Symbols :

$\exists$: there exists

$\forall$: For all

s.t. : such that

$\in$: Belongs to

$\mathbb{N}$: Set of Natural numbers

$\mathbb{Z}$: Set of Integers

$\mathbb{Q}$: Set of Rational nos.

$\mathbb{R}$: Set of Real nos.

$\mathbb{C}$: Set of Complex nos.

$\because$ Because

$\therefore$ Therefore

w.r.t : with respect to

GROUP THEORY

Binary Operation :

An operation '$*$' is said to be a binary operation on G, if G is closed under '$*$'.

That is, $\boxed{\forall\ x, y \in G,\quad x * y \in G}$. [Closure Property]

Ex- (i) '$+$' is a binary operation on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

(ii) '$-$' is a binary operation on $\mathbb{Z}$, but '$-$' is not a binary operation on $\mathbb{N}$,

$(\because\ 1, 2 \in \mathbb{N},\ 1-2 = -1 \notin \mathbb{N})$

* This property is called as closure property.

Let G be a non-empty set and $*$: Binary Operation on G

① Associative Property : $*$ is said to be associative if

$$\forall\, x, y, z \in G, \quad \boxed{(x * y) * z = x * (y * z)}$$

Ex- (i) $\mathbb{Z}^+$ = The set of +ve integeres.

$* = +$, binary operation

Then $(\mathbb{Z}^+, *)$ is associative.

(ii) $\mathbb{Z}^+$ = The set of +ve integeres.

$* = \diamond$ on $\mathbb{Z}^+$ as $a \diamond b = a^2 + b$.

Then $\diamond$ is not associative, take $2, 3, 4 \in \mathbb{Z}^+$

$$2 \diamond 3 = 2^2 + 3 = 7$$

$$(2 \diamond 3) \diamond 4 = 7 \diamond 4 = 7^2 + 4 = 53 \quad \text{—(i)}$$

$$3 \diamond 4 = 3^2 + 4 = 13$$

$$2 \diamond (3 \diamond 4) = 2 \diamond 13 = 2^2 + 13 = 17 \quad \text{—(ii)}$$

$\therefore$ (i) $\neq$ (ii). Therefore $\diamond$ is not associative on $\mathbb{Z}^+$.

Def: (Semi group)

Let $\phi \neq G$ and $*$: Binary operation.

Then $(G, *)$ is called a semigroup if the following conditions are satisfied:

(i) Closure: $a, b \in G \Rightarrow a * b \in G$

(ii) Associativity: $a * (b * c) = (a * b) * c$, for all $a, b, c \in G$.

Ex- Take $G = \{0, 2, 4, 6, \cdots\}$, $* := +$

(i) $a, b \in G \Rightarrow a + b \in G$ (Since a, b is even $\Rightarrow a+b$ is even)

(ii) $(a+b)+c = a+(b+c)$, $\forall\ a, b, c \in A$.

$\therefore$ $(A, +)$ is a semigroup.

② Existance of Identity :

An element 'e' in G_1 is said to be a left identity (right identity) if for all $x \in G_1$,

$$e * x = x \quad (x * e = x)$$

* 'e' is said to identity element of G_1, if it is both a left identity and a right identity.

i.e., $$e * x = x * e = x \quad , \quad \forall x \in G_1$$

Def- (Monoid)

$(G_1, *)$ is called a monoid if the following conditions are satisfied.

(i) $*$ is a closed Properety

(ii) $*$ is an associative Properety

(iii) existance of identity

Ex- Let $S \neq \phi$. $P(S)$ = Powere set of S.

$(P(S), \cup)$ is a monoid, ϕ is the identity.

$(P(S), \cap)$ is a monoid, S is the identity.

③ Existance of Inverse:

Let $a \in G$. An element b is said to be an inverese of a if -

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

Problem -

Let N be the set of all naturcal neumberes.

For each of the following determine whether $*$ is an associative operations.

(i) $a * b = \max\{a, b\}$

(ii) $a * b = \min\{a, b+2\}$

(iii) $a * b = a + 2b$

Def: (Group)

A group is a set G together with a binary operation

$$* : G \times G \longrightarrow G$$

satisfying three properties (called the group axioms).

(i) Associativity: $\forall x, y, z \in G, \; x * (y * z) = (x * y) * z$.

(ii) Existance of Identity:

$$\forall x \in G, \; \exists e \in G \text{ s.t. } x * e = x = e * x .$$

The element e is said to be an identity element of G.

(iii) Existance of Inverse:

$$\forall x \in G, \; \exists y \in G \text{ s.t } x * y = y * x = e .$$

The element y is said to be an inverse element of x in G.

Then we say that $(G, *)$ is a group,

or G is a group under the operation $*$.

* If $(G, *)$ is a group, the no. of elements in the set G is said to be the Orderc of G.

It is denoted by $|G|$ or $O(G)$.

* A group whose orderc is finite, is called finite group.

* A group whose orderc is infinite, is called infinite group.

* We denote $x * y$ as simply xy.

Remarck-

(i) $xy \neq yx$ in generral, in a group.

(ii) If x and y arce two elements such that $xy = yx$, then we say that x and y commute with each otherc.

(iii) Everey element commutes with the identity element.

(iv) Each element commutes with itself.

(v) If y is an inverse of x, then $xy = yx = e$, which means that x and y commute with each other.

Ex- (i) $(G = \{0\}, +)$ is a group. $|G| = 1$ (smallest group)

(ii) $(\mathbb{Z}, +)$ is a group (Infinite group).

Identity $= 0$, Inverse of $a = -a$

(iii) $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ are infinite groups.

Identity $= 0$, Inverse of $a = -a$

(iv) $(\mathbb{Z}, -)$ is not a group. [Associative fails]

$(2-3)-4 = -5 = \text{LHS}$

$2-(3-4) = 2-(-1)$

$= 3 = \text{RHS}$

$\therefore$ LHS $\neq$ RHS

(v) $(\mathbb{Z}, \cdot)$ is not a group. [Existance of Inverse fails]

For $5 \in \mathbb{Z}$, there is no $b \in \mathbb{Z}$ such that

$5 \cdot b = 1$

↖ Identity in $(\mathbb{Z}, \cdot)$

(vi) $\mathbb{Q}^+$: The set of positive rational numbers

$*$: $\times$ (usual multiplication)

Then $(\mathbb{Q}^+, \times)$ is a group.

