Problems:

(1) The algebraic structure $(I, +)$ where

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

is an abelian group.

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

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

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

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

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

(4) G = The set of $m \times n$ matrices is an abelian group w.r.t $b - 0$ $+^n$.

(5) V = The set of vectors is an abelian group w.r.t $b - 0$ $+^n$.

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

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

(8) The sets $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ of all rational, real and complex numbers are not groups w.r.t X^n. because the inverse of 0 is not defined.

(9) The sets $\mathbb{Q}^+$ and $\mathbb{R}^+$ of all +ive rational and real numbers are abelian groups under X^n.

(10) The sets $\mathbb{Q}^*$, $\mathbb{R}^*$ and $\mathbb{C}^*$ of all non-zero rational, real and complex numbers are abelian groups w.r.t X^n.

(11) Is the set of all rational number x s.t $0 < x \leq 1$, a group w.r.t X.

Sol^n: Let $G = \{ x \mid x$ is a rational number and $0 < x \leq 1 \}$ then it is not a group under X^n because if $a \in G$ and $0 < a < 1$ then inverse of 'a' is not possible in G.

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

(12) The set of all +ive rational numbers forms an abelian group under the composition $*$ defined by $a * b = \frac{ab}{2}$.

Elementary properties of Groups:

If G is a group with $b-o$
then the left and right cancellation laws hold in G.

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

$\Rightarrow b = c$ (L.C.L)

and (ii) $ba = ca$.

$\Rightarrow b = c$ (R.C.L)

Proof: Given that

G is a group w.r.t $b-o$.

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

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

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

Multiplying both sides a^{-1} on left.

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

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$ (Associative Property)

$\Rightarrow eb = ec$

$\Rightarrow b = c$ (Identity).

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

$\Rightarrow \boxed{b = c}$

→ If G is a group with b-o '$*$' then the left and right cancellation laws hold in G.

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

and $b*a = c*a \Rightarrow b = c$ (R.C.L).

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

⇒ If G is a group with b-o '$*$' and a & b are elements of G, then the linear eqns $ax = b$ and $ya = b$ have unique sol's x and y in G.

Proof :- Given that G is a group w.r.t b-o '$*$'

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

where 'e' is identity.

Now, we have

$ax = b$

multiplying both sides a^{-1} on left

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

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

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

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

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

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

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

we have,

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

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

To show that the sol^n is unique.

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

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

$\therefore$ The sol^n is unique.

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

Note: If G is a group with the b-o $*$ and a & b are two elements of G then the linear equations $a*x = b$ and $y*a = b$ have unique sol^n x and y in G.

Note [1]: cancellation laws hold in a group i.e

$\forall\ a, b, c \in G$.

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

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

[2] In a semi group, the cancellation laws may or may not hold.

Ex: Let S be the set of all 2×2 matrices with their elements as integers and X^n is b-o on 'S' then 'S' is a semi group but not satisfy the cancellations laws because if

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

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

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

3 $(N, +)$ is a semi group.

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

and $b+a = c+a$.

$\Rightarrow b = c$

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

$\therefore$ a semi group even if cancellation laws hold, the semi group is not a group.

4 A finite semi group $(G, \cdot)$ satisfy the cancellation laws is a group.

(or)

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

Uniqueness of identity:

The identity element in a group is unique

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

Since e_1 is an identity in G then

$$e_1 e_2 = e_2 = e_2 e_1 \quad \text{---(1)}$$

Since e_2 is identity in G then $e_1 e_2 = e_1 = e_2 e_1$ (2)

From (1) and (2), we have —

$$e_1 = e_1 e_2 = e_2$$

$$\Rightarrow \boxed{e_1 = e_2}$$

Uniqueness of Inverse:

Inverse of each element of a group is unique.

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

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

Since a' is an inverse of a in G.

$$\therefore aa' = a'a = e \quad \text{---(1)}$$

Since a'' is an inverse of a in G.

$$\therefore aa'' = a''a = e \quad \text{---(2)}$$

From (1) and (2), we have —

$$aa' = e = aa'' \Rightarrow aa' = aa''$$

$$\Rightarrow a' = a'' \text{ (By LCL)}$$

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

⇒ The identity element is its own inverse.

Since $ee = e \Rightarrow e^{-1} = e$.

⇒ If the inverse of a is a^{-1} then inverse of a^{-1} is a i.e $(a^{-1})^{-1} = a$.

