Subgroups

Set - III

Complex:

Any non-empty subset of a group G is called a 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 $MN = \{mn \in G / m \in M, n \in N\}$

$(MN)P = \{(mn)p \in G / m \in M, n \in N, p \in P\}$

$= \{m(np) \in G / m \in M, n \in N, p \in P\}$

$= M(NP)$

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

$$MN = \{mn \in G / m \in M, n \in N\}$$

$$\text{Now } (MN)^{-1} = \{(mn)^{-1} \in G / m \in M, n \in N\}$$

$$= \{n^{-1}m^{-1} \in G / m \in M, n \in N\}$$

$$= N^{-1}M^{-1}.$$

Subgroup:

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

$H_1 = (\{0\}, +_6)$, $H_2 = (\{0,3\}, +_6)$, $H_3 = (\{0,2,4\}, +_6)$

$\therefore H_1, H_2$ & H_3 are subgroups of G.

(5) $G = (\mathbb{Z}, +)$

$H_1 = \{3^n, n \in N\}$ is not a subgroups 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.

Ex: $H = \{-1\}$ 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 $x \in HH$

Let $x = h_1 h_2$ 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) $a \in H \Rightarrow \bar{a}^1 \in H$.

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) $a \in H \Rightarrow \bar{a}^1 \in H$

Conversely suppose that $H \subseteq G$ and

(i) $a, b \in H \Rightarrow ab \in H$;

(ii) $a \in H \Rightarrow \bar{a}^1 \in H$.

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) $\forall a \in H \subseteq G \Rightarrow \bar{a}^1 \in H \subseteq G$ (by (ii))

∴ $a \in H, \bar{a}^1 \in H \Rightarrow a\bar{a}^1 \in H \subseteq G$ (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 prop. of G)

∴ Identity axiom in H is satisfied.

(4) Since $a \in H \Rightarrow \bar{a}^1 \in H$

∴ 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

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

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 $b \in H \Rightarrow \bar{b}^1 \in H$

By closure axiom $a \in H, \bar{b}^1 \in H \Rightarrow a\bar{b}^1 \in H$.

S.C: Given that $a \in H, b \in H \Rightarrow a\bar{b}^1 \in H$

we have to prove that H is a subgroup of G.

Existence of identity:

$a \in H, a \in H \Rightarrow a\bar{a}^1 \in H \subseteq G$ (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:

$a = e \in H$; $b = a \in H \Rightarrow e\bar{a}^1 \in H \subseteq G$ (by hyp)

$\Rightarrow \bar{a}^1 \in H$ (by identity in G)

$\therefore \exists \bar{a}^1 \in H$ such that $a\bar{a}^1 = \bar{a}^1 a = e$.

$\therefore$ Inverse axiom is satisfied and $\bar{a}^1$ is the inverse of a in H.

Closure prop:

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

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

proof:

N.C:

Let H be a subgroup of G

TO P.T $H H^{-1} \subseteq H$

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

then $a \in H, b \in H$

Since H is a group

$\forall a \in H, b \in H$.

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

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

$\therefore H H^{-1} \subseteq H$.

S.C:

Let $H H^{-1} \subseteq H$

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

Since $H H^{-1} \subseteq H$

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

$\therefore$ 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.

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 repitition 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 $r > s$.

$\Rightarrow a^r \cdot a^{-s} = a^s \cdot a^{-s}$ $(\because a^s \in G \Rightarrow a^{-s} \in G)$

$\Rightarrow a^{r-s} = a^0$

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

$a \cdot a^{r-s-1} = a^{r-s} = e = a^{r-s-1} \cdot a$.

$\therefore$ 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

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

$= H(KK^{-1})H^{-1}$ ($\because$ complex multiplication is also.)

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

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

$= (KH)H^{-1}$ (by hyp)

$= K(HH^{-1})$

$= KH$ ($\because$ H is a subgroup of G $\Rightarrow HH^{-1} = H$)

$= HK$ (by hyp)

$\therefore HK$ is a subgroup of G

2nd part:

Let HK be a subgroup of G.