Identity : 1 ; Inverse of $a = 1/a$

(vii) S : The set of positive irrational numbers together with 1.

$*$: $\times$ (usual multiplication)

$(S, *)$ Satisfies all the property of a group, but '$*$' is not closed under multiplication. ($\because \sqrt{2} \times \sqrt{2} = 2 \notin S$) Hence $(S, *)$ is not a group.

(viii) $(\mathbb{R}, \times)$ is not a group, as 0 has no multiplicative inverse.

(ix) $(\mathbb{R} - \{0\}, \times)$ is a group.

(x) $H = \{1, -1\}$ and $K = \{1, i, -1, -i\}$, where $i = \sqrt{-1}$.

Then $(H, \times)$ and $(K, \times)$ are groups of order 2 and 4 respectively.

Ex- Show that the fourth roots of unity $\{1, -1, i, -i\}$ form a group under complex multiplication.

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

$\cdot$	1	-1	i	$-i$
1	$\boxed{1}$	-1	i	$-i$
-1	-1	$\boxed{1}$	$-i$	i
i	i	$-i$	-1	$\boxed{1}$
$-i$	$-i$	i	$\boxed{1}$	-1

$(a+ib)(c+id)$

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

(i) $(0+i)(0-i)$

$= (0-1) + i(0+0)$

$= -1$

(ii) $(-1+i0)(0+i)$

$= 0 + i(-1) = -i$

Closed: All entries in the table are in G.

Associative: $1 \cdot [(-1) \cdot i] = 1 \cdot -i = -i$

$[1 \cdot (-1)] \cdot i = -1 \cdot i = -i$

Identity: $1 \in G$

Inverse: Inverse of 1 is 1

" " -1 is -1

" " i is $-i$

" " $-i$ is i.

Problem:

Consider $(\mathbb{Z}, *)$, where '$*$' is defined by -

$$a * b = a + b - ab$$

Verify whether $*$ on $\mathbb{Z}$,

(i) Monoid

(ii) Group

Soln - (i) $a * b = a + b - ab \in \mathbb{Z}, \forall\ a, b \in \mathbb{Z}$ [closed]

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

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

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

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

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

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

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

(iii) $0 \in \mathbb{Z}$ is the identity as -

$$a * 0 = 0 * a = a$$

Therefore $(\mathbb{Z}, *)$ is a monoid.

(iv) For $3 \in \mathbb{Z}$, there is no $x \in \mathbb{Z}$, such that

$$3 + x - 3x = 0 \Rightarrow -2x = -3$$

i.e $x = \frac{3}{2} \notin \mathbb{Z}$

Hence $(\mathbb{Z}, *)$ is not a group.

H.W

Problem -

Show that $(\mathbb{Q} - \{-1\}, *)$, where $*$ is defined as $a * b = a + b + ab$, for all $a, b \in \mathbb{Q} - \{-1\}$,

Find the inverse of 15 ?

Ex- $\mathbb{C}$: The set of complex numberes

$$= \{ a+bi \mid a,b \in \mathbb{R},\ i^2 = -1 \}$$

$* : +$; $(a+bi)+(c+di)$

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

Identity : $0 = 0+0i$

Inverse of $a+bi = -a-bi$

Ex- $\mathbb{C}^*$: Set of all non zero complex numberes

$* : \times$ (usual multiplication)

Then $(a+bi)\cdot(c+di) = (ac-bd)+(ad+bc)i$

$(\mathbb{C}^*, \times)$ is a groeup, where -

Identity : 1

Inverse of $a+bi = \dfrac{1}{a+bi}$

$$= \frac{1}{a+bi} \times \frac{a-bi}{a-bi}$$

$$= \frac{a-bi}{a^2+b^2}$$

Problem -

Let $\mathbb{Z}_n$: Set of integers $\{0, 1, 2, \ldots, n-1\}$

$\odot$: Binary operation on $\mathbb{Z}_n$ such that

$a \odot b$ = remainder of ab divided by n.

(i) Construct the table for the operation $\odot$ for $n=4$.

(ii) Show that $(\mathbb{Z}_n, \odot)$ is a semigroup for any n.

Soln - (i) $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

Define $a \odot b$ = remainder of ab divided by n.

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	0

(ii) Let n be a positive integer.

Define $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ (Set of all possible remainders obtained by dividing an integer by n)

Multiplication Modulo n : $\odot$

$a \odot b = (ab) \bmod n$, for every $a, b \in \mathbb{Z}_n$.

(i) Closure:

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

$a \odot b = (ab) \bmod n$

$= r$, $0 \leq r < n$

$\in \mathbb{Z}_n$

(ii) Associativity:

For any $a, b, c \in \mathbb{Z}_n$,

$(a \odot b) \odot c = ((ab) \bmod n) \odot c$

$= ((ab)c) \bmod n$

$= (abc) \bmod n$

$a \odot (b \odot c) = a \odot ((bc) \bmod n)$

$= (a(bc)) \bmod n$

$= (abc) \bmod n$

(iii) Identity :

$$a \odot 1 = (a \cdot 1) \bmod n$$

$$= a$$

(iv) Inverse :

$$a \odot b = 1$$

$$\Rightarrow (ab) \bmod n = 1$$

Ex- $M_{2\times 2}(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a,b,c,d \in \mathbb{R} \right\}$

= The set of 2×2 matrices with real entries

$*$: Component wise addition

That is - $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix}$

Identity : $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$; Inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

Ex- $M_{2\times 2}(\mathbb{R})$, $*$: Matrix Multiplication

Then $(M_{2\times 2}(\mathbb{R}), *)$ is not a group.

[Existance of Inverse fails]

Inverse of a matrix 'A' can not be found if determinant of $A = 0$.

Ex- The determinant of a 2×2 matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is the number $ad-bc$.

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

of 2×2 matrices with real entries and non-zero determinants.

$*$: Matrix Multiplication

i.e. $$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2+b_1c_2 & a_1b_2+b_1d_2 \\ c_1a_2+d_1c_2 & c_1b_2+d_1d_2 \end{bmatrix}$$

(i) Closure Property :

To show : Product of two matrices with non zero determinants also has a non-zero determinant.

This follows from : $\det(AB) = (\det A)(\det B)$.

Identity : $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$.

Thus $(GL(2,\mathbb{R}), *)$ is a group.

It is called as general lineare group of 2×2 matrices over $\mathbb{R}$.

Basic Properties of Groups -

① Every group has a unique identity element.

Proof. Suppose e_1 and e_2 are both identity elements of a group G.