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

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

$$aa^{-1} = a^{-1}a = e.$$

Now $aa^{-1} = e$

multiplying both sides with $(a^{-1})^{-1}$ on the right —

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

$$\Rightarrow a(a^{-1}(a^{-1})^{-1}) = (a^{-1})^{-1} \quad [\text{by associative and } e \text{ is identity}]$$

$$\Rightarrow a(e) = (a^{-1})^{-1} \quad [\because (a^{-1})^{-1} \text{ is inverse of } a^{-1}]$$

$$\Rightarrow a = (a^{-1})^{-1} \quad [\because e \text{ is identity}]$$

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

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

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

⇒ Let $(G, \cdot)$ be a group.

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

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

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

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

for $b \in G$, $\exists\, b^{-1} \in G \Rightarrow ab \in G$

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

Now we have

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} \quad \text{(by Associative)}$$
$$= a e a^{-1} \quad \text{by inverse}$$
$$= a a^{-1} \quad \text{by identity}$$
$$= e \quad \text{by inverse}$$
$$= e \quad \text{---} (1)$$

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

Now, we have

$$(b^{-1}a^{-1})(ab) = e \quad \text{---} (2)$$

from (1) and (2), we have

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

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

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

Let $(G, +)$ be a group then

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

(2) Generalization ——

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

Def^n of a group based upon Left Axioms (or) Right Axioms:

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

(i) closure property:-

$ab \in G$, $\forall a, b \in G$.

(ii) Associative property:

$(ab)c = a(bc)$ $\forall a, b, c \in G$.

(iii) Existence of left identity:

$\exists e \in G$ such that $ea = a$ $\forall a \in G$,

$\therefore$ the element 'e' is called left identity in G.

(iv) Existence of left inverse:

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

$$aa^{-1} = e.$$

$\therefore$ The element a^{-1} is called the left inverse of a in G.

Theorem :

The left identity is also the right identity if 'e' is the left identity then $ae = a$ & a

Proof : Let $(G, \cdot)$ be the given group. and let e be the left identity.

To prove that 'e' is also the right identity.

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

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

Now we have $a^{-1}(ae) = (a^{-1}a) \cdot e$ (by Associative).

$= e \cdot e$ (by inverse)

$= e$ (by identity)

i.e e is left identity.

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

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

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

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

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

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

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

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

To prove that $aa^{-1} = e$.

Now, we have —

$$a^{-1}(aa^{-1}) = (a^{-1}a)\,a^{-1} \quad (\text{by Associative})$$
$$= ea^{-1} \quad (\text{by inverse})$$
$$= a^{-1} \quad (\because e \text{ is the left identity})$$
$$= a^{-1}e \quad (\because e \text{ is also right identity})$$

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

$\Rightarrow aa^{-1} = e \quad (\text{by LCL})$.

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

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

Problems:

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

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

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

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

(i) Closure Property:

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

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

Here $|AB| \neq 0$

because $|A| \neq 0, |B| \neq 0$)

(ii) Associative property:

Matrices multiplication is associative.

(iii) Existence of left Identity:

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

$|A| \neq 0$

such that $IA = A$

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

(iv) Existence of left Inverse:

for each $A_{n\times n} \in M$; $|A| \neq 0$ $\exists A^{-1} = \frac{adj\, A}{|A|}$

$(\because |A| \neq 0)$

such that

$A^{-1}A = I_{n\times n}$ (left Identity)

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

(v) Commutative Property:

$\forall A, B \in M$; $|A| \neq 0$, $|B| \neq 0 \Rightarrow AB \neq BA$.

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

Note:

M is the set of all $n \times n$ non-singular matrices with their elements as integers is not a group w.r.t X^n because there is no inverse of all matrices in the given set.

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

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

Now, we have

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

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

Bored

S.T the set of matrices.

$$A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$$ where α is a real number forms a group under matrix multiplication.

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

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

Closure prop. where $\alpha, \beta \in \mathbb{R}$.

where $\alpha+\beta \in \mathbb{R}$

since

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

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

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

$\therefore$ Closure prop. is satisfied.

(ii) Associative Bop:-

Matrix multiplication is associative.

(iii) Existence of left Identity.

since $0 \in \mathbb{R}$

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

Let $A_\alpha \in G$, $\alpha \in R \Rightarrow A_0 \in G$; $0 \in \mathbb{R}$,

such that $A_0 A_\alpha = A_{0+\alpha} = A_\alpha$.

