Theorem 3 : In a group $(G, *)$, $(a*b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$.

Proof : Let $x = a*b$, $y = b^{-1} * a^{-1}$

Now, $x * y = (a*b) * (b^{-1} * a^{-1})$

$= a * (b * b^{-1}) * a^{-1}$ Associative

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

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

$= e$

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

$= b^{-1} * (a^{-1} * a) * b$ Associative

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

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

$= e$

$x * y = e$ and $y * x = e \Longrightarrow x^{-1} = y$

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

Note: $(a*b*c)^{-1} = c^{-1} * b^{-1} * a^{-1}$

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

Theorem 4: In a group $(G, *)$.
(i) $a*b = a*c \Rightarrow b = c$ (Left cancellation law)
(ii) $a*b = c*b \Rightarrow a = c$ (Right cancellation law)

Proof: $a*b = a*c$

operate by a^{-1} on left

$a^{-1}*(a*b) = a^{-1}*(a*c)$
$(a^{-1}*a)*b = (a^{-1}*a)*c$ — Associative
$e*b = e*c$ — $a^{-1}*a = e$
$b = c$ — $e*b = b$ ($\because e$ is identity)

$a*b = c*b$
operating by b^{-1} on right

$(a*b)*b^{-1} = (c*b)*b^{-1}$ — Associative
$a*(b*b^{-1}) = c*(b*b^{-1})$ — identity
$a*e = c*e$
$a = c$

Theorem 5: In a group $(G, *)$, the equations $a * x = b$ and $y * a = b$, $a, b \in G$ have unique solutions in G.

Proof: Consider the equation $a * x = b$ — ①

operate ① by a^{-1} on left

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

$$(a^{-1} * a) * x = a^{-1} * b \quad \text{Associative}$$

$$e * x = a^{-1} * b \quad \text{identity}$$

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

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

To prove the uniqueness

Let x_1 and x_2 be 2 solns of ①

i.e., $a * x_1 = b$ and $a * x_2 = b$

$\Rightarrow a * x_1 = a * x_2$

$\Rightarrow x_1 = x_2$ (Left cancellation law)

$\Rightarrow a * x = b$ has unique sol^n in G.

Consider $y * a = b$ — ②

operate by a^{-1} on right

$$(y * a) * a^{-1} = b * a^{-1}$$

$$y * (a * a^{-1}) = b * a^{-1}$$

$$y * e = b * a^{-1}$$

$$y = b * a^{-1} \in G \quad \because b \in G,\ a^{-1} \in G$$

To prove uniqueness

Let y_1 and y_2 be 2 sol^ns of ②

$y_1 * a = b$ and $y_2 * a = b$

$\Rightarrow y_1 * a = y_2 * a$

$\Rightarrow y_1 = y_2$ right cancellation

Problems :

Q1 : In a group $(G, *)$, if $(a*b)^2 = a^2 * b^2$, $a, b \in G$, then show that G is abelian.

Soln : Given $(a*b)^2 = a^2 * b^2$

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

$$a*(b*a)*b = a*(a*b)*b \quad \text{Associative}$$

using left & right cancellation law we get

$$b*a = a*b$$

$\Rightarrow$ G is abelian.

Q2: Let G be a group in which every element is inverse of itself. Then show that G is abelian.

Soln : Given for $a, b \in G$, $a*a=e$ and $b*b=e$.

As $a*b \in G$,

$$(a*b)*(a*b) = e = e*e$$

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

Associative & $\boxed{\begin{array}{l} e=a*a \\ e=b*a \end{array}}$

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

By left and right cancellation law we get

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

$\Rightarrow$ G is abelian.

Q3: In a group $(G, *)$, if $a^2 = e$, for all $a \in G$, show that G is abelian.

Soln: $a^2 = e$

$a * a = e$ operate by a^{-1} on left

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

$(a^{-1} * a) * a = a^{-1}$ Associative & identity

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

$a = a^{-1}$

$\Rightarrow$ every element is inverse of itself

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

$\underline{\underline{a * b = b * a}}$

Q4: If a group $(G, *)$ has even number of elements, then show that at least one element (other than identity) must be its own inverse.