Then $e_1 = x e_1 = e_1 x$ ①

and $e_2 = x e_2 = e_2 x$ ②

$\forall\ x \in G$.

Since $e_2 \in G$, from ① we have $e_1 e_2 = e_1$ and since $e_1 \in G$, from ② we have $e_1 e_2 = e_2$.

$\Rightarrow e_1 = e_1 e_2 = e_2$.

$\Rightarrow e_1 = e_2$.

② Every element of a group has a unique inverse.

Proof. Let $x \in G$ be an element.

Then by axiom (iii), x has an inverse, say y.

Suppose z is also an inverse of x.

Then, if e denotes the identity element of G,

$$xy = yx = e \quad \text{——①}$$

and $$xz = zx = e \quad \text{——②}$$

To show: $y = z$.

Also since e is the identity element, we have

$$y = ye$$

$$= y(xz)$$

$$= (yx)z \quad [\because \text{Associative}]$$

$$= ez$$

$$= z \quad [\because \text{'e' is an identity element}]$$

$\therefore y = z$.

* Since each element x is guaranteed to have a unique inverse, we can denote this inverse as x^{-1}.

* From axiom (iii), it is clear that if y is an inverse of x, then x is also an inverse of y.

Thus $\boxed{(x^{-1})^{-1} = x}$.

Exercise - 1

Prove that $(xy)^{-1} = y^{-1}x^{-1}$.

Soln - Let $a = xy$ and $b = y^{-1}x^{-1}$.

To show: $a^{-1} = b$, we need to verify that

$ab = e$ and $ba = e$.

i.e., $(xy)(y^{-1}x^{-1}) = e$ and $(y^{-1}x^{-1})(xy) = e$.

Now, $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1}$ [Associativity]

$= xex^{-1}$

$= xx^{-1}$

$= e$

Similarly, $(y^{-1}x^{-1})(xy) = e$.

Thus $(xy)^{-1} = y^{-1}x^{-1}$.

Exercise - 2 : (Cancellation laws)

Prove that the (left and reight) Cancellation laws hold in every group.

i.e, Prove that if x and y are elements of a group G, then - (i) If $\exists\, a \in G$, $ax = ay$, then $x = y$.

(ii) If $\exists\, b \in G$, $xb = yb$, then $x = y$.

Soln - (i) Given $ax = ay$.

Left multiplying by a^{-1}, we have -

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

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

$$\Rightarrow ex = ey$$

$$\Rightarrow x = y$$

(ii) Similarly, given $xb = yb$.

Right multiplying by b^{-1},

$$xb(b^{-1}) = yb(b^{-1})$$

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

$$\Rightarrow xe = ye$$

$$\Rightarrow x = y$$

Abelian Group -

A group $(G, *)$ is said to be Abelian or commutative if $*$ is a commutative operation.

That is,

$$\forall\ a, b \in G,\ a * b = b * a .$$

* A group that is not Abelian is non-abelian.

Ex- (i) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are abelian groups.

(ii) $(\mathbb{Q} - \{0\}, \cdot)$ and $(\mathbb{R} - \{0\}, \cdot)$ are abelian groups.

(iii) $GL(2, \mathbb{R})$ is not abelian group.

Exercise - 5. Let G be a group.

① Prove that if every element of G is self-inverse, then G is Abelian. Is the converse true?

Soln- Suppose every element of G is self-inverse.

That is, for all $x \in G$, $x^{-1} = x$.

Let $a, b \in G$. Then $a^{-1} = a$ and $b^{-1} = b$.

To show: $ab = ba$.

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

But since $a^{-1} = a$, $b^{-1} = b$, $b^{-1}a^{-1} = ba$ ——— ②

Also, since G is closed, we get $a, b \in G \Rightarrow ab \in G$.

$\Rightarrow (ab)^{-1} = ab$ ——— ③

Applying ② and ③ in ①, we get -

$$ab = ba$$

Converse need not be true.

Ex- $(\mathbb{Z}, +)$ is an Abelian group in which not all elements are self inverse. Ex- $2 \in \mathbb{Z}$, $2^{-1} = -2$.

② Prove that G is Abelian if and only if

$$\forall\, x, y \in G : (xy)^{-1} = x^{-1}y^{-1}.$$

Soln – If G is abelian, then –

$$(xy)^{-1} = y^{-1}x^{-1} \quad [\text{by Exercise 1}]$$
$$= x^{-1}y^{-1} \quad [\because G \text{ is abelian}, x^{-1}, y^{-1} \in G]$$

Conversely, suppose that G satisfies the given property.

Then for any two elements x and y,

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

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

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

$$= yx$$

③ Prove that G is abelian iff $\forall a, b \in G$,

$$(ab)^2 = a^2 b^2 .$$

Soln - If G is abelian, then -

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

$$= a(ba)b \quad [\text{Associativity}]$$

$$= a(ab)b \quad [\because G \text{ is abelian}]$$

$$= a^2 b^2$$

Conversely, $(ab)^2 = a^2 b^2$

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

$$\Rightarrow abab = aabb$$

$$\Rightarrow bab = abb \quad [\text{Left cancelation}]$$

$$\Rightarrow ba = ab \quad [\text{right cancelation}]$$

Subgroups

Def:

A subgroup of a group $(G, *)$ is a subset $H \subseteq G$ such that $(H, *)$ is also a group.

Then we write $H \leq G$.

Ex-

(i) $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

So $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$.

$(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.

$(\mathbb{Q}, +)$ " " " $(\mathbb{R}, +)$.

(ii) $(\mathbb{Q} - \{0\}, \times)$ is a subgroup of $(\mathbb{R} - \{0\}, \times)$.

(iii) Fore the group $(\mathbb{Z}, +)$, $(E, +)$ where E is the set of all even integeres, is a subgroup.

(iv) $(k\mathbb{Z}, +)$ where $k \in \mathbb{Z}^+$, is a subgroup of $(\mathbb{Z}, +)$.

(v) Let $G = GL(\mathbb{Q}, \mathbb{R})$, $* : \times$, then $(G, *)$ is a group.

Take $H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G \mid ad \neq 0 \right\}$. Then $(H, *)$ is a subgroup of G.

Lemma -

Let $(G, *)$ be a group and $H \subseteq G$.

Then $(H, *)$ is a subgroup of G if and only if the following hold.

(i) H is closed under $*$.

That is, $\forall\, x, y \in H,\ x * y \in H$.

