x \in G$

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

$\Rightarrow (b^{-1}b)x = (b^{-1}x)b$ (by asso.)

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

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

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

$\Rightarrow xb^{-1} = b^{-1}x \ \forall x \in G$.

$\therefore b^{-1} \in Z$.

Now we shall show that $ab^{-1} \in Z$.

Now we have $xb^{-1} = b^{-1}x \ \forall x \in G$

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

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

$\Rightarrow (xa)b^{-1} = (ab^{-1})x$ ($\because ax = xa$).

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

$ab^{-1} \in Z$.

$\therefore Z$ a subgroup of G.

→ Show that $aHa^{-1} = \{aha^{-1} / h \in H\}$ is a subgroup of G. where H is subgroup of G and $a \in G$.

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

then $x = ah_1a^{-1}$ & $y = ah_2a^{-1}$ for some $h_1, h_2 \in H$.

Now we shall show that $y^{-1} \in aHa^{-1}$:

we have $y^{-1} = (ah_2a^{-1})^{-1}$

$= (a^{-1})^{-1} h_2^{-1} a^{-1}$ $(\because (ab)^{-1} = b^{-1}a^{-1})$

$= a h_2^{-1} a^{-1} \in aHa^{-1}$

$(\because H$ is a subgroup of G, $\therefore h_2 \in H \Rightarrow h_2^{-1} \in H)$.

Now we shall show that $xy^{-1} \in aHa^{-1}$:

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

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

$= ah_1(e)h_2^{-1}a^{-1}$ $(\because aa^{-1} = e$ in $G)$

$= a(h_1h_2^{-1})a^{-1} \in aHa^{-1}$ $(\because H$ is a subgroup of G, $h_1 \in H, h_2 \in H \Rightarrow h_1 \in H, h_2^{-1} \in H \Rightarrow h_1h_2^{-1} \in H)$

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

$\therefore a^{-1}Ha^{-1}$ is a subgroup of G.

Hw → Show that $a^{-1}Ha = \{a^{-1}ha / a \in H\}$ is a subgroup of G, where H is subgroup of G and $a \in G$.

→ If a be a fixed element of a group G and if $H = \{x \in G / xa^2 = a^2x\}$, $K = \{x \in G / xa = ax\}$ then show that $H < G$ & $K < H$.

(i.e., H is a subgroup of G & K is a subgroup of H).

Sol^n: Let a be a fixed element of a group G.

and $H = \{x \in G / xa^2 = a^2x\}$.

Let $x, y \in H$ then $xa^2 = a^2x$ & $ya^2 = a^2y$.

Now we shall show that $y^{-1} \in H$.

Now we have $ya^2 = a^2y$

$\Rightarrow y^{-1}(ya^2) = y^{-1}(a^2y)$

$\Rightarrow (y^{-1}y)a^2 = (y^{-1}a^2)y$ (by assoc.)

$\Rightarrow ea^2 = (y^{-1}a^2)y$.

$\Rightarrow a^2 = (y^{-1}a^2)y$

$\Rightarrow a^2y^{-1} = (y^{-1}a^2)yy^{-1}$

$\Rightarrow a^2y^{-1} = (y^{-1}a^2)e$

$\Rightarrow a^2y^{-1} = y^{-1}a^2$

$\Rightarrow y^{-1}a^2 = a^2y^{-1}$

$\therefore y^{-1} \in H$.

Now we shall show that $xy^{-1} \in H$

Now we have $a^2y^{-1} = y^{-1}a^2$

$\Rightarrow x(a^2y^{-1}) = x(y^{-1}a^2)$

$\Rightarrow (xa^2)y^{-1} = (xy^{-1})a^2$

$\Rightarrow (a^2x)y^{-1} = (xy^{-1})a^2 \quad (\because a^2x = xa^2)$

$\Rightarrow a^2(xy^{-1}) = (xy^{-1})a^2$

$\therefore xy^{-1} \in H$.

$\therefore H$ is a subgroup of G.

Let $K = \{x \in G / xa = ax\}$.

Now we shall show that $K \subseteq H$

Let $x \in K$

$xa = ax$.

$\Rightarrow (xa)a = (ax)a$

$\Rightarrow x(aa) = a(xa)$

$\Rightarrow xa^2 = a(ax) \quad (\because ax = xa)$

$\Rightarrow xa^2 = (aa)x$

$\Rightarrow xa^2 = a^2x$.

$\therefore x \in H$.

$\therefore K \subseteq H$.

Now we shall show that K is a subgroup of H.

Since $ea = ae$

$\therefore e \in K$

$\therefore K \neq \phi$.

Let $x, y \in K$ then $xa = ax$ & $yx = ay$.

we have $ya = ay \Rightarrow y^{-1}(ya) = y^{-1}(ay)$

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

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

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

$\Rightarrow ay^{-1} = (y^{-1}a)yy^{-1}$

$\Rightarrow ay^{-1} = y^{-1}a$

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

$\Rightarrow (xa)y^{-1} = (xy^{-1})a$

$\Rightarrow (ax)y^{-1} = (xy^{-1})a$ $(\because ax = xa)$

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

$\therefore xy^{-1} \in K$.

$\therefore K$ is a subgroup of H.

→ Let H be a subgroup of a group G and let $T = \{x \in G / xH = Hx\}$ Show that T is a subgroup of G.

Soln: Given that H is a subgroup of G.

Let $T = \{x \in G / xH = Hx\}$

Let $x, y \in T$. Then $xH = Hx$ & $yH = Hy$

Now we have $yH = Hy \Rightarrow y^{-1}(yH) = y^{-1}(Hy)$

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

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

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

$\Rightarrow Hy^{-1} = (y^{-1}H)yy^{-1}$

$\Rightarrow Hy^{-1} = (y^{-1}H)e$

$\Rightarrow Hy^{-1} = y^{-1}H$

$\Rightarrow x(Hy^{-1}) = x(y^{-1}H)$

$\Rightarrow (xH)y^{-1} = (xy^{-1})H$

$\Rightarrow (Hx)y^{-1} = (xy^{-1})H \quad (\because Hx = xH)$

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

$\Rightarrow xy^{-1} \in T$

$\therefore T$ is a subgroup of G.

→ Let P_n be the symmetric group of degree 'n'. i.e, the elements of P_n are permutations of degree 'n'. If A_n is the set of all even permutations of degree 'n', then $A_n \subseteq P_n$. and A_n is closed w.r.t multiplication of permutations. Therefore A_n is a subgroup of P_n.

→ A group can never be expressed as the union of two of its proper subgroups.

Ex: $G = \{\pm 1, \pm i, \pm j, \pm k\}$ is a multiplicative group of order 8.

$(\because i^2 = j^2 = k^2 = -1$

$ij = -ji = k, \; jk = -kj = i$

$ki = -ik = j)$

then $H_1 = \{\pm 1, \pm i\}$ & $H_2 = \{\pm 1, \pm j\}$ are two proper subgroups of G.

and $G \neq H_1 \cup H_2$.

→ Let G_1 be the multiplicative group of all +ve real numbers and $\mathbb{R}$ be the additive group of all real numbers. Is G a subgroup of $\mathbb{R}$?

Ans:- $G \subseteq \mathbb{R}$ but G_1 is not a subgroup of $\mathbb{R}$.

→ (i) Can an abelian group have a non-abelian subgroup ?

(ii) Can a non-abelian group have an abelian subgroup ?

(iii) Can a non-abelian group have a non-abelian subgroup ?

Ans (i) Every subgroup of an abelian group is abelian i.e, if G is an abelian group and H is a subgroup of G. then the operation on H is commutative because it is already commutative in G and H is a subset of G.

∴ An abelian group cannot have a non-abelian subgroup.

(ii) A non-abelian group can have an abelian subgroup

for example: the symmetric group P_3 of permutations of degree 3 and order 3! (i.e, 6) is non-abelian while its subgroup A_3 is abelian.

(iii) A non-abelian group can have a non-abelian subgroup.

Example:. P_4 is a non-abelian group and its subgroup A_4 is also non-abelian

Cosets:

→ Let $(H, \cdot)$ be a subgroup of the group $(G, \cdot)$ Let $a \in G$. Then the set $aH = \{ah / h \in H\}$ is called a left coset of H in G generated by 'a' and the set $Ha = \{ha / h \in H\}$ is called a right coset of H in G generated by a.

Also aH, Ha are called cosets of H generated by a in G.

Since every element of aH or Ha is in G.

$\therefore aH$ & Ha are subsets of G.

→ If e is the identity element in G.

then $eH = \{eh / h \in H\}$

$= \{h / h \in H\}$

$= H$

Similarly $He = H$.

∴ the subgroup of G is itself a left and a right coset of H in G.

→ If e is the identity element in G, it is the identity element in H.

$\because a \in G, e \in H \Rightarrow ea \in Ha$ & $ae \in aH$.

$\Rightarrow a \in Ha$ & $a \in aH$.

Hence the left coset or the right coset of H generated by 'a' is non-empty.

Further $a \in Ha$, $a \in aH$ and $Ha \cap aH \neq \phi$.

→ If the group G is abelian then every $h \in H$ we have $ha = ah$.

Hence $Ha = aH$.

i.e., right coset = left coset.

Even if G is not abelian we may have

$aH = Ha$ or $aH \neq Ha$.

Note:

If the operation in G is denoted by additively, then the left coset of H in G generated by a, denoted by $a+H$ is $\{a+h / h \in H\}$

i.e., $a+H = \{a+h / h \in H\}$

Similarly the right coset of H in G generated by a, denoted by $H+a$ is $\{h+a / h \in H\}$.

i.e., $H+a = \{h+a / h \in H\}$.

Ex: Let $G = \{1, -1, i, -i\}$ and $H = \{1, -1\}$

then $H(-1) = \{-1, 1\} \subseteq G$

$H(1) = \{1, -1\} \subseteq G$

$H(i) = \{i, -i\} \subseteq G$; and $H(-i) = \{-1, i\} \subseteq G$

Note: Left and right cosets need not be a subgroup of G.

Ex: Let G be the additive group of integers.

Now $G = \{\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$ and 0 is identity element in G.

Also G is abelian.

Let H be a subset of G where elements of H are obtained by multiplying each element of G by 3.

i.e., $H = \{\ldots -9, -6, -3, 0, 3, 6, 9, \ldots\}$

Clearly H is a subgroup of $(G, +)$.

Since G is abelian.

$\therefore$ left coset of H of an element in G = right coset of H in G.

$\therefore 0+H = H = \{\ldots -9, -6, -3, 0, 3, 6, \ldots\}$

Since $1 \in G$, $1+H = \{\ldots -8, -5, -2, 1, 4, 7, \ldots\}$

Since $2 \in G$, $2+H = \{\ldots -7, -4, -1, 2, 5, 8, \ldots\}$

observe that (i) $3+H = 6+H = \ldots = 0+H$

$4+H = 7+H = \ldots = 1+H$

$5+H = 8+H = \ldots = 2+H$.

(ii) $0+H, 1+H, 2+H$ are disjoint (iii) $(0+H) \cup (1+H) \cup (2+H) = G$.

Properties of cosets:

→ If H is a subgroup of G and $a \in H$ then show that $aH = H$ and $Ha = H$.

proof: Given that

H is a subgroup of G and $a \in H$

To prove that $aH = H$.

By hyp. $aH \subseteq G$

Let $h \in H \Rightarrow ah \in aH$

Since H is a subgroup of G.

$a \in H, h \in H \Rightarrow ah \in H$ (by closure axiom)

$\therefore aH \subseteq H$ —①

Let $h \in H$

Now $h = eh$

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

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

Since H is a subgroup of G.

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

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

$\therefore h = ah_1 \in aH$

$\Rightarrow h \in aH$

$\therefore H \subseteq aH$ —②

From ① & ② we have $aH = H$

Similarly $Ha = H$.

→ If H is a subgroup of G and $a, b \in G$ then $aH = bH \Leftrightarrow a^{-1}b \in H$ and $Ha = Hb \Leftrightarrow ab^{-1} \in H$

proof Given that H is a subgroup of G & $a, b \in G$ and $aH = bH$.

To prove that $a^{-1}b \in H$

Since $aH = bH$

Let $b \in bH$ then $b \in aH$

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

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

$\Rightarrow a^{-1}b \in eH$

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

Now $a^{-1}b \in H \Rightarrow a^{-1}bH = H$ $(\because e \in H \Rightarrow eH = H)$

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

$\Rightarrow (aa^{-1})(bH) = aH$

$\Rightarrow e(bH) = aH$

$\Rightarrow bH = aH$.

$\Rightarrow aH = bH$.

Now we have $Ha = Hb$.

Let $a \in Ha \Rightarrow a \in Hb$

$\Rightarrow ab^{-1} \in (Hb)b^{-1}$

$\Rightarrow ab^{-1} \in H(e)$

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

Now we have $ab^{-1} \in H$

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

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

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

$\Rightarrow Ha = Hb$.

→ If a, b are any two elements of a group G and H any subgroup of G. then $a \in bH \Leftrightarrow aH = bH$ and $a \in Hb \Leftrightarrow Ha = Hb$.

Proof $a \in bH \Rightarrow b^{-1}a \in b^{-1}(bH)$

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

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

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

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

$\Rightarrow (bb^{-1})aH = bH$

$\Rightarrow e(aH) = bH$

$aH = Hb$

Conversely Let $aH = bH$

$\Rightarrow a \in aH$

$\Rightarrow a \in bH$.

Similarly we can prove that $a \in Hb \Leftrightarrow Ha = Hb$.

Proof: Given that H is a subgroup of G.

To prove that G = the union of all left cosets of H in G.

Let H, aH, bH, cH, ... be all left cosets of H in G where $a, b, c, \ldots \in G$.

$\therefore H \cup aH \cup bH \cup \ldots \subseteq G$,

$\Rightarrow \bigcup_{a \in G} aH \subseteq G$ ——— (1)

W.K.T $a \in G \Rightarrow a \in aH$

$\Rightarrow a \in \bigcup_{a \in G} aH$

$\Rightarrow G \subseteq \bigcup_{a \in G} aH$ ——— (2)

from (1) & (2) we have $G = \bigcup_{a \in G} aH$.

Similarly G is equal to the union of all right cosets of H in G.

Right coset Decomposition of a group:

- Suppose H is a subgroup of a group G. No right coset of H in G is empty.
- Any two right cosets of H in G are either disjoint or identical.
- The union of all right cosets of H in G is equal to G. Therefore set of all right cosets of H in G gives us a partition of G.
- This partition is called the right coset decomposition of G w.r.t the subgroup H.

→ If H is a subgroup of G, there is a one-to-one correspondence b/w any two left cosets of H in G.

Proof: Given that H is a subgroup of G.

Let aH & bH be two left cosets of H in G. for $a, b \in G$.

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

proof: Let H be a subgroup of G.

Let aH & bH be two left cosets of H in G.

Two cases arise:

(i) When aH & bH have no common element.

$\therefore aH$ & bH are disjoint.

$\therefore aH \cap bH = \phi$.

(ii) When aH & bH have common element.

$\therefore aH$ & bH are not disjoint

Hence $aH \cap bH \neq \phi$.

Let 'c' be the common element of aH & bH

$\therefore c \in aH \cap bH$

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

Let $c = ah_1$, $h_1 \in H$ & $c = bh_2$, $h_2 \in H$.

$\therefore ah_1 = bh_2$.

$\Rightarrow b^{-1}(ah_1) = b^{-1}(bh_2)$ (pre multiply by b^{-1})

$\Rightarrow (b^{-1}a)h_1 = (b^{-1}b)h_2$

$\Rightarrow (b^{-1}a)h_1 = h_2$ $(\because b^{-1}b = e)$.

$\Rightarrow (b^{-1}a)h_1H = h_2H$. $(\because k \in H \Rightarrow kH = H)$

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

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

$\Rightarrow (bb^{-1})aH = bH$.

$\Rightarrow aH = bH$.

$\therefore$ If $aH \cap bH \neq \phi$ then $aH = bH$

Similarly we can prove

If $Ha \cap Hb \neq \phi$ then $Ha = Hb$.

→ If H is a subgroup of G then G is equal to the union of all left (right) cosets of H in G.

we have to prove that there is one-to-one correspondence b/w two left cosets aH & bH.

Define a function

$f: aH \to bH$ such that

$f(ah) = bh$ for $h \in H$.

To show f is 1-1:

for $h_1, h_2 \in H$, $ah_1, ah_2 \in aH$ and $bh_1, bh_2 \in bH$

Now $f(ah_1) = f(ah_2)$

$\Rightarrow bh_1 = bh_2$

$\Rightarrow h_1 = h_2$

$\Rightarrow ah_1 = ah_2$

$\therefore f$ is 1-1

To show f is onto:

$bh \in bH \Rightarrow \exists\ h \in H$ such that $bh \in bH$

$\Rightarrow \exists\ h \in H$ such that $ah \in aH$

For $ah \in aH$, $f(ah) = bh$

$\therefore f$ is onto.

$\therefore f$ is 1-1 & onto.

$\therefore$ there exists one-to-one correspondence between aH & bH.

Similarly there exists one-to-one correspondence between any two right cosets of H in G.

→ If H is a subgroup of a group G, then there is one to one correspondence between the set of all distinct left cosets of H in G and the set of all distinct right cosets of H in G.

Proof: In G, let G_1 = the set of all left cosets

and G_2 = the set of all right cosets.

Define a function $f: G_1 \to G_2$ such that

$f(aH) = Ha^{-1}$ $\forall a \in G$.

for let $aH, bH \in G_1$.

Now we have $aH = bH \Rightarrow b^{-1}a \in H$

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

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

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

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

$\therefore$ f is well defined.

To prove f is 1-1:

Let $aH, bH \in G_1$

$\therefore f(aH) = f(bH)$

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

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

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

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

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

$\Rightarrow aH = bH$

$\therefore$ f is 1-1

To show f is onto:

Let $Ha \in G_2$.

Since $a \in G$, $a^{-1} \in G$

$\therefore a^{-1}H \in G_1$ and $f(a^{-1}H) = H(a^{-1})^{-1}$
$= Ha$.

$\therefore$ f is onto.

$\therefore$ There is one to one correspondence between G_1 and G_2.

Note [1]. If H is a subgroup of a finite group G then the number of distinct left cosets of H in G is the same as the number of distinct right cosets of H in G.

[2]. Since H is common to both the set of left cosets of H of a finite group G and the set of right cosets of H of the finite group G, the number of elements in a left coset of H is equal to the number of elements in a right coset of H.

Congruence modulo H:

Let $(G, \cdot)$ be a group and $(H, \cdot)$ be a subgroup of G.

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

we say that $a \equiv b \pmod{H}$

Theorem In the group G, the relation $a \equiv b \pmod{H}$ is an equivalence relation.

Proof: (i) Reflexive:

Let e be the identity element in $(G, \cdot)$

Since H is a subgroup of G.