Soln: G is a group with $2n$ elements.

$G = \{e, a_1, a_2, \cdots a_{2n-2}, a_{2n-1}\}$

suppose $(a_1 \text{ and } a_2)$, $(a_3 \text{ and } a_4) \cdots (a_{2n-3} \text{ and } a_{2n-2})$

Then $a_{2n-1}^{-1} = a_{2n-1}$

Subgroup: Let $(G, *)$ be a group and H be a non empty subset of G.
H is said to be a **subgroup** of G, if H itself forms a group under $*$.

Example: 1) $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$

2) $\{\mathbb{Q} - \{0\}, \cdot\}$ is a subgroup of $(\mathbb{R} - \{0\}, \cdot)$

$\{i \; -1\}$

3) Let $G = \{1, -1, i, -i\}$

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	$+1$
$-i$	$-i$	i	1	-1

$(G, \cdot)$ is a group.

$\boxed{e = 1}$

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

$i^{-1} = -i$ $\quad (-i)^{-1} = i$

Let $H_1 = \{1, -1\}$ is a subset of G and it forms a group w.r.to multiplication.

$\boxed{H_3 = \{1 \;\; i \;\; -i\} \text{ is it a subgroup}}$

$\cdot$	1	-1
1	1	-1
-1	-1	1

identity $= 1$

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

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

Check whether $H_2 = \{i, -i\}$ is a subgroup

No (Since identity element is not there)

Note: $\{e\}$ and G are always subgroups of G and are called trivial subgroups

Problems :

Q1: A non empty subset H of a group $(G, *)$ is a subgroup of G if and only if the following are satisfied.

(i) $a * b \in H$, for all $a, b \in H$
(ii) $a^{-1} \in H$ for all $a \in H$

Soln: Suppose H is a subgroup of G, then (i) and (ii) follows by definition of subgroup.

Suppose H is a non empty subset of G satisfying (i) and (ii). To prove H is a subgroup of G.

Closure and inverse property follows from (i) and (ii). To check whether Associativity & identity law satisfied in H.

Elements of H are also elements of G. $\Rightarrow$ Associativity follows from G.

$\because$ $H \neq \phi$, there is an element $a \in H$

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

Now by (i), $a \in H$ and $a^{-1} \in H \Longrightarrow a * a^{-1} = e \in H$

$\Rightarrow$ Identity element exist.

$\Rightarrow$ H is a subgroup.

Q2: A non empty subset H of a group $(G, *)$ is a subgroup of G if and only if $a * b^{-1} \in H$ for all $a, b \in H$.

Soln: Suppose H is a subgroup of G.
As $a \in H$ and $b^{-1} \in H$, by closure property

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

Conversely, if $a * b^{-1} \in H$ for all $a, b \in H$, to prove H is a subgroup of G.

Since $H \neq \phi$, there is an element $a \in H$.

$\because$ $a \in H$ and $a \in H$ $\Rightarrow$ $a * a^{-1} \in H$ $\Rightarrow$ $e \in H$

$\Rightarrow$ identity element exist

$\because$ $e \in H$, $a \in H$ $\Rightarrow$ $e * a^{-1} \in H$ $\Rightarrow$ $a^{-1} \in H$

$\Rightarrow$ inverse exist

Since H is a subset of G, Associativity follows.

Let $a, b \in H$

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

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

$a * b \in H$

$\Rightarrow$ closure property.

$\Rightarrow$ $(H, *)$ is a group

$\Rightarrow$ H is a subgroup of G.

Q3: Let $(G, *)$ be a group. Let H_1 and H_2 be subgroups of G. Test whether $H_1 \cap H_2$ and $H_1 \cup H_2$ are subgroups of G.

Soln: Let H_1 and H_2 be subgroups of G.

So, by defn of subgroup, $e \in H_1$ also $e \in H_2$

$\Rightarrow e \in H_1 \cap H_2 \Rightarrow H_1 \cap H_2 \neq \phi$.