(ii) H contains the identity element (of G): $e \in H$.

(iii) The inverse of every element of H is also in H.

i.e., $\forall\, x \in H,\ x^{-1} \in H$.

Theorem -

Let $(G, *)$ be a group and H be a non-empty subset of G. Show that $(H, *)$ is a subgroup of G if and only if for any $x, y \in H$, $x * y^{-1} \in H$.

Proof - If $H \leq G$, then it is obviously non-empty (for $e \in H$) and for any $x, y \in H$, we have $x, y^{-1} \in H$

(Since H contains all the inverses of all its element)

$\Rightarrow x * y^{-1} \in H$ (closure)

Conversely, Suppose that $H \neq \phi$ and $\forall\ x, y \in H, x * y^{-1} \in H$.

(i) Since $H \neq \phi$, $\exists\ x \in H$.

Then $x, x \in H$

$\Rightarrow x * x^{-1} \in H$

$\Rightarrow e \in H$

(ii) If $x \in H$, then $e, x \in H \Rightarrow e * x^{-1} \in H$

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

(iii) If $x, y \in H$, then by (ii), $y^{-1} \in H$.

Thus $x, y^{-1} \in H \Rightarrow x * (y^{-1})^{-1} \in H$

$\Rightarrow x * y \in H$

$\therefore$ H is a subgroup of G by previous lemma.

Theorem:

(1) Let $(H,*)$ and $(K,*)$ be any two subgroups of $(G,*)$.

Then (1) $H \cap K \leq G$

(2) $H \cup K$ is not a subgroup of G

unless $H \subseteq K$ or $K \subseteq H$.

Proof: Clearly $e \in H$, $e \in K$

$\Rightarrow e \in H \cap K$

$\Rightarrow H \cap K \neq \phi$

Let $x, y \in H \cap K$.

$\Rightarrow x, y \in H \Rightarrow x * y^{-1} \in H$ [$\because$ H and K are subgroups of G]

and $x, y \in K \Rightarrow x * y^{-1} \in K$

$\Rightarrow x * y^{-1} \in H \cap K$

$\therefore (H \cap K, *)$ is a subgroup of $(G,*)$.

(2) Suppose that $H \not\subseteq K$ and $K \not\subseteq H$.

Then there exists an element $h \in H$ such that $h \notin K$ and there exists $k \in K$ such that $k \notin H$.

Then if $hk \in H \Rightarrow h^{-1}hk = k \in H$, a contradiction.

Therefore $hk \notin H$.

Similarly, $hk \notin K$.

Thus $hk \notin H \cup K$.

So, $H \cup K$ is not closed under the operation.

Hence $H \cup K$ is not a subgroup of G.

If $H \subseteq K$, then $H \cup K = K$, a subgroup of G.

The other case is similar.

Ex- Take $G = (\mathbb{Z}, +)$, $H = (2\mathbb{Z}, +)$, $K = (3\mathbb{Z}, +)$

Then H and K are subgroups of G, $H \not\subseteq K$ and $K \not\subseteq H$.

But $H \cup K$ is not a subgroup, since $2, 3 \in H \cup K$,

but $2 + 3 = 5 \notin H \cup K$.

Problem.

Let $(H, \cdot)$ and $(K, \cdot)$ be subgroups of $(G, \cdot)$.

Let $HK = \{ hk \mid h \in H, k \in K \}$

Show that $(HK, \cdot)$ is a subgroup of $(G, \cdot)$

if and only if $HK = KH$.

Proof: Suppose that $(HK, \cdot)$ be a subgroup of $(G, \cdot)$.

To prove: $HK \subseteq KH$

Take $x \in HK$.

Since $HK \leq G$, $x^{-1} \in HK$.

Write $x^{-1} = hk$, for some $h \in H$, $k \in K$.

Taking inverse:

$$\begin{aligned} x &= (x^{-1})^{-1} \\ &= (hk)^{-1} \\ &= k^{-1} h^{-1} \\ &\in KH \end{aligned}$$

Therefore, $HK \subseteq KH$.

On the other hand, take $y \in KH$.

Then $y = k_1 h_1$, for some $k_1 \in K$, $h_1 \in H$.

$$y^{-1} = (k_1 h_1)^{-1}$$

$$= h_1^{-1} k_1^{-1} \in HK$$

Now, $y = (y^{-1})^{-1} \in HK$ (since $HK \leq G$)

Therefore $KH \subseteq HK$.

Conversely, suppose that $HK = KH$.

Since H and K are non-empty, HK is non-empty.

Let $x, y \in HK$. To show: $xy^{-1} \in HK$.

$\Rightarrow x = h_1 k_1$ and $y = h_2 k_2$, for some $h_1, h_2 \in H$, $k_1, k_2 \in K$.

Then $xy^{-1} = (h_1 k_1)(h_2 k_2)^{-1} = (h_1 k_1)(k_2^{-1} h_2^{-1})$

$$= h_1 \underbrace{k_1 k_2^{-1}}_{\in K} h_2^{-1}$$

$$= h_1 \underbrace{k_3 h_2^{-1}}_{\in KH = HK}, \quad \text{where } k_3 = k_1 k_2^{-1}$$

$$= h_1 h_3 k_4 \quad \left[\because k_3 h_2^{-1} \in KH = HK \right.$$

$\left. \Rightarrow \exists\, h_3 \in H \text{ and } k_4 \in K \right.$

$\left. \text{s.t } k_3 h_2^{-1} = h_3 k_4 \right]$.

$\Rightarrow xy^{-1} = \underbrace{h_1 h_3}_{\in H} k_4$

$= h_4 k_4$, where $h_4 = h_1 h_3 \in H$

$\in HK$

Therefore $xy^{-1} \in HK$.

Thus $HK \leq G$.

Exercise 6.
Let G be a group.

1. The centre of G is defined by $Z(G) = \{ z \in G \mid zx = xz, \ \forall x \in G \}$. Prove that $Z(G) \leq G$.
2. Let $S \subseteq G$. Then the centraliser of S in G is $C_G(S) = \{ y \in G \mid yx = xy, \ \forall x \in S \}$. Prove that $C_G(S) \leq G$.
3. Show that any subgroup of an Abelian group is Abelian.
4. Let G be Abelian. For $n \in \mathbb{N}_0$, define $H = \{ x^n \mid x \in G \}$. Show that $H \leq G$.
5. Let G be Abelian. For $n \in \mathbb{N}_0$, define $H = \{ x \in G \mid x^n = e \}$. Show that $H \leq G$.