$\therefore e$ is the identity element in H.

Let $a \in G$

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

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

$\therefore a \equiv a \pmod{H}$.

(ii) - Symmetric:

Let $a \equiv b \pmod{H}$

for $a, b \in G$

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

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

$\Rightarrow b \equiv a \pmod{H}$.

(iii) Transitive:

Let $a \equiv b \pmod{H}$ and $b \equiv c \pmod{H}$

for $a, b, c \in G$

$\therefore b^{-1}a \in H$ and $c^{-1}b \in H$

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

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

$\Rightarrow c^{-1}ea \in H$

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

$\Rightarrow a \equiv c \pmod{H}$

$\therefore$ The congruence modulo H is reflexive, symmetric and transitive.

$\therefore$ it is an equivalence relation.

→ Let $(H,\cdot)$ be a subgroup of a group $(G,\cdot)$.
for $a \in G$, let the equivalence class $\bar{a} = \{x \in G / x \equiv a \pmod H\}$.
Then $\bar{a} = aH$.

proof: To prove $\bar{a} = aH$.
Let e be the identity element in G.
$\therefore e$ is also the identity in H.

let $x \in \bar{a} \Leftrightarrow x \equiv a \pmod H$
for $x, a \in G$
$\Leftrightarrow \bar{a}^{-1}x \in H$
$\Leftrightarrow \bar{a}^{-1}x = h \in H$ for some $h \in H$.
$\Leftrightarrow a(\bar{a}^{-1}x) = ah \in aH$
for some $h \in H$.
$\Leftrightarrow (a\bar{a}^{-1})x = ah \in aH$
for some $h \in H$
$\Leftrightarrow ex = ah \in aH$
for some $h \in H$.
$\Leftrightarrow x \in aH$
$\therefore \bar{a} = aH$.

Index of a subgroup of a finite group:

→ If H is a subgroup of a finite group G, then the number of distinct left (right) cosets of H in G is called the index of H in G and is denoted by $[G:H]$ or $i_G(H)$.

Ex: $G = \{-1, 1, i, -i\}$
$H = \{-1, 1\} \subseteq G$
$-1.H = \{1, -1\} = H$
$1.H = \{-1, 1\} = H$ and $i.H = \{-i, i\}$
& $-i.H = \{-i, i\}$
$i.H = -i.H$ & $1.H = -1.H$.
∴ The number of distinct left cosets of H in G is 2.
$\therefore [G:H] = 2$

Lagrange's theorem:

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

(or)

If G is a finite group and H is a subgroup of G then order of H is divisor of order of the group G. i.e, $o(H)/o(G)$.

proof: Since H is a subgroup of a finite group G

$\therefore H$ is finite.

Two cases arise:

(1) If $H = G$ then $o(H)/o(G)$

(2) If $H \neq G$.

Let $o(G) = n$ & $o(H) = m$

W.K.T every right coset of H in G has the same number of elements. and the number of right cosets of H in G is finite. (∵ G is finite)

Also since $H = He$

H is the right coset of H in G.

If $Ha, Hb, Hc, \ldots$ are right cosets of H in G then $o(Ha) = o(Hb) = \ldots\ldots = o(H) = m$

Let the number distinct right cosets of H in G be k.

All these right cosets are disjoint and induce a partition of G.

$\therefore o(G) = o(Ha) + o(Hb) + \ldots\ldots + o(H)$ (k times)

$= m + m + \ldots\ldots + m$ (k times)

$= mk$

$\therefore n = mk$

$\Rightarrow k = \frac{n}{m}$.

$\therefore o(H)$ divides $o(G)$.

Note: [1]. Lagrange's theorem can also be proved by taking left cosets of H in G.

[2]. Lagrange's theorem deals with finite groups only.

[3]. Since $K = \frac{n}{m}$,

the number of distinct left (right) cosets of H in G = $\frac{\text{Order of the group } G}{\text{Order of the subgroup } H \text{ of } G}$

$= \frac{O(G)}{O(H)}$

[4]. Converse of Lagrange's theorem doesn't always hold. i.e, if m is divisor of 'n' it is not necessary that G must be have a subgroup of order m.

Ex: $G = \{1, -1, i, -i\}$ is a multiplicative group of order 4.

Since 2 is divisor of 4 (order of G)

Let us examine whether a subset H (of order 2) of G which is a subgroup of G exists.

Consider $H_1 = \{1, -i\} \subseteq G$ is not a subgroup of G.

($\because i(-i) = 1 \notin H_1$).

Consider $H_2 = \{1, -1\} \subseteq G$

Clearly H_2 is a subgroup of G.

∴ In conclusion,

even if 'm' is a divisor of 'n' a subgroup of order m in G need not exist.

If G is a finite group and $a \in G$ then the order of 'a' divides O(G).

proof: Let G be a finite group.

$\forall\ a \in G$, $o(a)$ must exist ($\because$ In a finite group, order of every element exist).

Let $o(a) = m$

To prove $m \mid o(G)$

i.e., $o(a) \mid o(G)$

Since $o(a) = m$

$\therefore$ m is the least +ve integer such that

$a^m = e$ — (1)

Let $H = \{a^1, a^2, a^3, \ldots\ldots a^{m-1}, a^m = e\}$

$= \{e, a, a^2, \ldots\ldots, a^{m-1}\} \subseteq G$

This must turn out to be a subgroup of G.

Here H is finite ($\because$ G is finite)

To prove: H is closed.

$\forall\ a^i, a^j \in H$ where $0 \le i, j \le m$

Now, $a^i \cdot a^j = a^{i+j}$

$= a^{mq+r}$ ($\because i+j = mq+r$ where $0 \le r < m$)

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

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

$= e^q \cdot a^r$ ($\because a^m = e$)

$= a^r \in H$ ($\because 0 \le r < m$)

$\therefore a^i \cdot a^j \in H$

$\therefore H$ is closed.

$\therefore H$ is a subgroup of G ($\because H$ is finite subgroup of $G \Rightarrow ab \in H\ \forall a, b \in H$)

Also $o(H) = m$,

To prove: All the elements of H are distinct.

If possible let $a^i = a^j$ where $0 \le j < i < m$

$\Rightarrow a^i a^{-j} = a^j a^{-j}$ ($\because a^j \in G$, $a^{-j} \in G$)

$\Rightarrow a^{i-j} = a^0$

$= e$ where $0 < i-j < m$.

This contradicts (1)

$\therefore o(H) = m$

By Lagrange's theorem $o(H) / o(G)$

$\Rightarrow m / o(G)$

$\Rightarrow o(a) / o(G)$

→ If G is a finite group and $a \in G$ then $a^{o(G)} = e$.

proof: Given that G is a finite group and let $o(G) = n$

$\forall a \in G$, $o(a)$ must exist ($\because$ G is finite)

Let $o(a) = m$

then m is least +ve integer such that $a^m = e$.

Since G is a finite group.

$\therefore o(a) / o(G) \Rightarrow m / n$

$\Rightarrow n = mq$ for some integer q

$a^n = a^{mq}$

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

$\therefore a^n = e \Rightarrow a^{o(G)} = e$.

→ P.T a group of prime order cannot have a proper subgroup.

proof: Let $o(G) = p$ where p is a prime number.

Let H be any subgroup of G.

Then $o(H) / o(G)$. (By Lagrange's theorem)

$\Rightarrow o(H) / p$.

Case (i) when $o(H) = 1$

Here $H = \{e\}$

Case (ii) when $o(H) = p$.

Here $o(H) = p = o(G)$

$G = H$.

$\therefore$ H is either contains identity alone or $H = G$ itself.

But $H = \{e\}$ or $H = G$ are improper subgroups of G.

$\therefore$ G cannot have a proper subgroup.

Note: The total number of subgroups of a group of prime order is 2

→ Use Lagrange's theorem to prove that a finite group cannot be expressed as the union of two of its proper subgroups.

Sol^n: Let G be a finite group of order n. i.e $o(G)=n$

If possible let $G = H \cup K$.

where H & K are proper subgroups of G.

Since $e \in H$ and $e \in K$,

atleast one of H, K (say H) must contain more than half the number of elements of G.

Let $o(H) = p$.

$\therefore \frac{n}{2} < p < n$ ($\because$ H is a proper subgroup of G).

$\therefore$ n is not divisible by p.

which contradicts Lagrange's theorem

$\therefore$ Our assumption that $G = H \cup K$ is wrong.

$\therefore$ A finite group cannot be expressed as the union of two of its proper subgroups.

→ Show that two right cosets Ha, Hb of a group G are distinct iff the two left cosets $a^{-1}H$, $b^{-1}H$ of G are distinct.

i.e, $Ha \neq Hb \Leftrightarrow a^{-1}H \neq b^{-1}H$.

Sol^n: Suppose $Ha \neq Hb$

If possible let $a^{-1}H = b^{-1}H$

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

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

$\Rightarrow Ha = Hb$

which is a contradiction.

$\therefore a^{-1}H \neq b^{-1}H$.

Conversely let $a^{-1}H \neq b^{-1}H$

if possible let $Ha = Hb$

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

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

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

which is contradiction

$\therefore Ha = Hb$

→ If $H \subseteq K$ be two subgroups of a finite group G then show that $[G:H] = [G:K][K:H]$

Sol^{n}: Since $H \subseteq K \subseteq G$ and H, K are subgroups of a finite group G.

$\therefore H$ is subgroup of K.

By Lagrange's theorem,

$$[G:H] = \frac{O(G)}{O(H)}$$

Similarly $[G:K] = \frac{O(G)}{O(K)}$

$$[K:H] = \frac{O(K)}{O(H)}$$

$$\therefore [G:K][K:H] = \frac{O(G)}{O(K)} \times \frac{O(K)}{O(H)}$$

$$= \frac{O(G)}{O(H)}$$

$$\therefore [G:H] = [G:K][K:H]$$

→ Show that if H & K are subgroups of G and $a \in G$ then $Ha \cap Ka = (H \cap K)a$.

Sol^{n}: Let $x \in Ha \cap Ka$

then $x \in Ha$ and $x \in Ka$

$\Rightarrow x = ha$ and $x = ka$ for some $h \in H$, $k \in K$

$\Rightarrow ha = ka$

$\Rightarrow h = k$ (By RCL in G)

$\therefore h \in H \cap K$ and $x = ha \Rightarrow x \in (H \cap K)a$

$\therefore Ha \cap Ka \subseteq (H \cap K)a$ ——— ①

Let $x \in (H \cap K)a$

then $x = pa$ for some $p \in H \cap K$.

$\Rightarrow x = pa$ for $p \in H$ & $p \in K$.

$\Rightarrow x = pa$ for $p \in H$ and

$x = pa$ for $p \in K$

$\Rightarrow x \in Ha$ and $x \in Ka$

$\Rightarrow x \in Ha \cap Ka$

$\therefore (H \cap K)a \subseteq Ha \cap Ka$ ——— ②

$\therefore$ from ① & ② we have

$Ha \cap Ka = (H \cap K)a$.

Poincare's theorem:

If G is a group and H, K are two subgroups of finite index in G, prove that $H \cap K$ is of finite index.

Soln: Since H & K are two subgroups of G.

$\therefore H \cap K$ is also subgroup of G.

W.K.T $(H \cap K)a = Ha \cap Ka \quad \forall a \in G$.

i.e, any right coset of $H \cap K$ is the intersection of a right coset of H and right coset of K.

But the number of such intersections is finite.

Since $i_G(H)$ & $i_G(K)$

i.e, $[G:H]$ & $[G:K]$ is each finite.

Consequently, the number of right cosets of $H \cap K$ in G is finite.

$\therefore H \cap K$ is of finite index.

Imp

If H and K are finite subgroups of a group G, then $O(HK) = \frac{O(H)\,O(K)}{O(H \cap K)}$.

Proof: Given that H & K are two subgroups of G.

$\therefore HK$ is a subset of G.

It is not necessary that it will be a subgroup of G.

($O(HK)$ means, the number of distinct elements in HK)

Let $T = H \cap K$. Then T is a subgroup of K. ($\because T \subseteq K$)

Since K is a finite group

$$\therefore [K:T] = \frac{O(K)}{O(T)}$$

$$= m \text{ (say)} \quad \text{---} (1)$$

i.e, the number of distinct right cosets of T in K is m.

Let $Tk_1, Tk_2, Tk_3 \ldots\ldots Tk_m$ be the right cosets of T in K.

where $k_1, k_2, \ldots\ldots k_m \in K$.

Then $K = Tk_1 \cup Tk_2 \cup \ldots\ldots \cup Tk_m$

Now $HK = H(Tk_1 \cup Tk_2 \cup \ldots\ldots \cup Tk_m)$

$= HTk_1 \cup HTk_2 \cup \ldots\ldots \cup HTk_m$

$= Hk_1 \cup Hk_2 \cup \ldots\ldots \cup Hk_m$ ($\because T \subseteq H \Rightarrow HT = H$) ---(2)

Next we show that $Hk_1, Hk_2, \ldots\ldots Hk_m$ are all distinct.

Let, if possible,

$Hk_i = Hk_j$ for $1 \le i < j \le m$

$\Rightarrow k_i k_j^{-1} \in H$ ($\because Ha = Hb \Rightarrow ab^{-1} \in H$)

Also $k_i k_j^{-1} \in K$ ($\because K < G$, $\because k_i, k_j \in K \Rightarrow k_i k_j^{-1} \in K$)

$\Rightarrow k_i k_j^{-1} \in H \cap K = T$.

$\Rightarrow Tk_i = Tk_j$ $(\because ab^{-1} \in H \Rightarrow Ha = Hb)$ ... (4)

which is a contradiction.

$\therefore Hk_1, Hk_2, \ldots Hk_m$ are all distinct.

from (3) we obtain

$$O(HK) = O(Hk_1) + O(Hk_2) + \ldots + O(Hk_m)$$
$$= O(H) + O(H) + \ldots + O(H) \quad (m \text{ times})$$
$$(\because He = H \text{ i.e., } H \text{ is a right coset})$$
$$= m\,O(H)$$
$$\therefore O(HK) = m\,O(H)$$
$$= \frac{O(K)}{O(T)}\,O(H) \quad (\text{from } ①)$$
$$O(HK) = \frac{O(H)\,O(K)}{O(H \cap K)}$$

→ If H & K are subgroups of a finite group G and $O(H) > \sqrt{O(G)}$, $O(K) > \sqrt{O(G)}$ then $O(H \cap K) > 1$ i.e., $H \cap K \neq \{e\}$.

proof: Given that H & K are two subgroups of a finite group G.

$\therefore HK \subseteq G$,

$\therefore O(HK) \leq O(G)$

$\Rightarrow O(G) \geq O(HK)$

$$= \frac{O(H).O(K)}{O(H \cap K)}$$
$$> \frac{\sqrt{O(G)} \cdot \sqrt{O(G)}}{O(H \cap K)} \quad (\text{by hyp})$$
$$= \frac{O(G)}{O(H \cap K)}$$
$$\therefore O(G) > \frac{O(G)}{O(H \cap K)}$$
$$\Rightarrow O(H \cap K) > 1$$

Hence $H \cap K \neq \{e\}$

Ex 4

→ If G is a group of order 35, show that it cannot have two subgroups of order 7.

Sol": If possible let G has two subgroups H & K where $O(H) = O(K) = 7$ and $H \neq K$.

Since $H \cap K$ is a subgroup of H.

By Lagrange's theorem, $O(H \cap K) / O(H)$

i.e, $\frac{O(H)}{O(H \cap K)}$

But $O(H) = 7$ (prime number)

$\therefore O(H \cap K) = 1$ or 7

If $O(H \cap K) = 7$ then $H \cap K = H$

$\Rightarrow K = H$

which is a contradiction to $H \neq K$

If $O(H \cap K) = 1$.

Now $O(HK) = \frac{O(H)\,O(K)}{O(H \cap K)}$

$= \frac{7 \times 7}{1}$

$= 49 > O(G) = 35$

This is impossible

∴ our assumption that the two subgroups H & K of 7 is wrong.

∴ If G is a group of order 35 then it cannot have two subgroups of order 7.

→ If G is a group of order 91, show that it cannot have two subgroups of order 13.

→ Suppose G is a finite group of order pq where p & q are primes with $p > q$. Show that G has atmost one subgroup of order p.

proof: Suppose G has two subgroups H and K each of order p.

i.e, $O(H) = O(K) = p$.

Now $p>q \Rightarrow p^2 > pq = O(G)$ (by hyp)

$\Rightarrow p > \sqrt{O(G)}$.

i.e, $O(H) > \sqrt{O(G)}$ and $O(K) > \sqrt{O(G)}$

Since $HK \subseteq G$.

$\therefore O(HK) \leq O(G)$.

i.e, $O(G) \geq O(HK)$

$$= \frac{O(H)\,O(K)}{O(H\cap K)}$$

$$> \frac{\sqrt{O(G)}\,\sqrt{O(G)}}{O(H\cap K)}$$

$$= \frac{O(G)}{O(H\cap K)}$$

$$\therefore O(G) > \frac{O(G)}{O(H\cap K)}$$

$\Rightarrow O(H\cap K) > 1$

Since $H\cap K$ is a subgroup of H.

$\therefore$ By Lagrange's theorem,

$O(H\cap K)$ divides $O(H) = p$

i.e, $\frac{O(H)}{O(H\cap K)}$

$\Rightarrow O(H\cap K) = p$. ($\because O(H\cap K) > 1$)

$\Rightarrow O(H\cap K) = O(H)$

$\Rightarrow H\cap K = H$

$\Rightarrow K = H$.

$\therefore$ G has atmost one subgroup of order p.

→ Show that: a group G of order 15 has atmost one subgroup of order 5.

Soln: $O(G) = 15$

$= 5\times 3$ $(5>3)$

and both 5 and 3 are prime numbers

$\therefore$ A group of order 15 has atmost one subgroup of order 5.

→ Show that a group G of order $2p$ where p is prime and $p>2$, has exactly one subgroup of order p.

Soln: Suppose G has two subgroups H & K which

$O(H) = O(K) = p$; $H \neq K$

Since $H \cap K$ is subgroup of H.

$\therefore$ By Lagrange's theorem $o(H \cap K) / o(H)$ i.e., $\frac{o(H)}{o(H \cap K)}$

Since $o(H) = p$

$\therefore o(H \cap K) = 1$ or p ($\because p$ is prime)

If $o(H \cap K) = p$ then $o(H \cap K) = o(H)$

$\Rightarrow H \cap K = H$

$\Rightarrow H = K$

which is a contradiction

If $o(H \cap K) = 1$ then $o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)}$

$= \frac{p \cdot p}{1}$

$= p^2 > 2p = o(G)$

Since $p > 2$ and p is prime

But $o(HK) > o(G)$ is impossible.

$\therefore$ A group G of order $2p$ where p is prime and $p > 2$ has exactly one subgroup of order p.