$\therefore A_0$ is left identity.

(iv) Existence of left inverse:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Solution:

(ii) since $a * b = a+b-ab \quad \forall a, b \in \mathbb{Q} - \{1\}$ — (A)

(1) closure prop:

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

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

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

(2) Associative property:

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

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

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

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

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

Similarly ——

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

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

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

(3) Existence of left identity prop'

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

then $e*a = a$

Now $e*a = a$

$\Rightarrow e+a-ea = a$

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

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

$e \notin Q-\{1\}$

$\therefore e*a = 0*a$

$= 0+a-0(a)$

$= a.$

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

$0*a = a$

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

Existence of left Inverse:

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

then $b * a = e$

Now
$$b * a = e \quad \text{(by A)}$$
$$\Rightarrow b + a - ba = 0$$
$$\Rightarrow b(1-a) = -a$$
$$\Rightarrow b = \frac{-a}{1-a} \quad (\because a \neq 1)$$
$$= \frac{a}{a-1} \in Q - \{1\}.$$

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

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

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

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

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

Subgroups

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 $(R, +)$

(2) I_E is a complex of the group $(Z, +)$

(3) I_o is a complex of the group $(R, +)$

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 MN of G.

⇒ The multiplication of complexes of a group G is associative.

Solution: Let M, N, P, be any three complexes in a group G.

Let $m \in M$, $n \in N$, $p \in P$ ⇒ $m, n, p \in G$.

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

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

Def" If M is a complex in a group G then we define $M^{-1} = \{m^{-1} \in G \mid m \in M\}$

i.e m^{-1} is the set of all inverse of the elements of M clearly $M^{-1} \subseteq G$.

⇒ If M, N are any two complexes in a group G, then $(MN)^{-1} = N^{-1}M^{-1}$

Solution :

We have

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

Now

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

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) $G = (I, +)$

$H_1 = (2I, +)$ & $H_2 = (3I, +)$

H_1 & H_2 are subgroups of G.

(2) $G = (R, +)$

$H_1 = (Q, +)$, $H_2 = (I, +)$

H_1 & H_2 are subgroups of G.

$G = (R - \{0\}, \cdot)$

$H_1 = (Q - \{0\}, \cdot)$, $H_2 = (\{1, -1\}, \cdot)$

$H_3 = (\{1\}, \cdot)$, $H_4 = (\{2^n / n \in I\}, \cdot)$

$H_5 = (Q^+, \cdot)$, $H_6 = (R^+, \cdot)$ & $H_7 = (\{3^n / n \in I\}, \cdot)$

$\therefore$ $H_1, H_2, H_3, H_4, H_5, H_6$ & 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) $G = (Z, +)$

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

Note: Every subgroup of G is complex of G: but every complex is not always a subgroup

Def^n: 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 def^n 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 def^n)

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

$\therefore H \subseteq H^{-1}$ — (2)

From (1) and (2), we have

$H^{-1} = H$

Proved

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: $H=\{-\}$ is a complex of multiplicative group

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

Since inverse of -1 is -1.

$$\therefore H^{-1}=\{-\}$$

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 $x=h_1h_2$ where $h_1 \in H$ & $h_2 \in H$

Since H is a subgroup of G.

$h_1h_2 \in H$

$\Rightarrow x \in H$

$\Rightarrow HH \subseteq H$ —— (1)

Let $h_3 \in H$ and e be the identity element in H.

$\therefore h_3 = h_3e \in HH$

$\Rightarrow h_3 \in HH$.

$\Rightarrow H \subseteq HH$ —— (2)

From (1) and (2), we have

$$HH=H.$$

⇒ G is a group and $H \subseteq G$; H is a subgroup of G. iff (i) $a, b \in H \Rightarrow ab \in H$

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

Proof : Let H be a subgroup of G.

∴ By defⁿ H is a group w.r.t the b-o defined in G.

By closure axiom (i) $a, b \in H \Rightarrow ab \in H$

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

Conversely suppose that $H \subseteq G$ and

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

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

To prove that H is a subgroup of G.

(i) since $a, b \in H \subseteq G \Rightarrow ab \in H$ by (i)

∴ H is closed

(ii) Let $a, b, c \in H \subseteq G \Rightarrow (ab)\cdot c = a(bc)$ (by asso. prop. in G).

∴ Asso. prop. in H is satisfied.