$\therefore (HK)^{-1} = HK$

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

$\Rightarrow KH = HK$ ($\because$ H & K are subgroups $\therefore H^{-1} = H$ & $K^{-1} = K$)

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 $a, b \in H$

$\Rightarrow a, b \in \bigcap_{i \in N} H_i$

$\Rightarrow a, b \in H_i \ \forall i \in N$

$\Rightarrow ab^{-1} \in H_i \ \forall i \in N$ ($\because H_i$ 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.

Sol: 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 $+$.

Now $H_1 \cup H_2 = \{\ldots\ldots -9, -6, -4, -3, -2, 0, 2, 3, 6, 9, \ldots\}$

$2, 3 \in H_1 \cup H_2$

$\Rightarrow 2+3 = 5 \notin H_1 \cup H_2$

$H_1 \cup H_2$ 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 $b \in H_2 \Rightarrow b^{-1} \in H_2$

$\therefore b^{-1} \in H_2$, $ab \in H_2$

$\Rightarrow (ab)b^{-1} \in H_2$ by closure

$\Rightarrow a(bb^{-1}) \in H_2$

$\Rightarrow ae \in H_2$

$\Rightarrow a \in H_2$

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 $G = \{\ldots\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\ldots\}$ be the additive group of integers.

Let m be the fixed integer

Let $H = \{\ldots\ldots -3m, -2m, -m, 0, m, 2m, 3m, \ldots\ldots\}$

$= \{3m / m \in I\} \subseteq G$

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 $H = \{a^n / n \in I\}$

$= \{\ldots\ldots \bar{a}^3, \bar{a}^2, \bar{a}^1, a^0, a^1, a^2, \ldots\}$

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 $\bar{a}^s$.

Now we have

$ab^{-1} = a^r(a^s)^{-1}$

$= a^r \bar{a}^s$

$= a^{r-s} \in H$. $(\because r, s \in I \Rightarrow r-s \in I)$

$\therefore H$ 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 $3 \in G$

$$H = \{\cdots \bar{3}^3, \bar{3}^2, \bar{3}^2, 3^0, 3^1, 3^2, 3^3, \cdots\}$$

is a subgroup of G.

Prob 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 abelian group.

Does the subset H of all these elements of G which are of the form $(1,b)$ form a subgroup of G?

Soln: 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 $(a,b)\in G$ $\quad \exists\ (c,d)\in G$

$a\neq 0, b\in\mathbb{R}$ $\qquad c\neq 0, d\in\mathbb{R}$

such that $(c,d)\times(a,b) = (a,b)$

$$\Rightarrow (ca, da+b) = (a,b)$$
$$\Rightarrow ca = a, \ \& \ da+b = b$$
$$\Rightarrow c = 1 \ \& \ da = 0 \Rightarrow d = 0 \quad (\because a\neq 0)$$

$\therefore (c,d) = (1,0)\in G$

$\therefore$ $\forall\ (a,b)\in G$, $a\neq 0, b\in\mathbb{R}$ $\quad \exists\ (1,0)\in G$ 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 $(c,d)\times(a,b) = (1,0)$

$$\Rightarrow (ca, da+b) = (1,0)$$
$$\Rightarrow ca = 1, \ da+b = 0$$
$$\Rightarrow c = \frac{1}{a}, \ d = -\frac{b}{a} \quad (\because a\neq 0)$$

$\therefore (c,d) = \left(\frac{1}{a}, -\frac{b}{a}\right)\in G$ $\quad a\neq 0, b\in\mathbb{R}$

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

$$x \times y^{-1} = (1,b) \times (1,c)^{-1}$$
$$= (1,b) \times (1,-c)$$
$$= (1 \cdot 1, b \cdot 1 + (-c))$$
$$= (1, b-c) \in H$$

($\because b, c \in \mathbb{R} \Rightarrow b-c \in \mathbb{R}$)

$\therefore H$ 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 $\mathbb{R}$.

Soln: 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 $XY^{-1} = \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix}^{-1}$

$$= \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \frac{1}{a_2} & -\frac{b_2}{a_2} \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} \frac{a_1}{a_2} & -\frac{a_1 b_2}{a_2} + b_1 \\ 0 & 1 \end{pmatrix} \quad \left(\because \frac{a_1}{a_2} \neq 0,\ -\frac{a_1 b_2}{a_2} + b_1 \in \mathbb{R}\right)$$

$\therefore H$ 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^n: Since $ea = ae$.