Cyclic Subgroups

Def:

Let G be a group and x be any element of G.

The cyclic subgroup of G generated by 'x' is defined to be

$$\langle x \rangle = \{ x^n \mid n \in \mathbb{Z} \}$$

That is, $\langle x \rangle$ is a subset containing all powers (+ve, -ve, zero) of x.

Thus, every element of $\langle x \rangle$ is of the form x^k, for some integer k.

Exercise: Show that $H = \langle x \rangle$ is a subgroup of G.

Soln: Let $a \in H$ and $b \in H$

$\Rightarrow a = x^m$ and $b = x^n$, for some $m, n \in \mathbb{Z}$

Then $ab^{-1} = x^m (x^n)^{-1}$

$= x^m (x^{-1})^n$

$= x^m x^{-n}$

$= x^{m-n} \in H$

Thus H is a subgroup of G.

Def:

A group G is said to be Cyclic if it is equal to the cyclic subgroup generated by one of its elements.

That is, G is cyclic if there exists an element $g \in G$ such that $G = \langle g \rangle$.

Then g is a generator of G.

Ex - (i) $(\mathbb{Z}, +)$ is a group.

$\mathbb{Z} = \langle 1 \rangle$, Since every integer n can be written as $n \times 1$.

(Since $\mathbb{Z}$ is a group w.r.t. '$+$', we write 'nx' instead of 'x^n').

Also $\mathbb{Z} = \langle -1 \rangle$, since -1 is the inverse of 1.

(ii) $G = (\{1, -1, i, -i\}, \cdot)$ is a cyclic group with generators i and $-i$. $\left[(i)^1 = i, (i)^2 = -1, (i)^3 = -i, (i)^4 = 1\right]$

Ex- $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ for $n \geq 1$

$a +_n b = (a+b) \bmod n$

Then $(\mathbb{Z}_n, +_n)$ is a group.

For any $j > 0$ in $\mathbb{Z}_n$, the inverse of j is $n-j$.

The group is called group of integers modulo n.

$n=8$, $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$, $+_8$

Generators are $\mathbb{Z}_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$

$\langle 3 \rangle = \{3, 3+_8 3, 3+_8 3+_8 3, \cdots\}$

$= \{3, 6, 1, 4, 7, 2, 5, 0\} = \mathbb{Z}_8$

But $\langle 2 \rangle = \{2, 2+_8 2, 2+_8 2+_8 2, \cdots\}$

$= \{2, 4, 6, 0\} \neq \mathbb{Z}_8$

Thus $\langle 0 \rangle, \langle 2 \rangle, \langle 4 \rangle, \langle 6 \rangle$ are not the generators of $\mathbb{Z}_8$.

Ex- $U(n) = \{$Set of all positive integers $a (< n)$ and $\gcd(a, n) = 1\}$

$a \odot b$ = multiplicative modulo n

Then $(U(n), \odot)$ is an abelian group.

For $n=10$:

$U_{10} = \{1, 3, 7, 9\}$, $a \odot b = (ab) \bmod 10$

Generators of $U_{10} = \langle 3 \rangle = \{3^0, 3^1, 3^2, 3^3\}$

$\langle 7 \rangle = \{7^0, 7^1, 7^2, 7^3\}$

$3^0 = 1$

$3^1 = 3$

$3^2 = 3 \odot 3 = 9 \pmod{10} = 9$

$3^3 = 3 \odot 3 \odot 3 = 27 \pmod{10} = 7$

So, 3 and 7 are generators of $U(10)$.

Non-Ex- (Smallest non-cyclic group)

$U(8) = \{1, 3, 5, 7\}$, $a \odot b = (ab) \bmod 8$

$(U(8), \odot)$ is an abelian group, but not cyclic.

$\odot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Every element is its self inverse, hence the group is abelian.

$\langle 1 \rangle = \{ 1, 1^2, 1^3, 1^4 \cdots \} = \{ 1 \}$

$\langle 3 \rangle = \{ 3^0, 3^1, 3^2, \cdots \} = \{ 1, 3, 3 \odot 3, 3 \odot 3 \odot 3, \cdots \}$

$= \{ 1, 3, 9 \pmod 8, 27 \pmod 8, \cdots \}$

$= \{ 1, 3, 1, 3, \cdots \}$

$= \{ 1, 3 \}$

$\langle 5 \rangle = \{ 1, 5 \}$

$\langle 7 \rangle = \{ 1, 7 \}$

So $U(8) \neq \langle a \rangle$, for any $a \in U(8)$.

Problem.

If G is a cyclic group, then G is abelian.

Proof: Let $G = \langle g \rangle$ be a cyclic group.

If $a = g^i$ and $b = g^j$ are any two elements of a cyclic group $G = \langle g \rangle$, then -

$$ab = g^i \cdot g^j = g^{i+j}$$

$$= g^{j+i} \quad [\because i, j \in \mathbb{Z} \text{ and } (\mathbb{Z}, +) \text{ is abelian}, \; i+j = j+i]$$

$$= g^j \cdot g^i$$

$$= ba$$

Thus, any cyclic group is Abelian. But Converse not true.

Ex- $(U(8), \odot)$ is abelian, but not cyclic.

Division Algorithm -

Let a and b be integeres with $b > 0$. Then there exist unique integeres q and r with the properety that $a = bq + r$, where $0 \leq r < b$.

Theorem-

Every subgroup of a cyclic group is cyclic.

Proof- Consider a cyclic group $G = \langle g \rangle$ with generator 'g'.

Let H be any subgroup of G.

Every element of H is of the form g^k, for some integer 'k'.

Let 'n' be the least positive integer such that $g^n \in H$.

Claim: $H = \langle g^n \rangle$.

That is, every element of H is a power of g^n.

Clearly, since $H \leq G$ and $g^n \in H$, by closure property $\langle g^n \rangle \subseteq H$.

To show: $H \subseteq \langle g^n \rangle$.

Let g^m be an arbitrary element of H.

By division algorithm,

$$m = nq + r, \quad \exists\, q, r \in \mathbb{Z}, \quad 0 \leq r < n.$$

That is, we can divide m by n to obtain a quotient q and a remainder r (which must be non-ve numbers less than n)

Now, $g^m = g^{nq+r}$

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

$\Rightarrow g^r = (g^n)^{-q} \cdot g^m$

Since $g^n, g^m \in H$, this implies $g^r \in H$.