Problem:

→ Consider two subgroups $H = \{I, (1\,2)\}$ and $K = \{I, (1\,3)\}$ of S_3. Show that HK is not a subgroup of S_3

Sol: we have

$HK = \{I \cdot I = I,\ I(1\,3) = (1\,3),\ (1\,2)I = (1\,2),\ (1\,2)(1\,3) = (1\,3\,2)\}$

$= \{I, (1\,3), (1\,2), (1\,3\,2)\}$

Also $KH = \{I, (1\,2), (1\,3), (1\,3\,2)\}$

$= \{I, (1\,2), (1\,3), (2\,3)\}$

Since $HK \neq KH$

HK is not a subgroup of S_3

(or)

$o(HK)$ does not divide $o(S_3) = 6$.

$\therefore$ By Lagrange's theorem,

HK is not a subgroup of S_3.

CYCLIC GROUPS

Cyclic group:

— Suppose G is a group and there is an element $a \in G$ such that $G = \{a^n / n \in \mathbb{Z}\}$ then G is called a cyclic group and 'a' is called generator of G and G is denoted by $\langle a \rangle$ or (a) or $\{a\}$.

i.e, $G = \langle a \rangle$ or (a) or $\{a\}$

i.e, a group consisting of elements which are only the powers of a single element belonging to it is a cyclic group.

Note:

— If G is a cyclic group generated by a, then the elements of G will be $\ldots, a^{-2}, a^{-1}, a^0 = e, a^1, a^2, \ldots$ in multiplicative notation. and the elements of G will be $\ldots -2a, -a, 0, a, 2a, \ldots$ in additive notation.

— The elements of G are not necessarily distinct.

— There exist finite and infinite cyclic groups.

Ex: ① $G = \{1, -1\}$ is $\times^{ve}$ group.

Since $(-1)^0 = 1$, $(-1)^1 = -1$.

$\therefore G = \{(-1)^0, (-1)^1\}$

$\therefore (G, \cdot)$ is a cyclic generated by -1

i.e, $G = \langle -1 \rangle$

② $G = \{\ldots -4, -2, 0, 2, 4, \ldots\}$ is an additive group.

Since $G = \{2m / m \in I\}$

$= \{\ldots -4, -2, 0, 2, 4, \ldots\}$

$\therefore G$ is a cyclic group generated by 2.

i.e, $G = \langle 2 \rangle$.

(3) $G = \{1, -1, i, -i\}$

Since $G = \{(i), (i)^2, (i)^3, (i)^4\}$

$\therefore$ G is a cyclic group generated by i.

i.e, $G = \langle i \rangle$.

Similarly $G = \langle -i \rangle$.

(4) $G = \{1, \omega, \omega^2\}$ is a cyclic group and $G = \langle \omega \rangle$, $G = \langle \omega^2 \rangle$.

Note: There may be more than one generators of a cyclic group.

Ex: Suppose G is any group and $a \in G$.

Let H be the subgroup of G consisting of all integral powers of 'a'.

i.e, $H = \{a^n / n \in I\}$ then H is a cyclic subgroup of G generated by 'a'.

Ex: Show that the set of all n^{th} roots of unity w.r.t x^n is a cyclic group.

Sol: $1^{1/n} = (\cos 0 + i \sin 0)^{1/n}$

$= (\cos 2k\pi + i \sin 2k\pi)^{1/n}$

$= \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$

$= e^{\frac{2k\pi i}{n}}$; $k = 0, 1, 2, \ldots (n-1)$

$= e^{\frac{2k\pi i}{n}}$; $k = 0, 1, 2, \ldots n-1$.

Let $G = \{e^{\frac{2k\pi i}{n}} / k = 0, 1, 2, 3, \ldots n-1\}$

which is a group under x^n.

Let $G = \{w^0 = e, w^1, w^2, \ldots w^{n-1}\}$

where $w^k = e^{\frac{2k\pi i}{n}}$, $k = 0, 1, 2, \ldots (n-1)$

Since $w^0 = 1 = e$, $w^1 = w$, $w^2 = w^2$, $\ldots w^{n-1} = w^{n-1}$.

$\therefore$ Every element of G is some power of w.

i.e, $G = \langle w \rangle$

i.e $G = \langle e^{\frac{2\pi i}{n}} \rangle$.

→ Let $A=\begin{bmatrix}1&0\\0&1\end{bmatrix}$, $B=\begin{bmatrix}0&1\\-1&0\end{bmatrix}$ $C=\begin{bmatrix}-1&0\\0&-1\end{bmatrix}$ and $D=\begin{bmatrix}0&-1\\1&0\end{bmatrix}$

we have that $G=\{A,B,C,D\}$ with matrix multiplication as operation is a group whose composition table is given below.

•	A	B	C	D
A	A	B	C	D
B	B	C	D	A
C	C	D	A	B
D	D	A	B	C

Soln: Here $O(G)=4$

A is the identity element in G.

Now $B^1=B$, $B^2=B\cdot B=C$

$B^3=B^2\cdot B=C\cdot B=D$

$B^4=B^3\cdot B=D\cdot B=A$

$\therefore B\in G$ generates the group G and hence G is a cyclic group with B.

i.e, $G=\langle B\rangle$.

→ Describe all the elements in cyclic subgroup of multiplicative group G of 2×2 matrices over $\mathbb{R}$ generated by the given 2×2 matrix.

(a) $\begin{bmatrix}0&-1\\-1&0\end{bmatrix}$ (b) $\begin{bmatrix}1&1\\0&1\end{bmatrix}$ (c) $\begin{bmatrix}3&0\\0&2\end{bmatrix}$ (d) $\begin{bmatrix}0&-2\\2&0\end{bmatrix}$

Soln: (b) Let $A=\begin{bmatrix}1&1\\0&1\end{bmatrix}$ ....

Now $A^2=\begin{bmatrix}1&2\\0&1\end{bmatrix}$, $A^3=\begin{bmatrix}1&3\\0&1\end{bmatrix}$, ------

$A^{-1}=\begin{bmatrix}1&-1\\0&1\end{bmatrix}$, $A^{-2}=(A^2)^{-1}=\begin{bmatrix}1&-2\\0&1\end{bmatrix}$, ------

Let $H=\left\{\begin{bmatrix}1&n\\0&1\end{bmatrix} \middle/ n\in\mathbb{Z}\right\}$

$= \{A^n / n \in \mathbb{Z}\} \subseteq G$

Clearly which is subgroup of G and hence it is cyclic subgroup of G generated by A.

d) Let $A = \begin{bmatrix} 0 & -2 \\ -2 & 0 \end{bmatrix}$.

$A^2 = \begin{bmatrix} 4 & 0 \\ 0 & 4 \end{bmatrix}$, $A^3 = \begin{bmatrix} 0 & -8 \\ -8 & 0 \end{bmatrix}$, $A^4 = \begin{bmatrix} 16 & 0 \\ 0 & 16 \end{bmatrix}$, $A^5 = \begin{bmatrix} 0 & -32 \\ -32 & 0 \end{bmatrix}$

$\therefore$ All the matrices of the form

$\begin{bmatrix} 4^n & 0 \\ 0 & 4^n \end{bmatrix}$ or $\begin{bmatrix} 0 & -2^{2n+1} \\ -2^{2n+1} & 0 \end{bmatrix}$ for $n \in \mathbb{Z}$.

Let $H = \{A^n / n \in \mathbb{Z}\} \subseteq G$.

Clearly which is subgroup of G and hence it is a cyclic subgroup of G generated by A.

→ Find the order of the cyclic subgroup of the given group generated by the indicated element.

(a) The subgroup of $\mathbb{Z}_4$ generated by 3.

(b) The subgroup of U_6 generated by $\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$

(c) The subgroup of U_5 generated by $\cos\frac{4\pi}{5} + i\sin\frac{4\pi}{5}$

(d) The subgroup of U_8 generated by $\cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2}$

(e) The subgroup of U_8 generated by $\cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4}$.

(f) The subgroup of the x^{ve} group of invertible 4×4 matrices generated by $\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$

(g) The subgroup of the x^{ve} group G of invertible 4×4 matrices generated by

(i) $\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$ (ii) $\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$

Sol^n:

(a) Let Z_4 be the set of all residue classes modulo 4 is a group w.r.t $+^n$ of residue classes.

Let $Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ or $Z_4 = \{0, 1, 2, 3\}$.

Let $H = \langle 3 \rangle$

= the subgroup generated by 3

$= \{n(3) / n \in I\}$

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

Now $0(3) = 0$

$1(3) = 3$

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

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

$4(3) = 12 = 0$, etc.

$\therefore H = \langle 3 \rangle$

$= \{0, 1, 2, 3\}$ is the cyclic-subgroup of Z_4 generated by 3.

$\therefore O(H) = 4$ (or $o(H) = o(\text{generator})$ i.e., $o(H) = o(3) = 4$)

(b) $U_6 = \{z \in C / z^6 = 1\}$ i.e., $z = 1^{1/6}$

where $z = \cos\frac{2m\pi}{6} + i\sin\frac{2m\pi}{6}$;

$m = 0, 1, 2, 3, 4, 5$.

Let $U_6 = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5\}$ ($\because \omega^6 = 1$)

U_6 is the sixth roots of unity with $e = 1$.

Let $\omega^2 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$.

Let $H = \langle \omega^2 \rangle$

= the subgroup generated by ω^2.

$= \{(\omega^2)^n / n \in I\}$

$= \{\ldots\ldots (\omega^2)^{-2}, (\omega^2)^{-1}, (\omega^2)^0, (\omega^2)^1, (\omega^2)^2, \ldots\ldots\}$

Now $(\omega^2)^0 = 1$

$(\omega^2)^1 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$

$(\omega^2)^2 = \left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right)^2$

$= \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}$ (By DeMoivre's theorem)

$= \cos\left(\pi + \frac{\pi}{3}\right) + i\sin\left(\pi + \frac{\pi}{3}\right)$

$= -\cos\frac{\pi}{3} - i\sin\frac{\pi}{3}$.

$\neq 1$

$(\omega^2)^3 = \left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right)^3$

$= \cos 2\pi + i\sin 2\pi$

$= 1 = e$.

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

$= 1 \cdot \omega^2 = \omega^2$

$(\omega^2)^5 = (\omega^2)^4(\omega^2) = \omega^2 \cdot \omega^2 = (\omega^2)^2$

$(\omega^2)^6 = (\omega^2)^5(\omega^2) = (\omega^2)^2(\omega^2) = (\omega^2)^3 = 1$

$(\omega^2)^{-1} = \cos\left(-\frac{2\pi}{3}\right) + i\sin\left(-\frac{2\pi}{3}\right)$

$= \cos\frac{2\pi}{3} - i\sin\frac{2\pi}{3}$

$= \cos\left(\pi - \frac{\pi}{3}\right) - i\sin\left(\pi - \frac{\pi}{3}\right)$

$= -\cos\frac{\pi}{3} - i\sin\frac{\pi}{3}$

$= (\omega^2)^2$ etc.

$\therefore H = \langle \omega^2 \rangle$

$= \{1, \omega^2, (\omega^2)^2\}$ is the cyclic subgroup of U_6 generated by $\omega^2 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$.

$\therefore o(H) = 3$ (or $o(H) = o(\text{generator})$ i.e., $o(H) = o(\omega) = 3$).

Soln (B) Let $G = \{(a_{ij})_{4\times 4}\}$ is the $\times^{ve}$ group of invertible 4×4 matrices.

$5(1) = 0$; $6(1) = 1$ etc

$\therefore Z_5 = \langle 1 \rangle$

Similarly $Z_5 = \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle$.

$\therefore (Z_5, +)$ is a cyclic group.

→ Show that $(Z_m, +)$, where Z_m is the set of all residue classes modulo 'm' (prime) and $+$ is the residue class $+^n$, a cyclic group.

Sol" Let $Z_m = \{0, 1, 2, \ldots\ldots m-1\}$

Now $1(1) = 1$

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

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

$(m-1)(1) = m-1$

$m(1) = m = 0$ etc.

$\therefore 1$ is the generator of $(Z_m, +)$

i.e, $(Z_m, +) = \langle 1 \rangle$.

$\therefore (Z_m, +)$ is a cyclic group generated by 1.

Similarly we can prove that $2, 3, \ldots\ldots m-1$ are also generators

Some properties of cyclic groups:

Theorem: Every cyclic group is an abelian group.

proof: Let G be the cyclic group generated by a.

$\therefore G = \langle a \rangle$

$= \{a^n / n \in I\}$

Let $a^r, a^s \in G$ where $r, s \in I$

$\therefore a^r \cdot a^s = a^{r+s} = a^{s+r}$ $\ldots (\because r+s = s+r$ in $I)$

$= a^s \cdot a^r$.

$\therefore G$ is abelian.

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

Let $H = \langle A \rangle$

$= $ the subgroup of G generated by A.

$= \{A, A^2, A^3, \ldots\}$

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

$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

$= I$

$A^3 = A^2 \cdot A = I \cdot A = A$

$A^4 = A^3 \cdot A = A \cdot A = A^2 = I$ etc.

$\therefore H = \langle A \rangle$

$= \{I, A\} = \{A^2, A\}$ or $\{A, A^2\}$ is cyclic subgroup of G generated by A.

$\therefore O(H) = 2 = O(A)$.

→ Show that $(\mathbb{Z}_5, +)$ where $\mathbb{Z}_5$ is the set of all residue classes modulo 5, is a cyclic group w.r.t $+^n$ of residue classes.

Sol^n: Let $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ or $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

Since $0 \in \mathbb{Z}_5$

Now $1(0) = 0$

$2(0) = 0 + 0 = 0$ etc.

$\therefore 0$ is not generator of $\mathbb{Z}_5$.

Since $1 \in \mathbb{Z}_5$

Now $1(1) = 1$

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

$3(1) = 1 + 1 + 1 = 3$; $4(1) = 1 + 1 + 1 + 1 = 4$.

Note: The converse of the above theorem need not be true i.e, every abelian group need not be cyclic group.

Ex: Let $G = \{A, B, C, D\}$

where $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, $C = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $D = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$

and the matrix multiplication as the binary composition on G.

Construct composition table:-

	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

Clearly G is finite abelian group (of order 4) with identity element A

Also $B^2 = A$, $C^2 = A$ and $D^2 = A$.

i.e, each element is of order 2 (except the identity A)

Here there is no element of order 4 in G.

$\therefore$ G is not cyclic and hence every finite abelian group need not be cyclic.

→ If 'a' is a generator of a cyclic group G, then a^{-1} is also a generator of G.

(OR)

If $G = \langle a \rangle$ then $G = \langle a^{-1} \rangle$.

Proof: Given that $G = \langle a \rangle$:

$= \{ a^n / n \in I \}$

Let $a^r \in G$; $r \in I$ then $a^r = (a^{-1})^{-r}$; $-r \in I$.

$\therefore$ each element of G is generated by a^{-1}.

$\therefore$ a^{-1} is also generator of G. i.e, $G = \langle a^{-1} \rangle$

Theorem → Show that the number of generators of an infinite cyclic group is two.

proof: Let G be any infinite cyclic group generated by a.

$\therefore G = \langle a \rangle$

$= \{ a^n / n \in I \}$

$= \{ a^n / n = 0, \pm 1, \pm 2, \ldots \}$

Since G is infinite

$\therefore a^n = e \iff n = 0$ —— (1)

(Note: $a^m = e$ for $m \neq 0 \in Z$

$\Rightarrow G = \{ a, a^2, a^3, \ldots a^m = e \}$ which is finite)

Let $b \in G$ be any other generator of G.

$\therefore G = \langle b \rangle$

Since $b \in G = \langle a \rangle$, $b = a^n$ for some $n \in I$.

Since $a \in G = \langle b \rangle$, $a = b^m$ for some integer $m \in I$

$\therefore e = b^m$

$\rightarrow a = (a^n)^m$

$= a^{nm}$

Now $a = a^{nm} \Rightarrow a^{nm-1} = e$

$\Rightarrow nm - 1 = 0$ (by (1))

$\Rightarrow nm = 1$

$\Rightarrow n = 1, m = 1$ or $n = -1, m = -1$

$\therefore b = a$ or a^{-1}

$\therefore G$ has exactly two generators a & a^{-1}.

Note: The converse of the above theorem need not be true.

i.e, the subgroup is cyclic, the group need not be cyclic.

Ex: W.K.T $(\mathbb{Z},+)$ is a subgroup of $(\mathbb{R},+)$

Here $(\mathbb{Z},+)$ is a cyclic group generated by $+1$, and -1

But $(\mathbb{R},+)$ is not a cyclic group. ($\because$ it has no generators)

Theorem: If 'p' is a prime number then every group of order 'p' is a cyclic group.

i.e, a group of prime order is cyclic.

Proof: Let $p \geq 2$ be a prime number and G be a group such that $o(G) = p\ (\geq 2)$

Since the number of elements in G is atleast 2,

one of the elements of G will be different from the identity $e \in G$.

Let that be 'a'.

Let $\langle a \rangle$ be the cyclic subgroup of G generated by 'a'.

$\therefore a \in \langle a \rangle \Rightarrow \langle a \rangle \neq \{e\}$.

Let $\langle a \rangle$ be of order h.

$\therefore$ By Lagrange's theorem h/p i.e, $\frac{p}{h}$.

But p is prime number.

$\therefore h = 1$ or $h = p$.

But $\langle a \rangle \neq \{e\}$ and hence $h = p$.

$\therefore o(\langle a \rangle) = p = o(G)$

i.e, $\langle a \rangle = G$.

which shows that G is a cyclic group.

→ Every subgroup of a cyclic group is cyclic.

proof: Let G be a cyclic group generated by 'a'.

$\therefore G = \langle a \rangle$

Let H be a subgroup of G.

If $H = G$ or $\{e\}$, then H is cyclic.

If H is a proper subgroup of G, then the elements of H are integral powers of 'a'.

If $a^s \in H$ then $a^{-s} \in H$

$\therefore$ H contains the elements which are +ve as well as -ve integral powers of a.

Let 'm' be the least +ve integer such that $a^m \in H$ then we have to prove that $H = \langle a^m \rangle$

i.e, H is cyclic and is generated by a^m.

Let a^t be any arbitrary element of H. By division algorithm $\exists$ integers q & r such that

$t = mq + r$, $0 \le r < m$.

Now $a^m \in H \Rightarrow (a^m)^q \in H$ (By closure prop.)

$\Rightarrow a^{mq} \in H$

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

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

Also $a^t \in H$, $a^{-mq} \in H \Rightarrow a^{t-mq} \in H$

$\Rightarrow a^r \in H$ $(\because r = t - mq)$

Now 'm' is the least +ve integer such that $a^m \in H$ and $0 \le r < m$

$\therefore$ 'r' must be equal to zero.

$\therefore t = mq$

$\therefore a^t = a^{mq}$

$\Rightarrow a^t = (a^m)^q$

$\therefore$ every element $a^t \in H$ is of the form $(a^m)^q$.