$\therefore e \in N(a)$

$\therefore N(a)$ is non-empty set.

i.e., $N(a) \neq \phi$.

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 asso. 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 $xy^{-1} \in N(a)$.

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 asso. 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

$bx = xb \ \forall x \in G$

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

$\Rightarrow (\bar{b}^{1}b)x = (b^{-1}x)b$ (by asso.)

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

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

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

$\Rightarrow xb^{-1} = \bar{b}^{1}x \ \forall x \in G.$

$\therefore \bar{b}^{1} \in Z$

Now we shall show that $ab^{-1} \in Z$.

Now we have $xb^{-1} = b^{-1}x \ \forall x \in G$

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

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

$\Rightarrow (xa)b^{-1} = (ab^{-1})x$ $(\because ax = xa)$

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

$\therefore ab^{-1} \in Z$

$\therefore Z$ is a subgroup of G.

→ Show that $aHa^{-1} = \{aha^{-1} / h \in H\}$ is a subgroup of G. where H is a 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.
$h_1 \in H, h_2 \in H$
$\Rightarrow h_1 \in H, h_2^{-1} \in H$
$\Rightarrow h_1h_2^{-1} \in H)$

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

$\therefore aHa^{-1}$ 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 asso.)

$\Rightarrow ea^2 = (y^{-1}a^2)y$.

$\Rightarrow a^2 = (y^{-1}a^2)y$

$\Rightarrow a^2y^{-1} = (y^{-1}a^2)yy^{-1}$

$\Rightarrow a^2y^{-1} = (y^{-1}a^2)e$

$\Rightarrow a^2y^{-1} = y^{-1}a^2$

$\Rightarrow y^{-1}a^2 = a^2y^{-1}$

$\therefore y^{-1} \in H.$

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 $xa = ax$ & $ya = ay$.

we have $ya = ay \Rightarrow y^{-1}(ya) = y^{-1}(ay)$

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

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

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

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

$\Rightarrow ay^{-1} = y^{-1}a$

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

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

$\Rightarrow (ax)y^{-1} = (xy^{-1})a \quad (\because ax = xa)$

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

$\therefore xy^{-1} \in K.$

$\therefore K$ 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.

Sol^n: 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.

$(\because i^2 = j^2 = k^2 = -1$

$i \cdot j = -j \cdot i = k, \; j \cdot k = -k \cdot j = i$

$k \cdot i = -i \cdot k = j)$

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_1 a subgroup of $\mathbb{R}$?

Ans: $G_1 \subseteq \mathbb{R}$ 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 $He = H$

$\therefore$ 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.

$\therefore a \in G, e \in H \Rightarrow ea \in Ha$ & $ae \in aH$.

$\Rightarrow a \in Ha$ & $a \in aH$.

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 the 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 (say).

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. $a \in H \subseteq G$

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.

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

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

$\Rightarrow h_1 \in H$.

$\therefore h = ah_1 \in aH$

$\Rightarrow h \in aH$

$\therefore H \subseteq aH$ —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 $b \in aH$

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

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

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

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

NOW $\bar{a}^{-1}b \in H \Rightarrow \bar{a}^{-1}bH = H$ $\quad (\because e \in H \Rightarrow eH = H)$

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

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

$\Rightarrow e(bH) = aH$

$\Rightarrow bH = aH.$

$\Rightarrow aH = bH.$

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

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

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

$\Rightarrow (b^{-1}a)H = H \quad (\because a \in H \Rightarrow aH = H)$

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

$\Rightarrow (bb^{-1})aH = bH$

$\Rightarrow e(aH) = bH.$

$aH = Hb.$

Conversely Let $aH = bH$

$\Rightarrow a \in aH$

$\Rightarrow a \in bH.$

Similarly we can prove that $a \in Hb \Leftrightarrow Ha = Hb.$

→ 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})

$\Rightarrow (b^{-1}a)h_1 = (b^{-1}b)h_2$

$\Rightarrow (b^{-1}a)h_1 = h_2$ $(\because b^{-1}b = e)$

$\Rightarrow (b^{-1}a)h_1 H = h_2 H$. $(\because K \in H \Rightarrow KH = H)$

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

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

$\Rightarrow (bb^{-1})aH = bH$.