But n is the least positive integere such that $g^n \in H$, and $n > r \geq 0$, therefore $r = 0$.

Thus, we must have $g^m = (g^n)^q$, as required.

Def:

The ordere of an element x of a group G is defined as the least +ve integere 'n' (if any) such that $x^n = e$.

* If there is no such positive integere, then the element is said to have infinite ordere.

* The ordere of x is denoted by $|x|$ ore $O(x)$.

Theorem.

Let G be a finite group and $a \in G$.

Then the order of a is $|\langle a \rangle|$, the number of elements in $\langle a \rangle$.

That is, $O(a) = O(\langle a \rangle)$.

Proof: Let G be a finite group.

Then there is an integer $k \geq 1$ with $1, a, a^2, \cdots, a^{k-1}$ consisting of k distinct elements, while $1, a, a^2, \cdots, a^k$ has a repetition; hence $a^k \in \{1, a, a^2, \cdots, a^{k-1}\}$.

That is, $a^k = a^i$, for some i, $0 \leq i < k$.

If $i \geq 1$, then $a^{k-i} = 1$, contradicting the original list having no repetitions.

Therefore, $a^k = a^0 = 1$, and k is the order of 'a'.

(being the smallest positive such k). That is, $O(a) = k$.

If $H = \{1, a, a^2, \cdots, a^{k-1}\}$, then $O(H) = k$.

It suffices to show that $H = \langle a \rangle$.

Clearly $H \subseteq \langle a \rangle$.

Now, take $a^i \in \langle a \rangle$.

By division algorithm, $i = qk + r$, where $0 \leq r < k$.

Hence $a^i = a^{qk+r}$

$= a^{qk} \, a^r$

$= (a^k)^q \, a^r$

$= a^r \in H$

$\Rightarrow \langle a \rangle \subseteq H$.

Therefore $H = \langle a \rangle$.

Lagrange's Theorem

Def:

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

We say that a is congruent to $b \pmod H$, written as

$a \equiv b \pmod H$ if $ab^{-1} \in H$.

Theorem: The relation $a \equiv b \pmod H$ is an equivalence relation.

Proof.

(i) **Reflexive:**

Since $H \leq G$, we have that

$aa^{-1} = e \in H$, for $a \in G$

$\Rightarrow a \equiv a \pmod H$

(ii) **Symmetric:**

Suppose $a \equiv b \pmod H$

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

$\Rightarrow (ab^{-1})^{-1} \in H \quad [\because H \leq G]$

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

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

$\Rightarrow b \equiv a \pmod{H}$

(iii) Transitive:

Suppose $a \equiv b \pmod{H}$, $b \equiv c \pmod{H}$

$\Rightarrow ab^{-1} \in H$ and $bc^{-1} \in H$

$\Rightarrow (ab^{-1})(bc^{-1}) \in H$ [$\because H \leq G$, Closure Prop.]

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

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

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

$\Rightarrow a \equiv c \pmod{H}$

Therefore, the relation is an equivalence relation.

Def:

Let G be a group and $\phi \neq H \subseteq G$.

For any $a \in G$, $Ha = \{ha \mid h \in H\}$ is called a right coset of H in G.

$aH = \{ah \mid h \in H\}$ is called a left coset of H in G.

Lemma -

For all $a \in G$,

$$Ha = \{ x \in G \mid a \equiv x \bmod H \}$$

$$= \{ x \in G \mid ax^{-1} \in H \}$$

Proof - Let $[a] = \{ x \in G \mid ax^{-1} \in H \}$

First we show that $Ha \subset [a]$.

Let $b \in Ha$.

$\Rightarrow b = ha$, for some $h \in H$.

Now, $ab^{-1} = a(ha)^{-1}$

$= aa^{-1}h^{-1}$

$= eh^{-1}$

$= h^{-1} \in H$, since $H \leq G$.

$\Rightarrow b \in [a]$, by definition of congruence mod H.

$\Rightarrow ha \in [a]$, for everey $h \in H$.

$\Rightarrow Ha \subseteq [a]$.

Next to show $[a] \subset H$.

Let $x \in [a]$.

Then $ax^{-1} \in H$

$\Rightarrow (ax^{-1})^{-1} = (x^{-1})^{-1}a^{-1} \in H \quad [\because H \leq G]$

$= xa^{-1} \in H$

That is, $xa^{-1} = h$, fore some $h \in H$.

Multiplying both sides by 'a' from the right, we get -

$xa^{-1}a = ha$

$\Rightarrow x = ha \in Ha$

$\Rightarrow x \in Ha$

$\Rightarrow [a] \subseteq Ha$.

Thus, $Ha = [a]$.

Note:

- By Prev lemma, we see that Ha is the equivalence class of a in G.
- These equivalence classes yield a decomposition of G into disjoint subsets.

- Thus any two right cosets of H of G are either are identical or have no element in common.

Ex- ① $G = (\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}, +_6)$

$H = \{0, 3\}$ is a subgroup of G.

The left cosets of the subgroup H in $\mathbb{Z}_6$ are

$H = \{0, 3\}$, $1 + H = \{1, 4\}$, $2 + H = \{2, 5\}$

$3 + H = \{3, 0\} = H$

$\therefore$ H, $1 + H$, $2 + H$ are all distinct left cosets H of G.

② G = The additive group of integeres.

Let $H = \{\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots\}$

Then H is a subgroup of G.

Left cosets of H and Right cosets of H -

$1 \in G$, $1 + H = \{\cdots, -8, -5, -2, 1, 4, 7, 10, \cdots\} = H + 1$

$2 + H = \{\cdots, -7, -4, -1, 2, 5, 8, 11, \cdots\} = H + 2$

Properties of Cosets -

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

(i) $a \in aH$

(ii) $aH = H$ if and only if $a \in H$

(iii) $aH = bH$ or $aH \cap bH = \phi$

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

Analogues properties hold for right cosets.

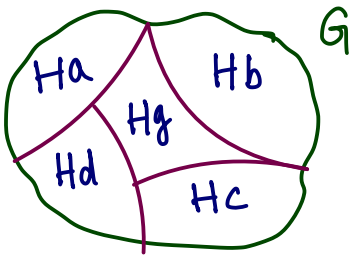
Remark -

* Every subgroup H itself is a coset (of itself).

  That is, $H = He = eH$.

* For any $h \in H$, $hH = Hh = H$ (Prove !)

* Left cosets of a subgroup partition the whole group into equally sized parts.