$\therefore$ H is a cyclic group and is generated by a^m.

Note [1]. we have by the above theorem if $o(G)=p$, (p a prime number) then every element of G which is not an identity is a generator of G.
i.e, the number of generators of G having p elements is equal to $p-1$.

[2]. Every Group G of order less than 6 is abelian.

for:
we know that every group G of order less than or equal to 4 is abelian.
Also w.k.t every group of prime order is cyclic and every cyclic group is abelian.
If $o(G)<5$ then G is abelian.
i.e, the smallest non abelian group is of order 6

[3]. The converse of the above theorem need not be true.
i.e, every cyclic group of order need not be a prime number.

Ex: 4^{th} roots of unity w.r.t $\times$ form a cyclic group and 4 is not a prime number.

Theorem: If a finite group of order 'n' contains an element of order 'n' then the group is cyclic.

proof: Let G be a finite group of order 'n'. i.e $o(G)=n$
Let $a \in G$ such that $o(a)=n$
i.e, $a^n = e$ where 'n' is the least +ve integer.
If H is a cyclic subgroup of G generated by 'a'
i.e, if $H = \{a^r / r \in Z\}$
then $o(H)=n$.
because the order of the generator 'a' of H is 'n'.
$\therefore H$ is a cyclic subgroup of G and $o(H)=n=o(G)$

$\therefore H = G$ and G itself is a cyclic group with 'a' as a generator.

Note: Suppose G is a finite group of order 'n' and we are to determine whether G is cyclic or not. For this we find the orders of the elements of G and if $a \in G$ exists such that $o(a) = n$, then G will be a cyclic group with 'a' as a generator.

Theorem Every finite group of composite order possesses proper subgroups.

Proof: Let G be a finite group of composite order mn where $m(\neq 1)$ and $n(\neq 1)$ are +ve integers.

(i) Let G be the cyclic group and generated by 'a'.

$\therefore G = \langle a \rangle$.

$\Rightarrow o(a) = o(G) = mn$.

$\Rightarrow a^{mn} = e$

$\Rightarrow (a^n)^m = e$

$\Rightarrow o(a^n) \leq m$.

Let $o(a^n) = p$ where $p < m$.

then $(a^n)^p = e \Rightarrow a^{np} = e$.

But $p < m \Rightarrow np < nm$.

$\therefore a^{np} = e$ where $np < mn$.

Since $o(a) = mn$ ($a^{mn} = e$), $a^{np} = e$ is not possible unless $p = m$.

$\therefore o(a^n) = m$.

$\therefore H = \langle a^n \rangle$ is a cyclic subgroup of G and $o(H) = o(a^n)$.

$\therefore o(H) = m$.

Since $2 \leq m < mn$.

$\therefore H$ is a proper subgroup of G.

(ii) Let G be not cyclic group.
Then order of each element of G must be less than mn.
So there exists an element say b in G such that $2 \leq o(b) < mn$.
Then $H = \langle b \rangle$ is a proper subgroup of G.

Theorem If a cyclic group G is generated by an element 'a' of order 'n', then a^m is a generator of G iff the greatest common divisor of m and n is 1. i.e, m, n are relatively prime.

proof: Let $G = \langle a \rangle$ such that $o(a) = n$
i.e, $a^n = e$.
The group G contains exactly 'n' elements

(i) Let m be relatively prime to 'n'.
NOD consider the cyclic subgroup $H = \langle a^m \rangle$ of G.
Clearly $H \subseteq G$ —①
Since m, n are relatively prime there exist two integers x & y such that $mx + ny = 1$.

$$\therefore a = a^1$$
$$= a^{mx+ny}$$
$$= a^{mx} \cdot a^{ny}$$
$$= a^{mx} \cdot (a^n)^y$$
$$= a^{mx} \cdot e^y$$
$$= a^{mx}$$
$$= (a^m)^x$$
$$\therefore a = (a^m)^x$$

∴ Each integral exponent of 'a' will also be some integral exponent of a^m.
$\therefore G \subseteq H$ —②
∴ From ① & ② we have $H = G$
and a^m is a generator of G.

(ii) Let $G = \langle a^m \rangle$

Let the greatest common divisor of m and n be $d(\neq 1)$ i.e, $d > 1$.

Then $\frac{m}{d}, \frac{n}{d}$ must be integers.

Now $(a^m)^{\frac{n}{d}} = a^{\frac{mn}{d}}$

$= (a^n)^{\frac{m}{d}}$

$= e^{\frac{m}{d}}$

$= e$

$\therefore (a^m)^{\frac{n}{d}} = e$

$\Rightarrow o(a^m) \leq \frac{n}{d} < n$

$\Rightarrow o(a^m) < n$

$\therefore a^m$ cannot be generator of G.

because $o(a^m) \neq o(G)$.

Hence d must be equal to 1.

$\therefore |G|$ is prime to n.

Theorem: If G is a finite cyclic group of order 'n' generated by 'a' then the subgroups of G are precisely the subgroups generated by a^m, where m divides n.

Proof: Since G is a finite cyclic group of order 'n' generated by 'a', then a^m generates a cyclic subgroup, say H, of G i.e $H = \langle a^m \rangle$.

Since $o(G) = n = o(a)$.

$\therefore a^n = e$ where $e \in G$.

Since H is a subgroup of G, $e \in H$

i.e, $a^n \in H$.

If 'm' is the least +ve integer such that $a^m \in H$ then by division algorithm, $\exists$ +ve integers q & r such that $n = mq + r$; $0 \leq r < m$.

$\therefore a^r = a^{n-r}$

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

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

But $a^m \in H \Rightarrow (a^m)^q \in H$

$\Rightarrow a^{mq} \in H$

Now $a^n \in H$, $a^{mq} \in H \Rightarrow a^{n-mq} \in H$

$\Rightarrow a^r \in H$.

But $0 < r < m$ and $a^r \in H$ is a contradiction to our assumption that m is the smallest +ve integer such that $a^m \in H$

$\therefore r = 0$

$\therefore n = mq$

i.e., m divides n.

and $a^n = a^{mq}$

$= (a^m)^q \in H$.

which means that a^m generates the cyclic subgroup H of G.

Ex: write down all the subgroups of a finite cyclic group of order 18, the cyclic group being generated by 'a'.

Soln: Let e be the identity element in G.

Now G, $\{e\}$ are trivial subgroups of G and generated by 'a' and $a^{18} = e$ respectively.

The other proper subgroups are precisely the subgroups generated by a^m where m divides 18.

Such m's are 2, 3, 6, 9.

∴ The subgroups are

$\langle a^2 \rangle = \{a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}, a^{18} = e\}$,

$\langle a^3 \rangle = \{a^3, a^6, a^9, a^{12}, a^{15}, a^{18} = e\}$, $\{a^6, a^{12}, a^{18} = e\} = \langle a^6 \rangle$

and $\{a^9, a^{18} = e\} = \langle a^9 \rangle$.

Euler ϕ-function:

If n is any +ve integer, then Euler ϕ-function, denoted by $\phi(n)$ is defined as $\phi(1)=1$,
$\phi(n)$ = number of +ve integers less than n and relatively prime to n, if $n>1$.

Ex: (1) $\phi(4)=2$, since 1, 3 are the +ve integers less than 4 and relatively prime to 4.

(2) $\phi(5)=4$, since 1, 2, 3, 4 are the +ve integers less than 5 and relatively prime to 5.

(3) $\phi(6)=2$, since 1, 5 are the +ve integers less than 6 and relatively prime to 6.

(4) $\phi(8)=4$, since 1, 3, 5, 7 are the +ve integers less than 8 and relatively-prime to 8.

(5) $\phi(p)=p-1$, if p is prime.

$\Rightarrow$

Note: I. The number of generators of a finite cyclic group of order 'n' is $\phi(n)$, where $\phi(n)$ is the Euler ϕ-function.

(or)

If $G=\langle a\rangle$ be a finite cyclic group of order 'n' then a^m is a generator of G iff $0<m<n$ and $(m,n)=1$

II. From number theory, if $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots\cdots p_k^{\alpha_k}$ where $p_1, p_2, \ldots\ldots p_k$ are all prime factors of n, then $\phi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\cdots\left(1-\frac{1}{p_k}\right)$.

Further if $n=p^{\alpha}$ where p is less than n and prime to n then $\phi(n)=p^{\alpha}\left(1-\frac{1}{p}\right)$

Problems:

Find the generators of a cyclic group of order 8.

Sol^n: we have $G = \langle a \rangle$, $a^8 = e$.

All the generators of G are a^1, a^3, a^5, a^7.

i.e, $G = \langle a \rangle = \langle a^3 \rangle = \langle a^5 \rangle = \langle a^7 \rangle$.

(∵ 1, 3, 5, 7 are +ve integers less than 8 and prime to 8.)

Note: Let U_n denote the group of integers relatively prime to n under multiplication mod n.

→ Show that U_9 is cyclic group. What are all its generators?

Sol^n: we have $U_9 = \{1, 2, 4, 5, 7, 8\}$

Now $2^1 = 2$, $2^2 = 2 \times_9 2 = 4$, $2^3 = 2 \times_9 2 \times_9 2 = 8$

$2^4 = 16 = 7$, $2^5 = 5$, $2^6 = 1$

$\therefore U_9 = \langle 2 \rangle$

$\therefore U_9$ is a cyclic group and $O(U_9) = 6$.

The +ve integers less than 6 and prime to 6 are 1, 5.

Hence all the generators of U_9 are $2^1, 2^5$ i.e, 2, 5.

→ Show that U_{17} is a cyclic group, what are all its generators?

Sol^n: $U_{17} = \{1, 2, \ldots, 16\}$

and $O(U_{17}) = 16$

All the +ve integers less than 16 and prime to 16 are 1, 3, 5, 7, 9, 11, 13, 15.

We can easily verify that $U_{17} = \langle 3 \rangle$.

i.e, every element of U_{17} is a power of 3.

All the generators of U_{17} are $3^1, 3^3 = 10, 3^5 = 5, 3^7 = 11, 3^9 = 14, 3^{11} = 7, 3^{13} = 12, 3^{15} = 6$.

Hence all the generators of U_{17} are

$3, 5, 6, 7, 10, 11, 12, 14$.

→ Is U_8 a cyclic group ?

Soln: Let $U_8 = \{1, 3, 5, 7\}$

$O(U_8) = 4$.

Since $3^1 = 3$, $3^2 = 1$, $3^3 = 3$, $3^4 = 1$, $3^5 = 1$ etc.

$\therefore$ 3 is not generator of U_8.

Since $5^1 = 5$, $5^2 = 1$, $5^3 = 5$ etc.

$\therefore$ 5 is not generator of U_8.

Similarly 7 is not generator of U_8.

$\therefore$ U_8 is not cyclic.

→ Find the number of generators of cyclic groups of orders 5, 6, 8, 12.

Soln: $O(G) = 5$,

the number of generators of $G = \phi(5)$

$= 5(1 - \frac{1}{5}) = 4$.

$O(G) = 6$.

the number of generators of $G = \phi(6)$

$= 6(1 - \frac{1}{2})(1 - \frac{1}{3})$

$= 6(\frac{1}{2})(\frac{2}{3})$

$= 2$ ($\because 6 = 2^1 \cdot 3^1$ i.e., 2, 3 are prime factors of 6)

$O(G) = 8$.

the number of generators of $G = \phi(8)$

$= 2^3(1 - \frac{1}{2}) = 4$ ($\because$ 2 is the only prime factor of 8)

$O(G) = 12$.

the number of generators of $G = \phi(12)$

$= 12(1 - \frac{1}{2})(1 - \frac{1}{3})$

$= 4$ ($\because 12 = 2^2 \times 3 = 2^2 \times 3^1$)

NORMAL SUBGROUPS

Def^n: A subgroup H of a group G is said to be a normal subgroup of G if $\forall x \in G$ and $\forall h \in H$, $xhx^{-1} \in H$.

From the definition we conclude that

(i) H is normal subgroup of G iff $xHx^{-1} \subseteq H \ \forall x \in G$
where $xHx^{-1} = \{xhx^{-1} / h \in H, x \in G\} \subseteq H$.

(ii) H is a normal subgroup of G iff $x^{-1}Hx \subseteq H \ \forall x \in G$
$(\because x \in G \Rightarrow x^{-1} \in G$
$\forall h \in H, x^{-1}h(x^{-1})^{-1} \in H$
$\Rightarrow x^{-1}hx \in H)$

(iii) the improper subgroup $H = \{e\}$ is a normal subgroup
$(\because e \in H \Rightarrow xex^{-1} \in H \ \forall x \in G)$

(iv) and the improper subgroup $H = G$ is a normal subgroup
$(\because h \in G \Rightarrow xhx^{-1} \in G, \forall x \in G)$

$H = \{e\}$ and $H = G$ are called improper or trivial normal subgroups of a group G and all other normal subgroups of G, if exist, are called proper normal subgroups of G.

Note: Any non-abelian group in which every subgroup is normal is called a Hamilton group.

Simple group: A group having no proper normal subgroups is called a simple group.

→ Every group of prime order is simple.

Theorem: A subgroup H of a group G is normal iff $xHx^{-1} = H \ \forall x \in G$.

Proof: (i) Let $xHx^{-1} = H \ \forall x \in G$
To prove that H is normal.
Since $xHx^{-1} \subseteq H \ \forall x \in G$.

$\therefore$ H is a normal subgroup of G

(ii) Let H be a normal subgroup of G.

we prove that $xHx^{-1} = H \quad \forall x \in G$

Since H is normal subgroup of G

$\therefore xHx^{-1} \subseteq H \quad \forall x \in G$ ——— (1)

Also $x \in G \Rightarrow x^{-1} \in G$

$\therefore \forall x \in G, \; x^{-1}H(x^{-1})^{-1} \subseteq H$

$\Rightarrow x^{-1}Hx \subseteq H$

$\Rightarrow x(x^{-1}Hx)x^{-1} \subseteq xHx^{-1}$

$\Rightarrow H \subseteq xHx^{-1}$ ——— (2)

from (1) & (2), we have

$\therefore xHx^{-1} = H \quad \forall x \in G.$

$\Longrightarrow$ A subgroup H of a group G is a normal subgroup of G iff each left coset of H in G is a right coset of H in G.

Proof: (i) Let H be a normal subgroup of G.

Then $xHx^{-1} = H \quad \forall x \in G$

$\Rightarrow (xHx^{-1})x = Hx \quad \forall x \in G$

$\Rightarrow xH = Hx \quad \forall x \in G$

$\Rightarrow$ every left coset of H in G is a right coset of H in G.

(ii) Let every left coset of H in G be a right coset of H in G.

Let $x \in G$ then $xH = Hy$ for some $y \in G$.

Since $e \in H$, $x = xe \in xH$

$\Rightarrow x \in xH$

Since $xH = Hy$

$\Rightarrow x \in Hy$.

$\Rightarrow Hx = Hy$ $(\because a \in bH \Rightarrow aH = bH$ & $a \in Hb \Rightarrow Ha = Hb)$

$\therefore xH = Hx \quad \forall x \in G$

$\Rightarrow xHx^{-1} = Hxx^{-1} \quad \forall x \in G.$

$\Rightarrow xHx^{-1} = H \quad \forall x \in G.$

H is a normal subgroup of G.

$\therefore$ H is a normal subgroup of $G \Leftrightarrow$ Every left coset of H in G is a right coset of H in G.

→ A subgroup H of a group G is a normal subgroup of G iff the product of two right (left) cosets of H in G is again a right (left) coset of H in G.

Proof: (i) Let H be a normal subgroup of G.

$\forall a, b \in G \Rightarrow ab \in G$

$\therefore Ha, Hb, Hab$ are right cosets of H in G.

Then $Ha \cdot Hb = H(aH)b$.

$= H(Ha)b$ $(\because H$ is normal $\Rightarrow aH = Ha)$

$= HHab$

$= Hab$ $(\because HH = H)$

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

(ii) For $a, b \in G$, $Ha \cdot Hb = Hab$.

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

we have $xhx^{-1} = (ex)(hx^{-1}) \in (Hx)(Hx^{-1})$

$\Rightarrow xhx^{-1} \in Hxx^{-1}$ $(\because Ha \cdot Hb = Hab)$

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

$\therefore H$ is a normal subgroup of G.

Similarly we can prove theorem for left cosets.

Note: (1) Let H be a normal subgroup of $(G, \cdot)$. Let $a, b \in G$ then Ha, Hb are two right cosets of H in G. Then right cosets multiplication is defined as $Ha \cdot Hb = Hab$.

[2]. If H is a normal subgroup of a group $(G, \cdot)$ then the following statements are equivalent to one another.

(i) $x^{-1}hx \in H$ for $x \in G$ and $h \in H$

(ii) $xHx^{-1} = H$ for $x \in G$

(iii) $xH = Hx$ for $x \in G$

(iv) the set of right (left) cosets of H in G is closed wrt coset multiplication.

→ Every subgroup of an abelian group is normal.

Proof: Let H be a subgroup of an abelian group G.

Let $h \in H$, $x \in G$ and e be the identity element in G.

$$\begin{aligned} h &= eh \\ &= (xx^{-1})h \\ &= x(x^{-1}h) \\ &= x(hx^{-1}) \quad (\because G \text{ is an abelian} \Rightarrow x^{-1}h = hx^{-1}) \\ &= xhx^{-1} \end{aligned}$$

i.e., $h \in H \Rightarrow xhx^{-1} \in H \quad \forall x \in G$

$\therefore H$ is normal subgroup of G.

Imp → If G is a group and H is a subgroup of index 2 in G, then H is a normal subgroup of G.

Proof: Since the index of the subgroup H in G is 2,

∴ the number of distinct right cosets of H in G = the number of distinct left cosets of H in G = 2.

Let $x \in G$

∴ The right cosets are H, Hx and two left cosets are H, xH.

Now $x \in H$ or $x \notin H$

– If $x \in H$ then $Hx = H = xH$ $\quad (\because a \in H \Rightarrow Ha = H \text{ or } aH = H)$

$\Rightarrow Hx = xH$.

$\therefore H$ is a normal subgroup of G.

- If $x \notin H$ then $Hx \neq H$ and $xH \neq H$.

Since the index of H in G is 2.

$\therefore G = H \cup Hx = H \cup xH$

Since there is no element common to H, Hx.

$\therefore$ we must have $Hx = xH$.

$\therefore H$ is a normal subgroup of G.

→ The intersection of any two normal subgroups of a group is a normal subgroup.

Proof: Let H & K be normal subgroups of a group G.

Since H & K are subgroups of G.

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

Let $n \in H \cap K$ and $x \in G$

$\therefore n \in H$ and $n \in K$;

$\therefore xnx^{-1} \in H$ and $xnx^{-1} \in K$

($\because H$ & K are normal subgroups of G.)