$\Rightarrow aH = bH$

$\therefore$ 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.

proof: Given that H is a subgroup of G.

To prove that G = the union of all left cosets of H in G.

Let $H, aH, bH, cH, \ldots$ be all left cosets of H in G where $a, b, c, \ldots \in G$.

$\therefore H \cup aH \cup bH \cup \ldots \subseteq G$.

$$\Rightarrow \bigcup_{a \in G} aH \subseteq G \quad \text{---(1)}$$

W.K.T $a \in G \Rightarrow a \in aH$

$$\Rightarrow a \in \bigcup_{a \in G} aH$$

$$\Rightarrow G \subseteq \bigcup_{a \in G} aH \quad \text{---(2)}$$

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 $a, b \in G$.

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.

$x \in \bar{a} \Leftrightarrow x \equiv a \pmod H$ for $x, a \in G$

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

$\Leftrightarrow a^{-1}x = h \in H$, for some $h \in H$.

$\Leftrightarrow a(a^{-1}x) = ah \in aH$ for some $h \in H$.

$\Leftrightarrow (aa^{-1})x = ah \in aH$ 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: $G = \{-1, 1, i, -i\}$
$H = \{-1, 1\} \subseteq G$
$-1 \cdot H = \{1, -1\} = H$
$1 \cdot H = \{-1, 1\} = H$ and $i \cdot H = \{-i, i\}$
& $-i \cdot H = \{-i, i\}$

$i \cdot H = -i \cdot H$ & $1 \cdot H = -1 \cdot H$.
$\therefore$ 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. ($\because$ 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 of 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 doesnot 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 $0 \le i, j < m$

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 $0 \le j < i < m$

$\Rightarrow a^i \bar{a}^j = a^j \bar{a}^j$ ($\because a^j \in G$, $\bar{a}^j \in G$)

$\Rightarrow a^{i-j} = a^0$

$= e$ 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 $O(H) = p = O(G)$

$\Rightarrow G = H$.

$\therefore$ 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, $Ha \neq Hb \iff a^{-1}H \neq b^{-1}H$.

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.

Sol^n: Since H & K are two subgroups of G.

$\therefore H \cap K$ is also subgroup of G.

W.K.T $(H \cap K)a = Ha \cap Ka$ $\forall a \in G$.

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.

→ 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 $k_i k_j^{-1} \in K$ ($\because K < G$, $\therefore k_i, k_j \in K \Rightarrow k_i k_j^{-1} \in K$)

$\Rightarrow k_i k_j^{-1} \in H \cap K = T$

$\Rightarrow Tk_i = Tk_j$ $(\because ab^{-1} \in H \Rightarrow Ha = Hb)$

which is a contradiction.

$\therefore Hk_1, Hk_2, \ldots\ldots Hk_m$ are all distinct

from (2) we obtain

$$o(HK) = o(Hk_1) + o(Hk_2) + \ldots\ldots + o(Hk_m)$$
$$= o(H) + o(H) + \ldots\ldots + o(H) \text{ (m times)}$$

($\because He = H$: i.e., H 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

$\therefore HK \subseteq G$

$\therefore o(HK) \leq o(G)$

$\Rightarrow o(G) \geq o(HK)$

$$= \frac{o(H) \cdot o(K)}{o(H \cap K)}$$
$$> \frac{\sqrt{o(G)} \cdot \sqrt{o(G)}}{o(H \cap K)} \quad \text{(by hyp)}$$
$$= \frac{o(G)}{o(H \cap K)}$$

$$\therefore o(G) > \frac{o(G)}{o(H \cap K)}$$

$\Rightarrow o(H \cap K) > 1$

Hence $H \cap K \neq \{e\}$

→ 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.

$\therefore$ our assumption that the two subgroups H & K of 7 is wrong.

$\therefore$ 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 where

$o(H) = o(K) = p$; $H \neq K$

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.

Soln: 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 $KH = \{I, (1\,2), (1\,3), (1\,3)(1\,2)\}$

$= \{I, (1\,2), (1\,3), (1\,2\,3)\}$

Since $HK \neq KH$

$\therefore HK$ is not a subgroup of $G = S_3$.

(or)

$O(HK)$ doesnot divide $O(S_3) = 6$.

$\therefore$ By Lagrange's theorem,

HK is not a subgroup of S_3.