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

∴ $a \in H, a^{-1} \in H \Rightarrow aa^{-1} \in H \subseteq G$ (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 axioms in H is satisfied

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

$\therefore$ each element of H possesses inverse in H.

$\therefore$ H itself is a group for the composition in G

$\therefore$ 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

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

Proof: N.C

Let H be a subgroup of G.

then by def^n H is a group of G w.r.t b-o defined in G.

By inverse axiom $b \in H \Rightarrow b^{-1} \in H$

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

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

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

Existence of Identity:

$a \in H, a \in H \Rightarrow aa^{-1} \in H \subseteq G$ (by hypothesis).

$\Rightarrow e \in H$ (by inverse axiom of G).

$\therefore \exists\, e \in H$ such that $ae = ea = a \quad \forall a \in H$

$\therefore$ Identity property is satisfied.

and 'e' is the identity element in H.

Existence of Inverse:

$a = e \in H$; $b = a \in H \Rightarrow ea^{-1} \in H \subseteq G$ (by hypothesis)

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

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

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

Closure property

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

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

$\Rightarrow ab \in H$ $(\because (b^{-1})^{-1} = b)$

$\therefore$ closure axiom in H is satisfied.

Associative property:

let $a, b, c \in H \subseteq G$

then $(ab)c = a(bc)$ (By associative prop. in G)

$\therefore$ Associative prop. in H is satisfied.

$\therefore H$ itself is a group for the composition in G.

$\therefore H$ is a subgroup of G.

Note: If the operation in G is $+$ then condition in the above theorem can be stated as follows

$a \in H, b \in H \Rightarrow a - b \in H$.

Theorem: A necessary and sufficient condition for a non-empty subset H of a group G to be a subgroup of G is that $HH^{-1} \subseteq H$.

Proof:

N.C

Let H be a subgroup of G.

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

Let $ab^{-1} \in HH^{-1}$ (by def^n).

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

Since H is a group.

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

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

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

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

S.C Let $HH^{-1} \subseteq H$.

$\Rightarrow$ let $a, b \in H \Rightarrow ab^{-1} \in HH^{-1}$ (by def^n)

since $HH^{-1} \subseteq H$

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

$\therefore H$ is a subgroup of G.

Proved

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)

From (1) and (2), we have $HH^{-1} = H$.

S.C

Let $HH^{-1} = H$.

$\Rightarrow HH^{-1} \subseteq H$

$\therefore H$ is a subgroup of G.

Proved

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.

I^st 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

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

$= H(KK^{-1})H^{-1}$ (∵ complex multiplication is associative)

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

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

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

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

$= KH$ (∵ 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.

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

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

$\Rightarrow KH = HK$

(∵ 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. **Proved**

Theorem: Intersection of an arbitrary family of subgroups of a group is a subgroup of the group.

Proof: Let $H_1, H_2, H_3, \ldots$ be arbitrary family of subgroups of G.

To prove that

$H_1 \cap H_2 \cap H_3 \cap \ldots$ is a subgroup of G.

Let $H = H_1 \cap H_2 \cap - - - - \cdot$

$= \bigcap_{i \in N} H_i$

Let $a, b \in H$

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

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

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

Theorem: The union of two subgroups of a group need not be a subgroup of the group.

Solution: For Example

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

is a group w.r.t $+^n$.

Let $H_1 = \{2n \mid n \in I\}$

$= \{ - - - , -6, -4, -2, 0, 2, 4, 6, - - \}$

and

$H_2 = \{3^n \mid n \in I\}$

$= \{ - - - , -9, -6, -3, 0, 3, 6, 9, - - - \}$

are two subgroups of a w.r.t $+^n$.

Now

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

$2, 3 \in H_1 \cup H_2$

$\Rightarrow 2 + 3 = 5 \notin H_1 \cup H_2$, $H_1 \cup H_2$ 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) and (2), we have —

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

$\Rightarrow a \cdot b \in H_1 \cup H_2$

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 associative)

$\Rightarrow eb \in H_1$ (by inverse).

$\Rightarrow b \in H_1$ (by identity).

which is contradiction to $b \notin H_1$.

Let $ab \in H_2$

Let $b \in H_2 \Rightarrow b^{-1} \in H_2$

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

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

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

$\Rightarrow ae \in H_2$

$\Rightarrow a \in H_2$

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 $H_2 \subset H_1$

Hence Proved