$\Rightarrow xnx^{-1} \in H \cap K$ for $x \in G$

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

Note: The arbitrary intersection of any number of normal subgroups of a group G is also normal subgroup of G.

Theorem:

A normal subgroup of a group G is commutative with every complex of G.

Proof: Let N be a normal subgroup and H be a complex of G.

To prove that $NH = HN$.

Let $nh \in NH$ where $n \in N$ & $h \in H$.

We can write

$nh = e(nh)$ $(\because e \in G)$

$nh = hh^{-1}(nh)$

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

But N is a normal subgroup of G.

$\therefore h^{-1}nh \in N.$

$\therefore nh \in HN.$

$\therefore NH \subseteq HN$ — ①

Similarly $hn \in HN.$

$\Rightarrow hn \in NH$ $(\because hn = (hn)h^{-1}h = (hnh^{-1})h \in NH)$

$\therefore HN \subseteq NH$ — ②

∴ from ① & ② we have $NH = HN$

→ If N is a normal subgroup of G and H is any subgroup of G, then HN is a subgroup of G.

Proof: Let N be a normal subgroup of G and H be a subgroup of G.

Since a normal subgroup of G is commutative with every complex of G.

We have $NH = HN.$

∴ HN is a subgroup of G. $(\because H \& K \text{ are subgroups of } G \Rightarrow HK = KH \Leftrightarrow HK < G).$

→ If H is a subgroup of G and N is a normal subgroup of G then (i) HN is a normal subgroup of H.

(ii) N is a normal subgroup of HN.

Proof:

(i) H, N are subgroups of G ⇒ HN is a subgroup of G.

⇒ HN is a subgroup of H $(\because HN \subseteq H)$

Let $x \in H.$

$\therefore x \in G.$

Let $y \in HN.$

$\therefore y \in H$ and $y \in N.$

Now $y \in N \Rightarrow xyx^{-1} \in N$ ($\because N$ is normal in G)

and $y \in H, x \in H \Rightarrow x^{-1} \in H, y \in H$

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

$\therefore xyx^{-1} \in H \cap N$.

$\therefore H \cap N$ is a normal subgroup of H.

(ii) $e \in H$ and $e \in N$

Since $H \neq \phi$, $N \neq \phi$.

$\therefore HN \neq \phi$.

Let $n \in N$ then $n = en$

$\therefore en \in HN \quad \forall n \in N$

$\Rightarrow N \subset HN$.

Since HN is a subgroup of G,

N is a subgroup of G and $N \subseteq HN$

$\therefore N$ is also subgroup of HN.

Let $n \in N$ and $h_1 n_1 \in HN$.

where $h_1 \in H$, $n_1 \in N$.

Now $(h_1 n_1) n (h_1 n_1)^{-1} = h_1 n_1 n n_1^{-1} h_1^{-1}$

$= h_1 (n_1 n n_1^{-1}) h_1^{-1} \in N$

($\because h_1 \in H \Rightarrow h_1 \in G$ and N is a normal subgroup of G)

$\therefore N$ is a normal subgroup of HN.

→ If N, M are normal subgroups of G, then NM is also a normal subgroup of G.

Proof: Since $N \neq \phi$, $M \neq \phi$.

$\Rightarrow NM \neq \phi$ and $MN \neq \phi$.

Since a normal subgroup of G is commutative with every complex of G, $NM = MN$

Since N, M are subgroups of G.

NM is also a subgroup of G.

Let $x \in G$ and $nm \in NM$.

$\therefore x(nm)x^{-1} = x(nx^{-1}x)mx^{-1}$

$= (xnx^{-1})(xmx^{-1}) \in NM$

$\therefore NM$ is a normal subgroup of G.

Theorem: If M, N are two normal subgroups of G such that $M \cap N = \{e\}$. Then every element of M commutes with every element of N.

Proof: Let $m \in M$ and $n \in N$.

To prove that $nm = mn$.

Since $n \in N$, $\bar{n}^1 \in N$ ($\because N$ is normal subgroup of G)

and $m \in G$

we have $m(\bar{n}^1)\bar{m}^1 \in N$.

Also by closure in N

$$nm\bar{n}^1\bar{m}^1 \in N \quad \text{---} (1)$$

Since M is normal.

$$nm\bar{n}^1 \in M \quad (\because n \in G)$$

By closure in M,

$$nm\bar{n}^1\bar{m}^1 \in M \quad \text{---} (2).$$

From (1) & (2) we have

$$nm\bar{n}^1\bar{m}^1 \in M \cap N.$$

But $M \cap N = \{e\}$.

$\therefore nm\bar{n}^1\bar{m}^1 = e$

$\Rightarrow nm\bar{n}^1 = m$

$\Rightarrow nm = mn$

$\therefore$ Every element of M commutes with every element of N.

Quotient group:

Theorem: If H is a normal subgroup of G. The set $\frac{G}{H}$ of all cosets of H in G w.r.t coset multiplication is a group.

Proof: Given that H is a normal subgroup of G.

$\therefore$ for $a \in G$, $aH = Ha$.

$\therefore \frac{G}{H}$ is the set of all cosets of H in G.

Let $\frac{G}{H} = \{Ha / a \in G\}$.

for $a, b \in G$,

we have $Ha, Hb \in \frac{G}{H}$.

we define coset multiplication on $\frac{G}{H}$ as

$(Ha)\cdot(Hb) = Hab$

we prove that the operation is well defined

Let $Ha = Ha_1$ and $Hb = Hb_1$ in $\frac{G}{H}$.

$\therefore ea = a = h_1 a_1$ and $eb = b = h_2 b_1$ for some $h_2 \in H$.

~~for some $h_1 \in H$~~

Now $Hab = H(h_1 a_1)(h_2 b_1)$

$= Hh_1(a_1 h_2) b_1$

$= Hh_1(h_3 a_1) b_1$ ($\because H$ is normal, $a_1 H = Ha_1$ so that $a_1 h_2 = h_3 a_1$ ~~for some $h_3 \in H$~~)

$= H(h_1 h_3) a_1 b_1$

$= Ha_1 b_1$ ($\because h_1 h_3 \in H \Rightarrow H(h_1 h_3) = H$)

i.e., $Ha\,Hb = Ha_1 \cdot Hb_1$.

$\therefore$ coset multiplication is well defined.

(i) Closure prop: $Ha, Hb \in \frac{G}{H}$

$\Rightarrow Ha \cdot Hb \in \frac{G}{H}$.

Since $a, b \in G \Rightarrow ab \in G$ and

$Ha \cdot Hb = Hab \in \frac{G}{H}$.

(ii) Associative prop: $Ha, Hb, Hc \in \frac{G}{H}$

$\Rightarrow (Ha\,Hb)\,Hc = Ha(Hb\,Hc)$

Since $(Ha\,Hb)\,Hc = (Hab)\,Hc$

$= H(ab)c$

$= Ha(bc)$ ($\because G$ is a group)

$= Ha \cdot Hbc$

$= Ha(Hb \cdot Hc)$

Existence of right identity:

Let $Ha \in \frac{G}{H}$ $\exists\ He\ (=H) \in \frac{G}{H}$ such that

$Ha \cdot He = Hae$

$= Ha \quad (\because ae = a\ \forall\ a \in G)$

$\therefore$ Identity exists in $\frac{G}{H}$ and it is $He\ (=H)$

Existence of right inverse:

Let $Ha \in \frac{G}{H}$ $\exists\ Ha^{-1} \in \frac{G}{H}$; $a \in G \Rightarrow a^{-1} \in G$

such that $Ha \cdot Ha^{-1} = H(a\,a^{-1})$

$= He \quad (=H) \quad (\because a a^{-1} = e)$

$\therefore$ Every element of $\frac{G}{H}$ is invertible

and $(Ha)^{-1} = Ha^{-1}$.

$\therefore \frac{G}{H}$ is a group w.r.t coset multiplication.

Def: If G is a group and H is a normal subgroup of G, then the set $\frac{G}{H}$ of all cosets of H in G is a group w.r.t multiplication of cosets. It is called the quotient group or factor group of G by H.

The identity element of the quotient group $\frac{G}{H}$ is H

Theorem: If H is a normal subgroup of a finite group G then $O\left(\frac{G}{H}\right) = \frac{O(G)}{O(H)}$

Proof: $O\left(\frac{G}{H}\right)$ = number of distinct cosets of H in G

= the index of H in G

$= [G : H]$

$= \frac{\text{number of elements in } G}{\text{number of elements in } H}$.

$= \frac{O(G)}{O(H)}$.

Theorem → Every quotient group of an abelian group is abelian.

proof: Let H be a subgroup of an abelian group G. But every subgroup of an abelian group is normal.

So H is a normal subgroup of G.

Let $\frac{G}{H}$ be the quotient group of G by H.

for $a, b \in G$, $ab = ba$ ($\because$ G is abelian)

$\therefore Ha, Hb \in \frac{G}{H}$

Now $(Ha)(Hb) = H(ab)$

$= H(ba)$

$= Hb\ Ha$.

$\therefore \frac{G}{H}$ is abelian

Let P_n be the symmetric group on 'n' symbols. prove that A_n is a normal subgroup of P_n.

proof: Let $\alpha \in P_n$ and $\beta \in A_n$

then β is an even permutation. and α may be odd or even.

Now we have to prove that $\alpha\beta\alpha^{-1}$ is an even permutation.

— If α is even then α^{-1} is also even.

Now $\alpha\beta$ is even and $\alpha\beta\alpha^{-1}$ is even.

— If α is odd, then α^{-1} is also odd.

Now $\alpha\beta$ is odd and $\alpha\beta\alpha^{-1}$ is even.

$\therefore \alpha \in P_n, \beta \in A_n \Rightarrow \alpha\beta\alpha^{-1} \in A_n$.

$\therefore A_n$ is a normal subgroup of P_n.

→ Show that $H = \{1, -1\}$ is a normal subgroup of the group of non-zero real numbers under $\times$.

Sol^{n}: Let $G = \mathbb{R} - \{0\}$ be a group w.r.t $\times$.

Clearly $H \subset G$ and H is a subgroup of G.

for $x \in G$, $x \cdot 1 \cdot x^{-1} = x \cdot \frac{1}{x} = 1$

and $x(-1)x^{-1} = -x \cdot \frac{1}{x} = -1$

$\therefore$ for $h \in H$ and $x \in G$

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

$\therefore H$ is a normal subgroup of G.

Note: Suppose H is the only subgroup of finite order 'm' in the group G. Then H is a normal subgroup of G.

Show that $H = \{1, -1\}$ is a normal subgroup of a group $G = \{1, -1, i, -i\}$ under $\times$. Also write the composition table for the quotient group $\frac{G}{H}$.

Sol^{n}: Clearly $H \subset G$ and H is a subgroup of G.

Since 1 is the identity element in H.

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

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

$iH = \{i, -i\}$, $-iH = \{-i, i\}$

Also $1H = H \cdot 1$

$(-1)H = H(-1)$.

$iH = H \cdot i$

$(-i)H = H(-i)$

$xH = Hx$ $\forall x \in G$.

$\therefore H$ is a normal subgroup of G.

$\therefore \frac{G}{H}$ is the quotient group of G by H.

Let $\frac{G}{H} = \{H, iH\}$.

composition table is:

	H	iH
H	H	iH
iH	iH	H

→ Show that $H = \{1, -1, i, -i\}$ is a normal subgroup of the group of non-zero complex numbers under x^n.

Sol^n: Let $G = \mathbb{C} - \{0\}$ be the given group w.r.t x^n.

Clearly $H \subset G$ and H is a subgroup of G.

for $z \in G$, $z \cdot 1 \cdot z^{-1} = z \cdot \frac{1}{z} = 1$,

$z(-1)z^{-1} = -z\frac{1}{z} = -1$

$z(i)z^{-1} = i$

$z(-i)z^{-1} = -i$.

and $h \in H$ and $z \in G$, $zhz^{-1} \in H$.

$\therefore$ H is a normal subgroup of G.

→ Every subgroup of a cyclic group is a normal subgroup.

proof: Every cyclic group is abelian group.

→ The quotient group of a cyclic group is cyclic.

proof: Let $G = \langle a \rangle$ be a cyclic group with generator a.

Let N be a subgroup of G.

Since G is abelian.

we take that N is normal in G.

W.K.T $\frac{G}{N} = \{Nx / x \in G\}$

Now $a \in G \Rightarrow Na \in \frac{G}{N}$

$\Rightarrow \langle Na \rangle \subseteq \frac{G}{N}$ ——— (1)

Also $Nx \in \frac{G}{N} \Rightarrow x \in G = \langle a \rangle$.

$\therefore x = a^n$ for some $n \in Z$.

$\therefore Nx = Na^n$

$= N(a.a.\ldots\ldots n \text{ times})$

When 'n' is +ve integer.

$= Na.Na.\ldots\ldots Na$ (n times)

$= (Na)^n$.

$\therefore$ we can prove that $Na = (Na)^n$ when $n = 0$ or n is +ve integer.

$Na \in \frac{G}{N} \Rightarrow N(a) \in \langle Na \rangle$

$\therefore \frac{G}{N} \subseteq \langle Na \rangle$ ——— (2)

from (1) & (2) we have $\frac{G}{N} = \langle Na \rangle$.

$\therefore \frac{G}{N}$ is a cyclic group.

Q: Let P_3 be the symmetric group on three symbols a, b, c and A_3 be the alternating group on three symbols a, b, c. Form the composition table for the quotient group $\frac{P_3}{A_3}$.

Soln: Let $P = \{a, b, c\}$

Let $P_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$.

where $f_1 = I$, $f_2 = (a\,b)$, $f_3 = (b\,c)$, $f_4 = (c\,a)$

$f_5 = (a\,b\,c)$ and $f_6 = (a\,c\,b)$.

Let A_3 = set of even permutations belonging to P_3.

i.e., $A_3 = \{f_1, f_5, f_6\}$

Clearly A_3 is a normal subgroup of P_3.

The elements of $\frac{P_3}{A_3}$ are the cosets of A_3 in P_3. (3

By Lagrange's theorem,

A_3 will have only two distinct cosets in P_3.

One is A_3 itself and other is $A_3 f_2$.

$(\because A_3 f_5 = A_3 f_6 = A_3 = A_3 f_1$

$A_3 f_2 = A_3 f_3 = A_3 f_4)$

The composition table for $\frac{P_3}{A_3}$ is:

	A_3	$A_3 f_2$
A_3	A_3	$A_3 f_2$
$A_3 f_2$	$A_3 f_2$	A_3

$\because (A_3 f_2)(A_3 f_2) = A_3 f_2 f_2$

$= A_3 f_1$

$= A_3$

2003 → If H is a subgroup of a group G such that $x^2 \in H$ for every $x \in G$, prove that H is a normal subgroup of G.

Soln: Let $g \in G$, so that $g^{-1} \in G$.

then $(g^{-1})^2 \in H$ (by hyp).

$\Rightarrow g^{-2} \in H$

and $h^{-1} g^{-2} \in H \ \forall h \in H$. ($\because H$ is subgroup & $h^{-1} \in H$)

Since $gh \in G \Rightarrow (gh)^2 \in H$. (by hypothesis)

Now $(gh)^2 \in H$ and $h^{-1} g^{-2} \in H$

$\Rightarrow (gh)^2 h^{-1} g^{-2} \in H$. ($\because H < G$)

$\Rightarrow ghgh h^{-1} g^{-1} g^{-1} \in H$

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

$\Rightarrow ghgg^{-1} g^{-1} \in H$.

$\Rightarrow ghg^{-1} \in H \ \forall g \in G, h \in H$

($\because ge g^{-1} = gg^{-1} = e$)

Hence H is normal subgroup of G.

→ Let N be a normal subgroup of G. Show that $\frac{G}{N}$ is abelian iff $xyx^{-1}y^{-1} \in N$ for all $x, y \in G$.

Soln: Let $X, Y \in \frac{G}{N}$ then $X = Nx$, $Y = Ny$; for some $x, y \in G$.

$\frac{G}{N}$ is abelian $\Leftrightarrow XY = YX$ $\forall X, Y \in \frac{G}{N}$.

$\Leftrightarrow NxNy = NyNx$ $\forall x, y \in G$.

$\Leftrightarrow Nxy = Nyx$ $\forall x, y \in G$.

$\Leftrightarrow (xy)(yx)^{-1} \in N$ $\forall x, y \in G$

$\Leftrightarrow (xy)(x^{-1}y^{-1}) \in N$, $\forall x, y \in G$.

$\Leftrightarrow xyx^{-1}y^{-1} \in N$ $\forall x, y \in G$.

$ab^{-1} \in H \Leftrightarrow$ like this

→ If H is a subgroup of a group G such that $x^2 \in H$ for all $x \in G$. Prove that $\frac{G}{H}$ is abelian.

Soln: Given that H is a subgroup of G such that

$x^2 \in H$ $\forall x \in G$. ——— (1)

$\therefore$ H is a normal subgroup of G.

Now we have to prove that $\frac{G}{H}$ is abelian

W.K.T $\frac{G}{H}$ abelian $\Leftrightarrow xyx^{-1}y^{-1} \in H$ $\forall x, y \in G$.

Let $x, y \in G$,

$\therefore x^{-1}y \in G \Rightarrow (x^{-1}y)^2 \in H$ (by (1))

Also $x^2 \in H$ & $y^{-2} \in H$.

$\therefore x^2(x^{-1}y)^2y^{-2} \in H$ $(\because H \subseteq G)$

$\Rightarrow xx(x^{-1}y)(x^{-1}y)y^{-1}y^{-1} \in H$

$\Rightarrow x(xx^{-1})yx^{-1}(yy^{-1})y^{-1} \in H$

$\Rightarrow xeyx^{-1}ey^{-1} \in H$

$\Rightarrow xyx^{-1}y^{-1} \in H$ $\forall x, y \in G$.

$\therefore \frac{G}{H}$ is abelian

Conjugate elements:

If a and b are two elements of a group G, we say that 'a' is conjugate to 'b' denoted as $a \sim b$, if there exists some element $x \in G$ such that $a = x^{-1}bx$.

- If $a = x^{-1}bx$, then 'a' is called the transform of b by 'x'.
- If 'a' is conjugate to 'b' i.e., $a \sim b$ then this relation in G is called the relation of conjugacy.

Note: we also define conjugate elements as follows:

$a \sim b \Leftrightarrow a = xbx^{-1}$ for some $x \in G$

Ex: $(123) \sim (132)$ in S_3

$\underset{a}{(123)} \quad \underset{b}{(132)}$

Take $\theta = (23) \in S_3$

Then $\theta (132) \theta^{-1} = (23)(132)(23)$

$= (13)(13)$

$= (123)$

→ Show that the relation ($\sim$) of conjugacy is an equivalence relation on a group G.