Problem -

Let H be a subgroup of $(G, *)$ and $a*H$, $b*H$ be two left cosets of H. Prove that either $a*H$ and $b*H$ are disjoint or they are identical.

Soln - Suppose $a*H$ and $b*H$ are not disjoint.

That is, $(a*H) \cap (b*H) \neq \phi$.

Then $\exists\ x \in (a*H) \cap (b*H)$

$\Rightarrow x \in a*H$ and $x \in b*H$

$\Rightarrow x = a*h_1$ and $x = b*h_2$, for some $h_1, h_2 \in H$.

$\Rightarrow a*h_1 = b*h_2$

Post Multiplying with h_1^{-1}, we get -

$$a = b*h_2*h_1^{-1}$$

For any $y \in a*H$, since $y = a*h_3$, for some $h_3 \in H$, we have -

$$y = a*h_3$$

$$= b*\underbrace{h_2*h_1^{-1}*h_3}_{\in H} \in b*H.$$

[$\because$ since $*$ is closed, $h_2, h_1^{-1}, h_3 \in H$ $\Rightarrow h_2*h_1^{-1}*h_3 \in H$]

Therefore, $a * H \subseteq b * H$.

In a similare way, we can prove that

$$b * H \subseteq a * H .$$

Therefore, $a * H = b * H$.

Observation:

This problem is true for right cosets also.

Problem.

Any two left (or right) cosets have same number of elements (or same cardinality).

OR

There is a one-to-one correcrespondence between any two right cosets of H in G.

Soln. Let $H \leq G$ and Ha, Hb be two (distinct) right cosets of H in G, for some $a, b \in H$.

Define $\phi : Ha \longrightarrow Hb$ by $\phi(ha) = hb$, for all $ha \in Ha$.

ϕ is One-One :

Let $h_1a, h_2a \in Ha$ such that

$$\phi(h_1a) = \phi(h_2a)$$

$$\Rightarrow h_1b = h_2b$$

$$\Rightarrow h_1 = h_2 \quad \text{[By right Cancellation Law]}$$

$$\Rightarrow h_1a = h_2a$$

Therefore ϕ is one-one.

ϕ is onto -

Let $hb \in Hb \Rightarrow h \in H$.

Now $ha \in Ha$ and $\phi(ha) = hb$.

Therefore, ϕ is onto.

Hence there is an one-to-one Correcrespondence and therefore have the same Cardinality.

Note: Since $H = He$ we have that H is also a right coset of H in G. Hence by Prev problem, we have any right coset of H in G have $O(H)$ elements.

Problem:

Let G be a finite group and H be a subgroup of G.

Let $x_1H, \cdots, x_kH$ be all the distinct left cosets of H in G.

Then $$G = \bigcup_{i=1}^{k} x_i H$$

Proof:

Let $x_1H, x_2H, \cdots, x_kH$ denote the distinct left cosets of H in G. Then, for each a in G, we have $aH = x_iH$, for some i.

Also, we have $a = ae \in aH = x_iH$, for some i.

Thus, each element of G belongs to one of the cosets x_iH.

Lagrange's Theorem -

If G is a finite group and H is a subgroup of G, then $O(H)$ is a divisor of $O(G)$.

Proof -

Let G be a finite group and H is a subgroup of G with $O(G) = n$, $O(H) = m$ (Since G is finite, H is also finite).

We know that any two left cosets are either disjoint or identical.

Now suppose $a_1H, a_2H, \cdots, a_kH$ are only distinct left coset of H in G.

$$\Rightarrow G = a_1H \cup a_2H \cup \cdots \cup a_kH$$

$$\Rightarrow O(G) = O(a_1H) + O(a_2H) + \cdots + O(a_kH)$$

$$= O(H) + O(H) + \cdots + O(H) \quad \text{(since every left coset has } O(H) \text{ elements)}$$

$$= k\,O(H)$$

$$\Rightarrow n = k \cdot m$$

$$\Rightarrow k = (n/m).$$ Hence $O(H)$ divides $O(G)$.

Def.

If H is a subgroup of G, then the index of H in G is the number of distinct right cosets of H in G.

It is denoted by $i(H)$ or $|G:H|$ or $(G:H)$.

Problem.

The order of every element of a finite group divides the order of the group.

Proof. Suppose G is a finite group and $a \in G$.

Let $O(G) = n$ and $O(a) = m$.

Let $H = \{a, a^2, \ldots, a^m = e\}$.

Clearly H is a subgroup of G.

To show: $O(H) = m$.

Suppose $O(H) < m$.

Then $a^i = a^j$, for some $0 \le i, j \le m$

$\Rightarrow a^i \cdot a^{-j} = a^j \cdot a^{-j}$ (if $j < i$)

$\Rightarrow a^{i-j} = a^0 = e$, where $0 < i-j < m$, which is a contradiction (since m is the least +ve integere such that $a^m = e$).

Therefore $O(H) = m = O(a)$.

Hence by Lagrange's theoreem $O(H) \mid O(G)$.

$\therefore O(a) \mid O(G)$.

Problem.

Any groop of preime oredere is cyclic.

Proof. Let G be a groop of oredere p, where p is preime numbere.

Since $p \geq 2$, G has at least one non-identity element, say 'g'.

Then $O(g) \mid O(G)$

That is, $o(g) \mid p$, which implies that $O(g) = 1$ ore p

But $g \neq e \Rightarrow O(g) \neq 1$.

Thus, $o(\langle g \rangle) = o(g) = p$.

$\Rightarrow o(\langle g \rangle) = o(G)$.

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

Problem -

Show that any group with at most five elements is abelian.

Sol^n - Since every group of prime order is cyclic, we have the groups of orders 2, 3 or 5 are cyclic.

Consider a group G of order 4.

If G has an element a of order 4, then $G = \langle a \rangle$.

Hence, G is cyclic.

Otherwise, every element $\neq e$ is of order 2;

that is, $G = \{e, a, b, c\}$ and $a^2 = b^2 = c^2 = e$.

Consider the product ab.

If $ab = e$, then $ab = aa$, which implies $b = a$, a contradiction.

Hence, $ab \neq e$.

Similarly, $ab \neq a$, $ab \neq b$.

Hence $ab = c$.

By the similare aregument, $ba = c$, $bc = a = cb$,

and $ca = b = ac$.

Hence, G is abelian.

Thus, all groups of oredere < 6 aree abelian.