To prove $H_1 \cap H_2$ is a subgroup of G, we show that for $a, b \in H_1 \cap H_2$, $a * b^{-1} \in H_1 \cap H_2$.

Let $a, b \in H_1 \cap H_2$.

$\Rightarrow a, b \in H_1$ and $a, b \in H_2$

$\Rightarrow a * b^{-1} \in H_1$ and $a * b^{-1} \in H_2$

$\Rightarrow a * b^{-1} \in H_1 \cap H_2$

$\Rightarrow H_1 \cap H_2$ is a subgroup of G.

But $H_1 \cup H_2$ is not necessarily a subgroup of G.

Eg: Consider the group $(\mathbb{Z}, +)$.

Let $H_1 = \{2n \mid n \in \mathbb{Z}\} = \{\ldots -6, -4, -2, 0, 2, 4 \ldots\}$

& $H_2 = \{3n \mid n \in \mathbb{Z}\} = \{\ldots -9, -6, -3, 0, 3, 6 \ldots\}$

But $H_1 \cup H_2$ is not a subgroup of G.

Because $2, 3 \in H_1 \cup H_2$ but $2 + 3 = 5 \notin H_1 \cup H_2$

Closure property is not satisfied.

Note: If $H_1 \cup H_2 = H_1$ or $H_1 \cup H_2 = H_2$, then $H_1 \cup H_2$ is a subgroup of G.

Eg: $H_1 : \{n \mid n \in \mathbb{Z}\}$ ✓
$H_2 : \{2n \mid n \in \mathbb{Z}\}$

Suppose neither $H_1 \cup H_2 = H_1$ nor $H_1 \cup H_2 = H_2$ then there is an element $x \in H_1$ with $x \notin H_2$ & $y \in H_2$ with $y \notin H_1$.

If $x * y \in H_1$ as $x^{-1} \in H_1$ then $x^{-1} * (x * y) = y \in H_1$ contradiction.

If $x * y \in H_2$ as $y^{-1} \in H_2$, then $(x * y) * y^{-1} = x \in H_2$. a contradiction.

$\Rightarrow x * y \notin H_1 \cup H_2$

$\Rightarrow H_1 \cup H_2$ is not a subgroup of G.

Q4: Let $(H, \circ)$ and $(K, \circ)$ be 2 subgroups of a group $(G, \circ)$. Define $HK = \{(h \circ k) \mid h \in H, k \in K\}$. Prove that $(HK, \circ)$ is a subgroup of $(G, \circ)$ if and only if $HK = KH$.

Soln: Suppose HK is a subgroup of G. To prove $HK = KH$.

Let $x \in KH \Rightarrow x = kh$ for some $k \in K$, $h \in H$

$x^{-1} = (kh)^{-1} = h^{-1}k^{-1} \in HK$

$x^{-1} \in HK$ & as HK is a subgroup we have

$$(x^{-1})^{-1} = x \in HK$$

$\therefore x \in KH$ and $x \in HK \Rightarrow KH \subseteq HK$ — (1)

Similarly we can show $HK \subseteq KH$ — (2)

$\Rightarrow \underline{\underline{HK = KH}}$

Conversely, let $HK = KH$. To prove HK is a subgroup of G.

$e \in H, e \in K \Rightarrow e \cdot e = e \in HK \Rightarrow HK \neq \phi$

Let $a, b \in HK$, then $a = h_1 k_1$ and $b = h_2 k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$.

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

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

as $k_1 k_2^{-1} h_2^{-1} \in KH = HK \Rightarrow k_1 k_2^{-1} h_2^{-1} = h_3 k_3$ for some $h_3 \in H$, $k_3 \in K$

$\Rightarrow ab^{-1} = h_1 (h_3 k_3)$

$\Rightarrow ab^{-1} \in HK \Rightarrow HK$ is a subgroup of G.

Q5. Show that cube root of unity forms a group under multiplication.

Soln :

$\circ$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

1 is the identity element

ω is inverse of ω^2

Closure & associativity property satisfied.

$\Rightarrow$ Is a Group.