Proof: Let $a, b, c \in G$

Reflexive: $a \sim a$, since $a = eae$

$= e^{-1}ae$, $e \in G$

Symmetric:

Let $a \sim b$ then $a = x^{-1}bx$, $x \in G$

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

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

$= ebe$

$= b$

$\therefore xax^{-1} = b$

$\Rightarrow b = (x^{-1})^{-1}ax^{-1}$; $x^{-1} \in G$

$\Rightarrow b \sim a$

Transitive: Let $a \sim b$ and $b \sim c$ then $a = x^{-1}bx$ and $b = y^{-1}cy$ for some $x, y \in G$.

$\Rightarrow a = x^{-1}(y^{-1}cy)x$ —

$= (yx)^{-1}c(yx)$; $yx \in G$

$\Rightarrow a \sim c$.

$\therefore$ The relation ($\sim$) of conjugacy is an equivalence relation on G.

Note: [i]. For $a \in G$, the equivalence class of 'a', denoted by $C(a)$ (or) $[a]$, is given by

$$C(a) = \{x \in G / x \sim a\}$$

$$= \{x \in G / x = y^{-1}ay, y \in G\}$$

$$\therefore C(a) = \{y^{-1}ay / y \in G\}.$$

This equivalence class of 'a' is also called the conjugate class of 'a'.

Since the conjugacy relation $\sim$ is an equivalence relation on G.

$\therefore$ It will partition G into disjoint equivalence classes, called classes of conjugate elements.

So $G = \bigcup_{a \in G} [a]$

i.e, G is expressible as the union of mutually disjoint conjugate classes.

Lemma:

If $f \in S_n$ be such that $f: i \to j$. Then $\theta f \theta^{-1}: \theta(i) \to \theta(j)$ for all $\theta \in S_n$.

proof: Let $\theta: i \to s$ and $j \to t$

Then $\theta^{-1}: s \to i$ and $t \to j$

$\therefore \theta f \theta^{-1}: s \xrightarrow{\theta^{-1}} i \xrightarrow{f} j \xrightarrow{\theta} t$.

Here we have applied right to left

Hence $\theta f \theta^{-1} : S \to t$

(or)

$$\boxed{\theta f \theta^{-1} : \theta(i) \to \theta(j)}$$

Rule: In order to compute $\theta f \theta^{-1}$: replace every symbol in f by its θ-image.

Ex: $\theta(123)\theta^{-1} = (\theta(1)\ \theta(2)\ \theta(3))$

If $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} \in S_5$

then $\theta(123)\theta^{-1} = (5\ 4\ 1)$

→ Find out all the conjugate classes of S_3.

Sol: $S_3 = \{I, (12), (23), (13), (123), (132)\}$

Now we write various conjugate classes in S_3 are:

$[I] = \{\theta I \theta^{-1} / \theta \in S_3\}$

$= \{I\}$

$[(12)] = \{\theta(12)\theta^{-1} / \theta \in S_3\}$

$= \{(\theta(1)\ \theta(2)) / \theta \in S_3\}$ (by lemma)

Here $[(12)]$ consists of all 2-cycles of S_3.

i.e, $[(12)] = \{(12), (13), (23)\}$.

Similarly $[(23)] = \{(12), (23), (13)\} = [(13)]$

Now $[(123)] = \{\theta(123)\theta^{-1} / \theta \in S_3\}$

$= \{(\theta(1)\ \theta(2)\ \theta(3)) / \theta \in S_3\}$

Here $[(123)]$ consists of all 3-cycles of S_3.

i.e, $[(123)] = \{(123), (132)\}$

Similarly $[(132)] = \{(123), (132)\}$

Hence all the distinct conjugate classes of S_3 are

$\{I\}, \{(12), (23), (31)\}, \{(123), (132)\}$

and their union is S_3.

The number of conjugate classes of S_3 is 3.

H.W → Find out all the conjugate classes of S_4.

Note: [1]. $C(e) = \{e\}$

where e is the identity element of the group G.

i.e, $C(e) = \{y^{-1}ey \mid y \in G\}$

$= \{e\}$.

[2]. If G is finite group then the number of distinct elements in $C(a)$ is denoted by C_a (or) $O(C(a))$.

[3]. In an abelian group G.

$C(a) = \{a\}$ $\forall a \in G$

$\because C(a) = \{x^{-1}ax \mid x \in G\}$

$= \{x^{-1}xa \mid x \in G\}$

$= \{a\}$ $\forall a \in G$.

$\therefore O(C(a)) = 1$

Normalizer of an element of a group:

If a is an element of a group G, then the normalizer of 'a' in G is the set of all those elements of G which commute with 'a'. The normalizer of 'a' in G is denoted by $N(a)$.

where $N(a) = \{x \in G \mid ax = xa\}$.

The normalizer of 'a' i.e, $N(a)$ is a subgroup of G.

Note: [1] If $e \in G$, $ex = xe = x$ $\forall x \in G$

$\Rightarrow N(e) = G$.

[2] If G is abelian group and $a \in G$

then $xa = ax$ $\forall x \in G$

$\therefore N(a) = G$

To prove f is 1-1:

$f(x^{-1}ax) = f(y^{-1}ay)$

$\Rightarrow N(a)\cdot x = N(a)\cdot y$ (by ②)

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

$\Rightarrow xy^{-1}a = axy^{-1}$ (by defn. of $N(a)$)

$\Rightarrow x^{-1}ax = y^{-1}ay$

$\therefore f$ is 1-1.

To prove f is onto:

for any $X \in \Sigma$.

$\Rightarrow X = N(a)\cdot g$; $g \in G$

$\Rightarrow X = f(g^{-1}ag)$ (by ②)

and $g^{-1}ag \in C(a)$.

$\therefore f$ is onto.

$\therefore$ there exists a one-to-one correspondence between $C(a)$ and Σ.

Since G is finite.

$\therefore$ Number of distinct elements in $C(a)$ = Number of distinct right cosets of $N(a)$ in G.

i.e. $o(C(a)) = o(\Sigma)$

= the number of distinct right cosets of $N(a)$ in G

= the index of $N(a)$ in G.

$= \frac{o(G)}{o(N(a))}$

$= i_G N(a)$.

$\therefore o(C(a)) = \frac{o(G)}{o(N(a))}$

→ If G is a finite group then C_a (or) $o[C(a)] = \frac{o(G)}{o(N(a))} = i_G(N(a))$

where $N(a)$ is the normalizer of a in G.

(or)

If G is a finite group, then the number of elements conjugate to 'a' in G is the index of the normalizer of 'a' in G.

Proof: Define a relation $\sim$ on G as follows:

$a \sim b \Leftrightarrow a = x^{-1}bx$ for some $x \in G$

Then $\sim$ is an equivalence relation on G and the equivalence class of 'a' is

$C(a) = \{x^{-1}ax / x \in G\}$.

which is the conjugate class of 'a'.

further more $G = \bigcup_{a \in G} C(a)$ ——— (1)

i.e, G is expressible as the union of mutually disjoint conjugate classes.

Let Σ denote the set of all distinct right cosets of $N(a)$ in G.,

where $N(a) = \{x \in G / xa = ax\}$.

Define a function $f : C(a) \to \Sigma$

as $f(x^{-1}ax) = N(a) \cdot x$, $x \in G$ ——— (2)

TO prove f is well defined: —

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

$\Rightarrow ax = xy^{-1}ay$

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

$\Rightarrow xy^{-1} \in N(a)$. ($\because N(a)$ is normalizer)

$\Rightarrow N(a)x = N(a)y$ ($\because N$ is subgroup)

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

$\therefore f$ is well defined.

Class equation of a group:

If G is a finite group then $o(G) = \sum_{a \in G} i_G(N(a))$

$$= \sum_{a \in G} \frac{o(G)}{o(N(a))}$$

where the sum runs over one element 'a' in each conjugate class.

Proof: Define a relation on G as follows:

$a \sim b \Leftrightarrow a = x^{-1}bx$ for some $x \in G$.

Then $\sim$ is an equivalence relation on G and the equivalence class of 'a' in G is $C(a) = \{x^{-1}ax / x \in G\}$ which is the conjugate class of 'a' in G.

Further more $G = \bigcup_{a \in G} C(a)$ ——— (1)

i.e, G = the union of mutually disjoint conjugate classes.

Since G is finite group.

∴ the number of distinct conjugate classes of G will be finite say k.

i.e, If $C(a_1), C(a_2), \ldots\ldots C(a_k)$ are the k distinct conjugate classes of G.

$\therefore G = C(a_1) \cup C(a_2) \cup \ldots\ldots \cup C(a_k)$.

i.e, the number of elements in G = the number of elements in $C(a_1)$ + the number of elements in $C(a_2)$ + ... + number of elements in $C(a_k)$.

(∵ two distinct conjugate classes have no common element)

$$\Rightarrow o(G) = \sum_{a \in G} o(C(a))$$

where the sum runs over one element 'a' in each conjugate class.

W.K.T $o(C(a)) = \frac{o(G)}{o(N(a))}$

$\therefore o(G) = \sum_{a \in G} \frac{o(G)}{o(N(a))}$

$= \sum_{a \in G} i_G(N(a))$

This equation is known as class equation of the finite group G.

→ verify the class equation for S_3.

Sol: $S_3 = \{ I, (12), (23), (13), (123), (132) \}$

If $G = S_3$ then $o(G) = 6$.

By definition, $N(a) = \{x \in G / xa = ax\}$

Now $N(I) = S_3$.

$N(12) = \{I, (12)\}$

Since $I \in S_3$, $I(12) = (12)I$

$(12) \in S_3$.

$(12)(12) = (12)(12)$

$(23) \in S_3$, $(23)(12) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$= (132)$

and $(12)(23) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$

$\therefore (23)(12) \neq (12)(23)$

Similarly $(13)(12) \neq (12)(13)$

$(123)(12) \neq (12)(123)$

$(132)(12) \neq (12)(132)$

$N[(123)] = \{I, (123), (132)\}$

$\therefore \sum_{a \in G} \frac{o(G)}{o(N(a))} = \frac{o(G)}{o(N(I))} + \frac{o(G)}{o[N(12)]} + \frac{o(G)}{o\{N[(123)]\}} = \frac{6}{6} + \frac{6}{2} + \frac{6}{3}$

$= 6 = o(G)$

Self-conjugate element of a group:

Def: $(G, \cdot)$ is a group and $a \in G$ such that $a = x^{-1}ax$ $\forall x \in G$.

Then 'a' is called self conjugate element of G.

A self-conjugate element is some times called an invariant element.

Here $a = x^{-1}ax$.

The centre of a group:

The set Z of all self conjugate elements of a group G is called the centre of the group.

i.e, $Z = \{x \in G / xx = xx \ \forall x \in G\}$.

→ The centre Z of a group G is subgroup of G.

→ The centre Z of a group G is normal subgroup of G.

proof: Given that Z is the centre of a group G.

i.e, $Z = \{x \in G / zx = xz \ \forall x \in G\}$.

Clearly Z is a subgroup of G.

Let $x \in G$, $z \in Z$. then $xzx^{-1} = (xz)x^{-1}$

$= (zx)x^{-1}$ (by defn of Z)

$= zxx^{-1}$

$= ze$

$= z \in Z$

$\therefore xzx^{-1} \in Z$, $\forall x \in G$.

$\therefore$ Z is a normal subgroup of G.

→ $a \in Z$ iff $N(a) = G$.

∴ If G is finite, $a \in Z$ iff $O(cl(a)) = O(G)$.

proof: Let $a \in Z$ then by defn of Z we have $ax = xa$ $\forall x \in G$.

Also $N(a) = \{ x \in G / ax = xa \}$.

Now $a \in Z \Leftrightarrow ax = xa \ \forall x \in G$ (by defn of Z)

$\Leftrightarrow x \in N(a) \ \forall x \in G$ (by defn of $N(a)$)

$\Leftrightarrow N(a) = G$.

($\because N(a) \subseteq G$ and each element of G is in $N(a)$)

If the group G is finite,

then $a \in Z \Leftrightarrow N(a) = G$

$\Leftrightarrow o(G) = o(N(a))$

$\therefore$ If the group G is finite then $a \in Z$

$\Leftrightarrow o(G) = o(N(a))$.

Theorem Second form of class equation:

If G is a finite group then

$$o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o(N(a))}$$

where Z being the centre of the group G.

and the summation runs over one element a in each conjugate class containing more than one element.

Proof: The class equation of finite group G is

$$o(G) = \sum_{a \in G} \frac{o(G)}{o(N(a))}$$

$Z \subseteq G$.

(or)

$$o(G) = \sum_{a \in Z} \frac{o(G)}{o(N(a))} + \sum_{a \notin Z} \frac{o(G)}{o(N(a))} \quad \text{---(1)}$$

($\because G = Z \cup G \setminus Z$)

$G = Z \cup G \setminus Z$

WKT If G is finite, $a \in Z \Leftrightarrow o(N(a)) = o(G)$.

i.e $a \in Z \Leftrightarrow \frac{o(G)}{o(N(a))} = 1$ i.e $o(a) = 1$

$\Leftrightarrow$ the conjugate class of 'a' in G contains only one element

i.e, the number of ... each having only one element is equal to $o(Z)$.

$$\therefore o(Z) = \sum_{a \notin Z} \frac{o(G)}{o(N(a))}$$

$$\therefore (1) \Rightarrow o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o(N(a))}$$

The equivalent forms of class equation of a finite group G are:

$$o(G) = \sum_{a \in G} \frac{o(G)}{o(N(a))},$$

$$o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o(N(a))},$$

$$o(G) = o(Z) + \sum_{a \notin Z} i_G(N(a)),$$

$$o(G) = o(Z) + \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$$

→ If $o(G) = p^n$ where p is a prime number, then the centre $Z \neq \{e\}$. i.e, $o(Z) > 1$.

Proof:

The class equation of a finite group G is

$$o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o(N(a))} \quad \text{---(1)}$$

where the summation runs over one element a in each conjugate class containing more than one element.

Now $\forall a \in G$, $N(a)$ is a subgroup of G.

∴ By Lagrange's theorem $o(N(a))$ divides $o(G)$ i.e, $\frac{o(G)}{o(N(a))}$

Also $a \notin Z \Rightarrow N(a) \neq G$.

$\Rightarrow o(N(a)) < o(G) = p^n$.

$\therefore$ If $a \notin Z$ then $O(N(a))$ must be of the form p^k where $1 \le k \le n$.

$$\therefore \frac{O(G)}{O(N(a))} = \frac{p^n}{p^k} = p^{n-k}$$

$\Rightarrow p$ divides $\frac{O(G)}{O(N(a))}$

$\Rightarrow p$ divides $\sum_{a \notin Z} \frac{O(G)}{O(N(a))}$ ——— (2)

Also p divides $O(G) = p^n$ ——— (3)

From (2) & (3),

p divides $\left[O(G) - \sum_{a \notin Z} \frac{O(G)}{O(N(a))} \right]$

$= O(Z)$ (by (1))

$\therefore p$ divides $O(Z)$

i.e., $\frac{O(Z)}{p}$

Since p is prime,

$O(Z)$ is atleast 2

$\therefore O(Z) > 1$

i.e., $Z \neq \{e\}$.

2002 → If $O(G) = p^2$, where p is prime number then G is abelian.

Proof: Since $O(G) = p^2$, p is prime

$\therefore Z \neq \{e\}$ i.e., $O(Z) > 1$

By Lagrange's theorem

$O(Z)$ divides $O(G) = p^2$

i.e., $\frac{O(G)}{O(Z)}$ i.e., $\frac{p^2}{O(Z)}$

$\therefore O(Z) = p^2$ or p.

Case(i) Let $O(Z) = p^2$

then $O(Z) = O(G) \Rightarrow Z = G$ ($\because Z < G$)

Since $\forall a \in G \Rightarrow a \in Z \Rightarrow ax = xa \quad \forall x \in G$

$\therefore G$ is abelian.

Case(ii): Let $O(Z) = p$

Since $O(G) = p^r > p$

i.e, $p < p^r$

i.e, $O(Z) < O(G)$

$\therefore Z$ is proper subgroup of G.

So that there exists some $a \in G$ such that $a \notin Z$

w.k.t $N(a) = \{ x \in G / xa = ax \}$ is a subgroup of G and $a \in N(a)$.

Also $a \in Z \Rightarrow x \in N(a)$

$\because Z \subseteq N(a)$.

$a \notin Z \Rightarrow O(Z) < O(N(a))$

$\Rightarrow p < O(N(a))$

By Lagrange's theorem

$O(N(a))$ divides $O(G) = p^r$ i.e, $\frac{O(G)}{O(N(a))}$

and $O(N(a)) > p$.

$\therefore O(N(a)) = p^r \Rightarrow O(N(a)) = O(G)$.

$\Rightarrow N(a) = G \quad (\because N(a) \subseteq G)$.

$\Rightarrow x \in N(a) \quad \forall x \in G$.

$\Rightarrow a \in Z$.

which is a contradiction.

$\therefore O(Z) = p$ is impossible.

$\therefore O(Z) = p^r$.

In this case we have already proved that G is abelian.

→ If G is a non-abelian group of order p^3, where p is prime number, show that $O(Z) = p$.

Sol^{n}: Since, $O(G) = p^3$, p is prime.

$\therefore Z \neq \{e\}$, i.e., $O(Z) > 1$ ——— (1)

By Lagrange's theorem

$O(Z)$ divides $O(G) = p^3$.

i.e., $\frac{O(G)}{O(Z)} = \frac{p^3}{O(Z)}$

$\therefore O(Z) = 1$ or p or p^2 or p^3.

By (1),

$O(Z) = p$ or p^2 or p^3.

Let, if possible $O(Z) = p^2$

then $O\left(\frac{G}{Z}\right) = \frac{O(G)}{O(Z)} = \frac{p^3}{p^2} = p$.

$\therefore \frac{G}{Z}$ is cyclic.

(∵ a group of prime order is cyclic).

$\therefore G$ is abelian.

(∵ if $\frac{G}{Z}$ is cyclic then G is abelian).

which is contradiction to hyp.

$\therefore O(Z) \neq p^2$.

Let, if possible $O(Z) = p^3$

$= O(G)$

$\Rightarrow Z = G$ (∵ $Z \subset G$).

$\forall a \in G \Rightarrow a \in Z$.

$\Rightarrow ax = xa \ \forall x \in G$

$\Rightarrow G$ is abelian.

which is contradiction to hyp.

$\therefore O(Z) \neq p^3$.

$\therefore O(Z) = p$

Sct - VI

Homomorphisms, Isomorphisms of Groups:

→ Let $(G, \cdot)$, $(G', *)$ be two groups.

A mapping $f: G \to G'$ is called a homomorphism, if

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

In other words, a homomorphism preserves the compositions in the groups G and G'.

However, if we are not specific about the compositions of the groups G and G', we say that a mapping $f: G \to G'$ is a homomorphism, if

$$f(ab) = f(a) \cdot f(b) \quad \text{---------} (1)$$
$$\forall a, b \in G$$

Note: In equation (1), the product ab on LHS takes place in G, while the product $f(a).f(b)$ on RHS takes place in G'.