Normal Subgroup

Def:

A subgroup N of G is said to be a normal subgroup of G if for every $g \in G$, $gNg^{-1} \subseteq N$.

We denote it by $N \trianglelefteq G$ or $N \triangleleft G$.

Note:

The statement $gNg^{-1} \subseteq N$ is equivalent to the statement that for all $n \in N$, $gng^{-1} \in N$.

Ex-

For any group, the trivial subgroup and G itself are always the normal subgroups.

* A non-trivial group that has no normal subgroups other than these two is called a simple group.

Exercise 7.

1. If G is an Abelian group, which subgroups of G are normal?
2. Prove that a finite Abelian group is simple if and only if its order is a prime number. Hint: Every element generates a subgroup.
3. For any group G, prove that its centre $Z(G)$ is always a normal subgroup.
4. Let $H \leq G$ (not necessarily normal), and define $N = \bigcap_{x \in G} xHx^{-1}$. Show that $N \trianglelefteq G$.
5. Let N be a subgroup of index 2 in G (i.e., $|G : N| = 2$). Show that $N \trianglelefteq G$. Hint: If N has only two left cosets, and only two right cosets, and one of them is N in each case, what is the other?

Theorem.

Let $N \leq G$. Then $N \trianglelefteq G$ if and only if fore all $x \in G$, $xNx^{-1} = N$.

Soln. If $N \trianglelefteq G$, then fore any $x \in G$, $xNx^{-1} \subseteq N$. ——①

To show: $N \subseteq xNx^{-1}$.

Since $x \in G$, we have $x^{-1} \in G$.

Therefore $x^{-1}N(x^{-1})^{-1} \subseteq N$

$\Rightarrow x^{-1}Nx \subseteq N$

$\Rightarrow xx^{-1}Nx \subseteq xN$

$\Rightarrow Nx \subseteq xN$

$\Rightarrow Nxx^{-1} \subseteq xNx^{-1}$

$\Rightarrow N \subseteq xNx^{-1}$ ——②

From ① and ②, we have that $N = xNx^{-1}$.

Converse: Suppose that $xNx^{-1} = N$, fore everey $x \in G$.

$\Rightarrow xNx^{-1} \subseteq N$

Therefore, N is a noremal subgroup of G.

Problem.

(i) The subgroup N of G is normal subgroup of G if and only if every left coset of N is a right coset of N in G.

[ii] Prove that if the index of subgroup H in group G is 2, then H is normal.

Soln. (i) Suppose N is normal in G.

$\Rightarrow gng^{-1} \in N$, for every $n \in N$, $g \in G$.

$\Rightarrow gng^{-1} = n'$, for some $n' \in N$.

$\Rightarrow gn = n'g \in Ng$

Thus $gN \subseteq Ng$.

Since $g \in N$, we have $g^{-1} \in N$.

$\Rightarrow g^{-1}n(g^{-1})^{-1} \in N$, for every $n \in N$.

$\Rightarrow g^{-1}ng \in N$

$\Rightarrow g^{-1}ng = n''$, for some $n'' \in N$.

$\Rightarrow ng = gn'' \in gN$.

Therefore $Ng \subseteq gN$.

$\therefore Ng = gN$.

$\therefore$ Every left coset of N in G is a right coset of N in G.

Converse:

Suppose every left coset of N in G is a right coset of N in G.

Then for every $x \in G$, $xN = Nx$.

Let $xn \in xN = Nx$.

Then $xn = n'x$, for some $n' \in N$.

$\Rightarrow xnx^{-1} = n' \in N$

$\Rightarrow xnx^{-1} \in N$.

Therefore, N is a normal subgroup of G.

(ii) Suppose that $(G:N) = 2$ (Index of H in G)

That is, the no. of distinct right/left cosets of N in $G = 2$.

Then the set of left cosets is $\{eN, aN\}$, where e is the identity element and $a \notin N$, $a \in G$.

The set of right cosets is $\{Ne, Na\}$.

Also, $G = N \cup aN = N \cup Na$

Then $Na = G - N = aN$

$\therefore$ Right cosets of N = left cosets of N.

$\Rightarrow$ By (i), N is normal.

Problem -

Show that $Z(G) = \{ g \in G \mid xg = gx, \forall x \in G \}$

(Centre of G) is a normal subgroup of G.

Soln - Since $e \in G$ s.t $xe = ex$, $\forall x \in G$, we have

$Z(G)$ is non-empty.

Let $a, b \in Z(G)$.

$\Rightarrow xa = ax$ and $xb = bx$, $\forall x \in G$.

To show: $ab^{-1} \in Z(G)$

Closure: $x(ab) = (xa)b$ [$\because$ Associative]

$= (ax)b$

$= a(xb)$

$= a(bx)$

$= (ab)x$

$\Rightarrow ab \in Z(G)$.

Inverse:

Let $a \in Z(G)$

$\Rightarrow xa = ax \quad , \quad \forall x \in G.$

$\Rightarrow xax^{-1} = axx^{-1}$ [Post multiply with x^{-1}]

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

$\Rightarrow x^{-1}xax^{-1} = x^{-1}a$ [Pre multiply with x^{-1}]

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

Therefore, $x^{-1} \in Z(G)$.

Thus $Z(G)$ is a subgroup of G.

To show: $Z(G)$ is normal.

Take $z \in Z(G)$ and $g \in G$. Then $zg = gz$, $\forall g \in G$.

Now, for any $x \in G$,

$$(gzg^{-1})x = (gz)g^{-1}x$$
$$= (zg)g^{-1}x$$
$$= z(gg^{-1})x$$
$$= zex$$

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

$$= xz \qquad [\because z \in Z(G)]$$

$$= xze$$

$$= xz(gg^{-1})$$

$$= x(zg)g^{-1}$$

$$= x(gz)g^{-1} \qquad [\because zg = gz]$$

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

$$\Rightarrow gzg^{-1} \in Z(G).$$

Therefore, $Z(G)$ is a normal subgroup of G.

Inverse:

Let $a \in Z(G)$. To show $a^{-1} \in Z(G)$.

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

$\Rightarrow xa = ax$, $\forall\, x \in G$.

$\Rightarrow a^{-1}xa = a^{-1}ax$ [Pre multiply with a^{-1}]

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

$\Rightarrow a^{-1}xaa^{-1} = xa^{-1}$ [Post multiply with a^{-1}]

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

Therefore, $x^{-1} \in Z(G)$.

Thus $Z(G)$ is a subgroup of G.