→ If $f: G \to G'$ is a homomorphism and onto then the group G' is said to be a homomorphic image of a group G or f is said to be a homomorphism G onto G'. we write this as $f(G) = G'$. In this case write $G \simeq G'$.

(read as G is homomorphic to G')

— Homomorphism onto sometimes called as ephimorphism.

→ Let G, G' be two groups. If $f: G \to G'$ is homomorphism and one-one then 'f' is called isomorphism from $G \to G'$.

→ If $f: G \to G'$ is homomorphism, one-one and onto then G' is called isomorphic image of G (or) G is isomorphic to G' and we write $G \cong G'$.

Note: If the group G is finite, then G can be isomorphic to G', only if G' is also finite and the number of elements in G is equal to the number of elements in G'.

otherwise there will exist no mapping from G to G' which is one-one and onto.

→ A homomorphism of a group G into itself is called an endomorphism.

→ An isomorphism of a group into itself is called an automorphism.

1-1 homomorphism = Isomorphism

1-1 Endomorphism = Automorphism.

Examples:

Let $G=(\mathbb{Z},+)$ and $G'=\{2^n / n\in\mathbb{Z}\}$. where G' is a group w.r.t $\times^n$.

Now we define a mapping, $f: G\to G'$ such that

$$f(n)=2^n \quad \forall n\in\mathbb{Z}.$$

Now for all $n_1, n_2 \in G$

$$\Rightarrow n_1+n_2\in G \text{ and } f(n_1)=2^{n_1},\ f(n_2)=2^{n_2}$$

Now we have

$$f(n_1+n_2) = 2^{n_1+n_2} \quad (\text{by def}^n)$$
$$= 2^{n_1}\cdot 2^{n_2}$$
$$= f(n_1)\cdot f(n_2)$$

$\therefore f(n_1+n_2) = f(n_1)\cdot f(n_2) \quad \forall n_1, n_2 \in G.$

$\therefore f$ is homomorphism.

To show f is 1-1:

Let $n_1, n_2 \in G$. then we have $f(n_1)=f(n_2)$.

$$\Rightarrow 2^{n_1}=2^{n_2}$$
$$\Rightarrow n_1=n_2$$

$\therefore f$ is 1-1.

$\therefore f$ is an isomorphism.

→ $G=\mathbb{R}^+$ is a group under $\times^n$ and $G'=\mathbb{R}$ is a group under $+^n$.

Sol^n: Now we define a mapping, $f: G\to G'$.

Such that $f(x) = \log_{10} x$, $\forall x \in G$.

Now for all $x_1, x_2 \in G \Rightarrow x_1 \cdot x_2 \in G$ and $f(x_1) = \log_{10} x_1$

$f(x_2) = \log_{10} x_2$

Now we have

$$f(x_1 \cdot x_2) = \log_{10}(x_1 \cdot x_2) \quad \text{(by defn)}$$
$$= \log_{10} x_1 + \log_{10} x_2$$
$$= f(x_1) + f(x_2)$$

$\therefore f$ is homomorphism.

To show f is 1-1:

we have $f(x_1) = f(x_2)$. $\forall x_1, x_2 \in G$:

$\Rightarrow \log_{10} x_1 = \log_{10} x_2$

$\Rightarrow x_1 = x_2$

$\therefore f$ is 1-1

$\therefore f$ is isomorphism.

To show f is onto:

Let $y \in G' = \mathbb{R}$.

$\therefore 10^y$ is a +ve real number.

$\Rightarrow 10^y \in G = \mathbb{R}^+$.

$$\therefore f(10^y) = \log_{10} 10^y$$
$$= y \log_{10} 10$$
$$= y(1)$$
$$= y$$

$\therefore f(10^y) = y$.

$\therefore$ for every $y \in G'$, $\exists\ 10^y \in G$ such that $f(10^y) = y$.

$\therefore f$ is onto.

G' is isomorphic image of G.

Properties of homomorphism:

Theorem Let $(G, \cdot)$, $(G', \cdot)$ be two groups. Let f be a homomorphism from G into G' then

(i) $f(e) = e'$ where 'e' is the identity in G and e' is the identity in G'.

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

Proof: (i) $f(e) = f(ee)$

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

$\Rightarrow f(e).f(e) = e'f(e)$ ($\because$ f is homomorphism and $e', f(e) \in G'$)

$\Rightarrow f(e) = e'$ (By RCL in G').

(ii) Let $a \in G \Rightarrow a^{-1} \in G$ and $a a^{-1} = e$.

Now we have

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

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

$= f(e)$

$= e'$ where $f(a), f(a^{-1}), f(e) \in G'$

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

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

Theorem (2) If f is a homomorphism from a group $(G, \cdot)$ into $(G', \cdot)$ then $(f(G), \cdot)$ is a subgroup of G'.

Proof: By defn $f(G) = \{f(a) / a \in G\}$ and $f(G) \subseteq G'$

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

$\therefore \exists\ a, b \in G$ such that $f(a) = a'$ & $f(b) = b'$.

Now $a'(b')^{-1} = f(a).[f(b)]^{-1} = f(a).f(b^{-1})$

$= f(ab^{-1})$ ($\because$ f is homo.)

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

$\therefore a'(b')^{-1} \in f(G)$ $\forall a', b' \in f(G)$

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

i.e, the homomorphic image of the group G

is a subgroup of G'.
i.e, the homomorphic image of a group is a group.

Theorem① Every homomorphic image of an abelian group G is abelian.

proof: Let $(G,\cdot)$ be an abelian group. and $(G',\cdot)$ be a group.
Let $f: G \to G'$ be a homomorphism and onto.
$\therefore G'$ is the homomorphic image of G.
i.e $G' = f(G)$.
Let $a', b' \in G'$
$\therefore \exists$ elements $a, b \in G$ such that $f(a) = a'$ & $f(b) = b'$.
Since G is abelian.
$\therefore ab = ba$.
Now $a'b' = f(a)f(b)$
$= f(ab)$
$= f(ba)$
$= f(b)\cdot f(a)$
$= b'a'$
$\therefore a'b' = b'a' \quad \forall a', b' \in G'$
$\therefore G'$ is an abelian.

Note: The converse of the above theorem need not be true
i.e, If the homomorphic image of a group G is abelian.
then the group need not be abelian.

Ex: S_3 is non-abelian group.
A_3 is normal subgroup of S_3.
The quotient group $\frac{S_3}{A_3}$ is a homomorphic image of S_3
Now $\frac{S_3}{A_3}$ is of order 2 and is abelian.

Note: Even if f is an isomorphism:
If substitute 'isomorphism' for homomorphism in Theorem① and it is true. The same proof holds

(ii) Substitute 'isomorphism' for homomorphism in Theorem (2) and it is true. The same proof holds.

(iii) Substitute isomorphism onto for homomorphism onto in Theorem (3) and it is true. The same proof holds. The converse of the theorem is ~~not~~ true.

Theorem: Let G be a group and G' be a non-empty set. If there exists a mapping f from G onto G' such that $f(ab)=f(a)\cdot f(b)$ for $a,b\in G$ then G' is a group.

Proof: $f: G \to G'$ is onto such that $f(ab) = f(a)\cdot f(b)$ $\forall a,b\in G$.

TO prove that G' is a group.

(i) Closure prop:

Let $a', b' \in G'$.

Since f is onto, $\exists\ a,b\in G$ such that

$$f(a)=a' \ \&\ f(b)=b'.$$

Also $ab\in G \Rightarrow f(ab)\in G'$.

$$\therefore a'b' = f(a)\,f(b) = f(ab)\in G'$$

$$\therefore a'b'\in G'.$$

(ii) Asso. prop:

Let $a', b', c' \in G'$.

Since f is onto, $\exists\ a,b,c\in G$ such that

$f(a)=a'$, $f(b)=b'$, $f(c)=c'$.

Now $a'(b'c') = \big(f(a)\cdot f(b)\big)\cdot f(c)$

$= f(ab)\cdot f(c)$ by def^n

$= f[(ab)c]$

$= f[a(bc)]$ $(\because G$ is group$)$

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

$= f(a)\,[f(b)\cdot f(c)]$

$= a'(b'c')$

$\therefore G'$ is Asso.

Existence of left identity:

Let $a' \in G'$.

Let e be the identity element in G.

Since f is onto,

$\therefore f(e) = e' \in G'$, $\exists\, a \in G$ such that $f(a) = a'$.

Now $e'a' = f(e)\,f(a)$

$= f(ea)$

$= f(a)$ $\quad (\because ea = a \;\forall\, a \in G)$

$= a'$.

$\therefore e'a' = a'$

$\therefore$ Identity exists in G' and it is $f(e) = e'$.

Existence of left inverse:

Let $a' \in G'$, $\exists\, a \in G$ such that $f(a) = a'$.

$\therefore a^{-1} \in G$ and $f(a^{-1}) \in G'$.

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

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

$= f(e)$

$= e'$.

$\therefore f(a^{-1})\,a' = e'$

$\therefore f(a^{-1})$ is the inverse of a' in G'.

$\therefore$ Every element of G' is invertible.

$\therefore G'$ is a group.

Note: When f is a one-one mapping from G into G', this theorem is not true.

Kernel of a Homomorphism:

Let G & G' be two groups, $f: G \to G'$ be a homomorphism then the set 'K' of all those elements of G whose image is the identity element e' of G' is called the kernel of the homomorphism 'f'.

i.e., Kernel $f = \{ x \in G \mid f(x) = e' \} = K$.

Sometimes Kernel f is written as Ker f.

Note: If $e \in G$ then $f(e) = e'$.
i.e, $e \in \ker f$.
$\therefore \ker f$ is non-empty.

Ex(1): The function $f: (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$ such that $f(a) = \log_a x \ \forall x \in \mathbb{R}^+$ is a homomorphism.
'0' is the identity element in $\mathbb{R}$,
$f(1) = \log_a 1 = 0$ (identity in $\mathbb{R}$)
$\therefore$ 1 is the only element with this property.
$\therefore \ker f = \{1\}$.

Ex(2): The function $f: (\mathbb{R}, +) \to (\mathbb{R}^+, \times)$ defined as $f(x) = a^x$; $a > 0$ and $a \neq 1$. and its homomorphism.
$f(0) = a^0 = 1$ (identity in $\mathbb{R}^+$)
$\therefore$ 0 is the only element with this property.
$\therefore \ker f = \{0\}$.

Ex(3): Let $G = I$ is a group w.r.t $+^n$.
$G' = \{1, -1\}$ is a group w.r.t $\times^n$.
Define $f: G \to G'$ as follows:
$f(n) = 1$, n is even
$= -1$, n is odd.
1 is the identity element in G'.
To prove f is homomorphism:
Let $n_1, n_2 \in G$ then we have the following possibilities:
Case(i): Both n_1 and n_2 are even.
$\therefore n_1 + n_2$ is even.
$\therefore f(n_1) = 1$, $f(n_2) = 1$
$\therefore f(n_1 + n_2) = 1$ ($\because n_1 + n_2$ is even).
$= 1 \cdot 1$
$= f(n_1) \cdot f(n_2)$

Case(ii): One of n_1, n_2 is even and other is odd.

Let n_1 be even and n_2 be odd.

$\therefore n_1+n_2$ is odd.

$\therefore f(n_1)=1$, $f(n_2)=-1$

Now $f(n_1+n_2)=-1$,

$= 1\cdot(-1)$

$= f(n_1)\cdot f(n_2)$.

Case(iii): Both n_1 & n_2 are odd.

$\therefore n_1+n_2$ is even.

$\therefore f(n_1)=-1$, $f(n_2)=-1$

Now $f(n_1+n_2)=+1$

$=(-1)(-1)$

$= f(n_1)f(n_2)$

$\therefore f$ is a homomorphism from $G \to G'$.

$\therefore \ker f = \{n \mid n \text{ is even}\}$.

2008

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

Proof: Let e be the identity element in G and e' be the identity element in G' and $f: G \to G'$ is a homomorphism.

Let $K = \ker f$ then $K = \{x \in G \mid f(x) = e'\}$.

Since $e \in G$.

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

$\therefore K$ is non-empty subset of G.

Let $a, b \in K$ then $f(a)=e'$, $f(b)=e'$.

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

$= f(a)[f(b)]^{-1}$

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

$= e'\cdot e'$

$= e'$.

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

$\therefore ab^{-1} \in K$.

$\therefore K$ is a subgroup of G.

Let $x \in G$

$\therefore f(xax^{-1}) = f(x)\, f(a)\, [f(x)]^{-1}$

$= f(x) \cdot e' [f(x)]^{-1}$

$= f(x) [f(x)]^{-1}$

$= e'$

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

$\therefore xax^{-1} \in K$.

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

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

(or)

If $f: G \to G'$ is a homomorphism onto then $\ker f = \{e\}$.

$\Leftrightarrow$ f is 1-1.

Proof: Let $f: G \to G'$ be a homomorphism and onto.

Let e, e' be the identity elements in G & G'.

Let K be the kernel of f.

$\therefore K = \{x \in G / f(x) = e'\}$

Suppose that $f: G \to G'$ is isomorphism. then

f is 1-1

To prove $K = \{e\}$.

Let $a \in K$

$\therefore f(a) = e'$

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

$\Rightarrow a = e$ ($\because f$ is 1-1)

$\therefore e$ is the identity element in G.

which belongs to K.

$\therefore K = \{e\}$.

Converse

Suppose that $K = \{e\}$.

Let $a, b \in G$.

Now we have $f(a) = f(b)$

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

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

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

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

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

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

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

$\Rightarrow ae = b$

$\Rightarrow a = b$

$\therefore f$ is 1-1

$\therefore f$ is an isomorphism from G to G'.

Theorem → Let f be a homomorphism from a group G onto a group G'. Let $\ker f = K$.
Let 'a'' be a given element of G such that $f(a) = a' \in G'$
Then the set of all those elements of G which have the image a' in G' is the coset Ka of K in G.

Proof: Let $f: G \to G'$ be homomorphism & onto.
Let e be the identity element in G and e' be the identity element in G'.
Let $\ker f = K$ then $K = \{x \in G \mid f(x) = e'\}$
Let $a \in G$ such that $f(a) = a' \in G'$.

$$f^{-1}(a') = \{x \in G \mid f(x) = a'\} = T \text{ (say)}.$$

Now to prove that $f^{-1}(a') = Ka$

Let $y \in Ka$. Then $y = ka$ for some $k \in K$.

$\therefore f(y) = f(ka)$

$= f(k) f(a)$ $\quad (\because k \in K \Rightarrow f(k) = e')$

$= e' f(a)$

$= f(a)$

$= a'$

$\therefore f(y) = a'$

$\Rightarrow y \in f^{-1}(a')$.

$\because y \in Ka \Rightarrow y \in f^{-1}(a')$

$\therefore Ka \subseteq f^{-1}(a')$ — (1)

Let $x \in f^{-1}(a')$ then $f(x) = a'$.

Now we have

$$f(xa^{-1}) = f(x)\, f(a^{-1})$$
$$= f(x)[f(a)]^{-1}$$
$$= a'(a')^{-1}$$
$$= e' \quad (\because f(a)\cdot[f(a)]^{-1} = e')$$

$\therefore f(xa^{-1}) = e'$

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

$\Rightarrow (xa^{-1})a \in Ka$

$\Rightarrow x \in Ka$.

$\therefore x \in f^{-1}(a') \Rightarrow x \in Ka$

$\Rightarrow f^{-1}(a') \subseteq Ka$ — (2)

from (1) & (2), we have

$$f^{-1}(a') = Ka.$$

Theorem: Let G be a group and N be a normal subgroup of G. Let f be a mapping from $G \to \frac{G}{N}$ defined by $f(x) = Nx$ for $x \in G$. Then f is a homomorphism of G onto $\frac{G}{N}$ and $\ker f = N$.

Proof: Let $f: G \to \frac{G}{N}$ such that $f(x) = Nx$ $\forall x \in G$.

To show f is onto:

Let $Nx \in \frac{G}{N}$ then $x \in G$.

$\therefore f(x) = Nx$.

$\therefore f$ is onto.

To show f is homomorphism:

Let $a, b \in G \Rightarrow ab \in G$.

Now we have

$$f(ab) = N(ab) \quad \forall ab \in G \text{ (by defn)}$$
$$= Na \cdot Nb. \quad (\because N \text{ is normal})$$
$$= f(a)\cdot f(b)$$

$\because f$ is homomorphism from $G \to \frac{G}{N}$ and onto.

i.e, f is homomorphism of G onto $\frac{G}{N}$.

i.e, every quotient group of a group is a homomorphic image of the group.

Now to prove $\ker f = N$.

Let K be kernel of this homomorphism f.

The identity of the quotient group $\frac{G}{N}$ is the coset N.

$\therefore K = \{ y \in G / f(y) = N \}$.

Let $k \in K \Leftrightarrow f(k) = N$.

$\Leftrightarrow Nk = N$ ($\because$ by defn of f i.e, $f(x) = Nx \ \forall x \in G$)

$\Leftrightarrow k \in N$.

($\because a \in H \Leftrightarrow Ha = H$)

$\therefore K = N$.

i.e, $\ker f = N$.

Note: The mapping $f: G \to \frac{G}{N}$ such that $f(x) = Nx \ \forall x \in G$ is called Natural (or) Canonical homomorphism.

Fundamental theorem on Homomorphism of groups:

Every homomorphic image of a group G is isomorphic to some quotient group of G.

(or)

If f is a homomorphism from a group G onto a group G', then $\frac{G}{\ker f}$ (i.e, $\frac{G}{K}$) is isomorphic with G'.

(or)

If $f: G \to G'$ is a homomorphism and onto with kernel K, then prove that $\frac{G}{K} \cong G'$.

Proof: By defn of kernel f is

$K = \{ x \in G / f(x) = e' ; e' \text{ is the identity element in } G' \}$

W.K.T K is a normal subgroup of G.

$\therefore$ the quotient group $\frac{G}{K}$ is defined.

where $\frac{G}{K} = \{ Ka / a \in G \}$

Given that the mapping $f: G \to G'$ is homomorphism and onto.

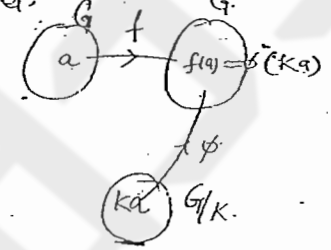
$\Rightarrow f(a) \in G' \ \forall a \in G$.

Now we shall prove that $\frac{G}{K} \cong G'$

i.e, G' is isomorphic image of $\frac{G}{K}$.

Define a mapping $\phi: \frac{G}{K} \to G'$ such that

$\phi(Ka) = f(a) \ \forall a \in G$.



(i) Now we shall show that ϕ is well defined:

for $a, b \in G$; $Ka, Kb \in \frac{G}{K}$

we have $Ka = Kb$

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

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

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

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

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

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

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

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

$\Rightarrow \phi(Ka) = \phi(Kb)$ (by defn)

$\therefore \phi$ is well defined.

(ii) To prove ϕ is 1–1

for $a, b \in G$, $Ka, Kb \in \frac{G}{K}$.

Now we have $\phi(Ka) = \phi(Kb)$

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

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

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

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

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

$\Rightarrow Ka = Kb.$

$\therefore \phi$ is 1-1

(iii) To prove that ϕ is onto:

Let $x \in G'$

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

$\therefore \exists\ a \in G$ such that $f(a) = x.$

$\therefore Ka \in \frac{G}{K}$ and $\phi(Ka) = f(a) \quad \forall a \in G.$

$= x.$

$\therefore \phi(Ka) = x \quad \forall a \in G.$

$\therefore \phi$ is onto.

(iv) To prove ϕ is homomorphism:

for $a, b \in G$, $Ka, Kb \in \frac{G}{K}$.

Now we have

$\phi[(Ka)(Kb)] = \phi(Kab)$ ($\because K$ is normal)

$= f(ab)$ ($\because$ by defn)

$= f(a)f(b)$

$= \phi(Ka)\,\phi(Kb).$

$\therefore \phi[(Ka)(Kb)] = \phi(Ka).\phi(Kb).$

$\therefore \phi$ is homomorphism.

$\therefore \phi$ is an isomorphism from $\frac{G}{K}$ onto G'.

i.e, G' is an isomorphic image of $\frac{G}{K}$.

i.e, $\frac{G}{K} \cong G'.$

Problems:

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

Sol^{n}: $f: G \to G$ such that $f(x) = x^2 \; \forall x \in G$.

— is a homomorphism.

Let $x, y \in G \Rightarrow xy \in G$.

$\therefore f(x) = x^2$, $f(y) = y^2$, $f(xy) = (xy)^2$

Since f is homomorphism,

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

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

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

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

$\Rightarrow yx = xy$

$\therefore G$ is abelian.

⟶ Let G be a x^{ve} group and $f: G \to G$ such that $a \in G$, $f(a) = a^{-1} \; \forall \; a$. Prove that f is 1–1 and onto. Also prove that f is homomorphism iff G is commutative.

Sol^{n}: $f: G \to G$ is a mapping such that $f(a) = a^{-1}$ for $a \in G$.

(i) To show f is 1–1 :-

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

Now we have

$f(a) = f(b)$

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

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

$\Rightarrow a = b$

$\therefore f$ is 1–1.

(ii) To prove f is onto:

Let $a \in G$.

$\therefore a^{-1} \in G$ such that $f(a^{-1}) = (a^{-1})^{-1} = a$

$\therefore f$ is onto.

(iii) Suppose f is a homomorphism.

for $a, b \in G \Rightarrow ab \in G$.

$\therefore f(a) = a^{-1}$, $f(b) = b^{-1}$ and $f(ab) = (ab)^{-1}$

Since f is homomorphism.

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

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

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

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

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

$\Rightarrow ab = ba$.

$\therefore G$ is abelian.

Suppose G is abelian.

for $a, b \in G$

Now we have

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

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

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

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

$\therefore f$ is homomorphism.

$\longrightarrow$ If $f: G \to G'$ is defined by $f(x) = 1$; $x > 0$

$= -1$; $x < 0$.

where G = set of non-zero real numbers and $G' = \{1, -1\}$ are groups.

Prove that f is a homomorphism. and find kernel.

Sol^n: Clearly $G = R - \{0\}$.

$G' = \{1, -1\}$ are groups w.r.t $\times$.

and identity in G' is 1.

Let $x, y \in G$ then $f(x), f(y) \in G'$.

(i) Let $x > 0$, $y > 0$

$\Rightarrow xy > 0$

$\therefore f(x) = 1$, $f(y) = 1$ & $f(xy) = 1$

Now $f(xy) = 1 = 1 \cdot 1 = f(x) \cdot f(y)$.

(ii) Let $x<0,\ y<0$

$\Rightarrow xy>0$

$\therefore f(x)=-1,\ f(y)=-1$ and $f(xy)=1$

NOW $f(xy)=1$

$=(-1)(-1)$

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

(iii) Let $x>0,\ y<0$ (or $x<0,\ y>0$)

$\Rightarrow xy<0$

$\therefore f(x)=1,\ f(y)=-1$ & $f(xy)=-1$

NOW $f(xy)=-1$

$=(1)(-1)$

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

$\therefore$ from (i), (ii), (iii)

we have

$\forall x, y \in G$

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

$\therefore f$ is homomorphism from $G \to G'$.

Kernel $f=\{x\in G / f(x)=1,$ identity in $G'\}$.

$=\{x\in G / x>0\}$.

$\longrightarrow$ Let $(G,+)$ is a group of real number and $(G',\cdot)$ is a group of the real numbers. Let $f: G\to G'$ be a mapping such that $f(x)=e^x$ for $x\in G$. Show that f is an isomorphism & onto.

Soln: If x is a real number, $e^x>0$ and hence $e^x\in G'$.

Let $a, b\in G$

$\therefore e^a, e^b \in G'$.

i.e, $f(a)=e^a$ & $f(b)=e^b$.

Now we have $f(a)=f(b)$

$\Rightarrow e^a=e^b$.

$\Rightarrow a = b$

$\therefore f$ is 1-1.

Let $c \in G'$

i.e, c is a +ve real number and $\log c$ is real number. (+ve or -ve or zero).

Also $\log c \in G$.

$\therefore f(\log c) = e^{\log c}$ (by defn)

$= c$

$\therefore \exists \log c \in G$ such that $f(\log c) = c$.

$\therefore f$ is onto.

Let $a, b \in G \Rightarrow a+b \in G$.

$\therefore f(a) = e^a$, $f(b) = e^b$ & $f(a+b) = e^{a+b}$.

Now we have

$f(a+b) = e^{a+b}$

$= e^a \cdot e^b$.

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

$\therefore f$ is homomorphism, which is 1-1 & onto.

$\therefore f$ is an isomorphism.

$\rightarrow$ If f' is a homomorphism of G onto G' and g' is homomorphism of G' onto G'', show that gof is a homomorphism of G onto G''.

Also show that the kernel of f is a subgroup of the kernel of gof.

Soln: $f: G \to G'$ is a homomorphism & onto.

$g: G' \to G''$ is a homomorphism & onto.

$\therefore gof: G \to G''$ is a mapping of G onto G'' such that $(gof)(x) = g(f(x))$ $\forall x \in G$.

Let $a, b \in G$

Then $(gof)(ab) = g[f(ab)]$

$= g[f(a) \cdot f(b)]$. ($\because f$ is homo.)

$= g(f(a)) \cdot g(f(b))$ ($\because$ g is homo).

$= (gof)(a) \cdot (gof)(b)$.

$\therefore$ gof is homomorphism from G onto G''.

Let e' be identity element in G'.

If k' be the kernel of f

then $k' = \{ x \in G / f(x) = e' \}$.

Let e'' be the identity element in G''.

If k'' be the kernel of gof.

then $k'' = \{ y \in G / (g \circ f)(y) = e'' \}$.

To show that the kernel of f is a subgroup of the kernel of gof

i.e, to show that $k' \subseteq k''$

Let $k' \in K'$ then $f(k') = e'$.

Also $-k' \in G$.

Now $(gof)(k') = g(f(k'))$

$= g(e')$

$= e''$ ($\because$ g is homo).

$\therefore k' \in k''$

$\therefore k' \in K' \Rightarrow k' \in K''$.

$\therefore K' \subseteq K''$

Theorem 2005 → Let $f: G \to G'$ be a homomorphism.

If the order of $a \in G$ is finite then the order of $f(a)$ is a divisor of the order of a.

i.e, $\frac{o(a)}{o(f(a))}$.

Proof: Let $a \in G$ and $o(a) = m$ then $a^m = e$.

where m is the least +ve integer.

$\therefore f(a^m) = f(e)$

$\Rightarrow f[a \cdot a \cdots a \text{ (m times)}] = e'$.

Note: [1] If the order of 'a' is finite then the order of f(a) cannot be finite. Because if the order of f(a) is finite and is equal to 'm'. (i.e, $O(f(a)) = m$), then $a^m = e$.

$\therefore O(a)$ is finite

which is a contradiction.

[2]. Let f be an isomorphic mapping of a group G into a group G'. then

(i) the f-image of the identity element 'e' of G is the identity element e' of G'.

i.e, $f(e) = e'$.

(ii) The f-image of the inverse of an element 'a' of G is the inverse of the f-image of a.

i.e, $f(a^{-1}) = [f(a)]^{-1}$.

(iii) The order of an element 'a' of G is equal to the order of its image. f(a).

i.e, $O(a) = O(f(a))$.

[3]. Suppose we are to prove that a group G is isomorphic to another group G', then we should try to find a 1-1 mapping from G onto G' which also preserves compositions in G and G'. while forming such a mapping we should keep in mind the above three facts (i.e, in Note [2]) that an isomorphic mapping must preserve identities, inverses and orders.

Problems

→ Show that the group $(G = \{0, 1, 2, 3\}, +_4)$ and the group $(G' = \{1, -1, i, -i\}, \cdot)$ are isomorphic.

Sol^n: Here 0 is the identity element in G and 1 is the identity element in G'.

$\Rightarrow f(a) \cdot f(a) \cdots$ m times $= e'$ ($\because$ f is homo).

$\Rightarrow [f(a)]^m = e'$.

$\therefore$ If 'n' is the order of $f(a)$ in G', then 'n' must be a divisor of 'm'.

($\because$ If the element 'a' of a group G is of order 'n' then $a^m = e \Leftrightarrow$ n is a divisor of m).

Theorem 2005

If $f: G \to G'$ is an isomorphism (i.e, $o(f(a))$ divides order of a, $a \in G$), then the order of $a \in G$ is equal to the order of its image $f(a)$.

Proof: Let $o(a) = n$; $a \in G$ then $a^n = e$. where n is the least +ve integer.

$\therefore f(a^n) = f(e)$

$\Rightarrow f(a \cdot a \cdots n \text{ times}) = f(e)$

$\Rightarrow f(a) \cdot f(a) \cdots n \text{ times} = f(e)$ ($\because$ f is homo).

$\Rightarrow [f(a)]^n = f(e) = e'$ where e' is identity in G'.

$\Rightarrow o[f(a)] \leq n$ — (1)

Let $o[f(a)] = m$ then

$[f(a)]^m = e'$. where m is the least +ve integer

$\Rightarrow f(a) f(a) \cdots m \text{ times} = e'$

$\Rightarrow f(a \cdot a \cdots m \text{ times}) = f(e)$

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

$\Rightarrow a^m = e$ ($\because$ f is 1-1)

$\Rightarrow o(a) \leq m$ — (2)

from (1) & (2) we have

$m \leq n$ & $n \leq m$.

$\Rightarrow m = n$

$\Rightarrow o[f(a)] = o(a)$.

∴ If f is isomorphism of G onto G' then $f(0)=1$ (i.e, the identity element in G is mapped onto the identity element in G')

In G, the orders of $1, 2, 3$ are $4, 2$ and 4 respectively

In G', the orders of $-1, i, -i$ are $2, 4$ and 4 respectively.

W.K.T in isomorphic mapping only elements of equal order can be mapped on each other

$\therefore f(2) = -1$ and $f(1) = i$ or $-i$ & $f(3) = i$ or $-i$.

Let $f(1) = i$ and $f(3) = -i$.

Now we observe that $f(\bar{a}^1) = [f(a)]^{-1}$ for $a \in G$

Since $f(\bar{i}^1) = f(3) = -i$

$= i^{-1}$

$\therefore f(\bar{i}^1) = [f(1)]^{-1}$

$f(2^{-1}) = f(2)$

$= -1$

$= -1^{-1}$

$= [f(2)]^{-1}$

Similarly $f(3^{-1}) = [f(3)]^{-1}$

∴ The mapping $f: G \to G'$ is $1-1$ and onto.

To Show f is homomorphism:

Now we form the composition tables for G & G'.

$(G, +_4)$

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

$(G', \cdot)$

$\cdot$	1	−1	i	$-i$
1	1	−1	i	$-i$
−1	−1	1	$-i$	i
i	i	$-i$	−1	1
$-i$	$-i$	i	1	−1

for $a, b \in G$

$f(a +_4 b) = f(a) \cdot f(b)$.

Since $f(0 +_4 2) = f(2)$

$= -1$.

and $f(0) \cdot f(2) = 1(-1) = -1$.

$\therefore f(0+_4 2) = f(0)\cdot f(2)$, etc.

$\therefore f$ is homomorphism.

Also f is 1–1 & onto.

$\therefore f$ is an isomorphism of G onto G'.

Hence G' is isomorphic image of G.

Note: The $\phi : G \to G'$ defined $\phi(0)=1$, $\phi(2)=-1$, $\phi(1)=-i$ and $\phi(3)=i$ is also an isomorphism of G onto G'. In this case we have only two isomorphisms of G onto G'.

H.W → Show that the multiplicative group $G=\{1,-1,i,-i\}$ is isomorphic to the permutation group $G'=\{I,(a\,b\,c\,d),(a\,c)(b\,d),(a\,d\,c\,b)\}$ on four symbols a,b,c,d.

H.W → Show that the x^ve group $G=\{1,\omega,\omega^2\}$ is isomorphic to the permutation group $G'=\{I,(a\,b),(a\,c\,b)\}$ on three symbols a,b,c.

→ Show that the mapping $f: G \to G'$ such that $f(x+iy)=x$ where G is a group of complex numbers under $+$, G' is a group of real numbers under $+$ is a homomorphism onto and find kernel.

Sol^n: Let $a=a_1+ib_1$, $b=a_2+ib_2 \in G$.

$\Rightarrow a+b \in G$.

$\therefore f(a) = f(a_1+ib_1) = a_1$

and $f(b) = f(a_2+ib_2) = a_2$

Now $f(a+b) = f\big((a_1+ib_1)+(a_2+ib_2)\big)$

$= f\big((a_1+a_2)+i(b_1+b_2)\big)$

$= a_1+a_2$ (by def^n)

$= f(a)+f(b)$

$\therefore$ f is a homomorphism.

Let $C \in G'$ where C is a real number.

and $C+iy \in G$.

so that $f(C+iy) = C$ for $y \in \mathbb{R}$.

$\therefore$ f is onto.

$\therefore$ f is a homomorphism from G onto G'.

The identity in G' is 0.

Since $\ker f = \{x+iy \in G / f(x+iy) = x = 0\}$.

$\ker f = \{0+iy / y \in \mathbb{R}\}$.

→ Show that the mapping $f: G \to G'$ such that $f(z) = |z|$, for $z \in G$, where G is a multiplicative group of non-zero complex numbers and G' is a x^ve group of non-zero real numbers is a homomorphism. Find kerf.

Sol^n: Let $z_1, z_2 \in G$.

$\therefore f(z_1) = |z_1|$

$f(z_2) = |z_2|$.

Now we have

$f(z_1 z_2) = |z_1 z_2|$

$= |z_1|\,|z_2|$

$= f(z_1)\, f(z_2)$.

$\therefore$ f is homomorphism.

The identity in G' is 1.

$\therefore \ker f = \{a+ib \in G / f(a+ib) = |a+ib| = \sqrt{a^2+b^2} = 1\}$.

Theorem: If H and N are subgroups of a group G and N is normal subgroup of G. then $\frac{HN}{N} \cong \frac{H}{H \cap N}$.

proof: Since H & N subgroups of G.

and N is a normal subgroup of G.

$\therefore HN$ is a normal subgroup of H.

Also HN is a subgroup of G and $N \subseteq HN$.

Since N is normal in G.

$\therefore N$ is normal subgroup of HN.

$\therefore$ The quotient groups $\frac{HN}{N}$ & $\frac{H}{H \cap N}$ are defined.

Now we define

$\phi : H \to \frac{HN}{N}$ such that

$\phi(x) = Nx \quad \forall x \in H$ ——— (1) ($\because N \subseteq HN$, $x \in H \Rightarrow x \in HN$. $\therefore Nx \in \frac{HN}{N}$)

To show ϕ is well defined:

$x_1, x_2 \in H$

we have $x_1 = x_2$

$\Rightarrow Nx_1 = Nx_2$

$\Rightarrow \phi(x_1) = \phi(x_2)$

$\therefore \phi$ is well defined.

To show ϕ is homomorphism:

Let $x_1, x_2 \in H$,

$Nx_1, Nx_2 \in \frac{HN}{N}$

then $\phi(x_1) = Nx_1$ & $\phi(x_2) = Nx_2$ (by (1))

Now we have

$\phi(x_1 \cdot x_2) = N(x_1 \cdot x_2)$ (by (1))

$= Nx_1 \cdot Nx_2$

$= \phi(x_1)\,\phi(x_2)$ ($\because N$ is normal in HN)

$\therefore \phi$ is homomorphism

To show ϕ is onto:

Let $x \in \frac{HN}{N}$

then $x = Ng$ for some $g \in HN$.

Now $g \in HN \Rightarrow g = hn$ for some $h \in H, n \in N$.

Since N is normal in G —

$\therefore HN = NH$.

$\therefore \exists\ n' \in N,\ h' \in H$ such that $hn = h'h'$ ...

we have $\phi(h') = Nh'$

$= (Nn')h'$ ($\because n' \in N \Rightarrow Nn' = N$)

$= N(n'h')$

$= N(hn) = Nhn$.

$\therefore Ng \in \frac{HN}{N} \Rightarrow \exists\ h' \in H$ such that $\phi(h') = Ng$

$\therefore \phi$ is onto.

$\therefore \phi$ is homomorphism of H onto $\frac{HN}{N}$.

Since $\phi : H \to \frac{HN}{N}$ is homomorphism and onto.

$\therefore$ By fundamental theorem of homomorphism,

we have $\frac{H}{\ker\phi} \cong \frac{HN}{N}$ ——— (2)

$f : G \to G'$ homo & onto
$\phi : \frac{G}{K} \to G'$
$\frac{G}{K} \cong G'$

Now to show that the kernel of $\phi = H \cap N$

Now $\ker\phi = \{ x \in H / \phi(x) = N \}$ where N is the identity in $\frac{HN}{N}$

Let $x \in \ker\phi$.

$\Leftrightarrow \phi(x) = N$ and $x \in H$

$\Leftrightarrow Nx = N$ and $x \in H$

$\Leftrightarrow x \in N$ ($\because N$ is normal in G)

and $x \in H$.

$\Leftrightarrow x \in H \cap N$.

$\therefore \ker\phi = H \cap N$. ——— (3)

from (2) & (3)

$$\frac{H}{H \cap N} \cong \frac{HN}{N}.$$

Hence $\frac{HN}{N} \cong \frac{H}{H \cap N}$