Subgroup:

If a subset H of a group G is itself a group under the operation of G, we say that H is a subgroup of G.

Notation:

$H \leq G \Rightarrow H$ is a subgroup of G.

$H < G \Rightarrow H$ is a proper subgroup of G.

Example:

Consider $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$H = \{0, 2, 4\}$ is a subgroup of G.

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

$H_1 = \{0, 2, 3\}$ is not a subgroup of G.

$H_2 = \{0, 4\}$ is not a subgroup of G.

Subgroup Tests:

(I) One-Step Subgroup Test:

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

Proof: First,

Let H be a subgroup of G

and let $a, b \in H$ $\left(\because H \leq G\right.$ Inverse of b exists in H$\left.\right)$

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

$\Rightarrow ab^{-1} \in H$ (Closure property of H)

$\therefore ab^{-1} \in H \quad \forall\, a, b \in H$

Conversely ($\Leftarrow$) Let $ab^{-1} \in H \quad \forall\, a, b \in H$

TS H is a subgroup of G.

(i) Associativity:

Since, the operation of H is the same as that of G. Therefore, operation is associative in H.

(ii) Identity:

$\because$ H is nonempty, Let $x \in H$

let $a = x, b = x \in H \Rightarrow ab^{-1} = xx^{-1} \in H$

$\Rightarrow e \in H$

$\therefore$ Identity element exists in H.

(iii) Inverse:

let $a = e, b = x \in H \Rightarrow ab^{-1} = ex^{-1} \in H$

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

$\therefore$ Inverse of every element exists in H.

(IV) Closure Property:

Let $a, b \in H \Rightarrow a, b^{-1} \in H$ ($\because$ Inverse of b exists)

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

$\Rightarrow ab \in H$

$\therefore ab \in H \quad \forall a, b \in H$

$\Rightarrow H$ is closed

Thus, H is itself a group under the operation of G

$\Rightarrow H$ is a subgroup of G.

Example: Let G be an Abelian group with identity e.

Then $H = \{x \in G \mid x^2 = e\}$ is a subgroup of G.

Proof: $\because e^2 = e$ and $e \in G \Rightarrow e \in H$

$\Rightarrow H$ is nonempty.

Now let $a, b \in H \Rightarrow a^2 = e,\ b^2 = e$.

Now, $(ab^{-1})^2 = (ab^{-1})(ab^{-1}) = a(b^{-1}a)b^{-1}$ (Associativity)

$= a(ab^{-1})b^{-1}$ ($\because G$ is abelian)

$= a^2(b^{-1})^2$

$= a^2(b^2)^{-1}$ $[\because (g^n)^{-1} = (g^{-1})^n]$

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

$= e$

$\therefore ab^{-1} \in H \Rightarrow H \leq G$.

(II) Two - step subgroup Test:

Let G be a group and H be a nonempty Subset of G. Then H is a subgroup of G if and only if (i) $ab \in H$ $\forall a, b \in H$ (H is closed)

(ii) $a^{-1} \in H$ $\forall a \in H$ (Inverse of each element exists)

Proof: Similar to one-step subgroup Test.

(III) Finite subgroup Test:

Let H be a nonempty finite subset of a group G. Then H is a subgroup of G if and only if H is closed under the operation of G.

Proof: First, let H be a subgroup of G then clearly H is closed under the operation of G.

Conversely ($\Leftarrow$) let H be closed under the operation of G.

TS $H \leq G$.

$\because$ H is closed under the operation of G

$\therefore ab \in H \quad \forall a, b \in H$ ——— (1)

According to two-step subgroup test, we need to prove only that $a^{-1} \in H \quad \forall a \in H$.

If $a = e$, then $a^{-1} = e^{-1} = e \in H$ and we are done.

If $a \neq e$, consider the sequence

$a, a^2, a^3, \ldots$

Since H is finite and closure implies that all these powers of a are in H.

Therefore, all of these powers of a are not distinct.

$\therefore a^i = a^j$ for some $i > j$

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

$\Rightarrow i - j > 1 \qquad (\because a \neq e)$

Thus, $a^{i-j} = a \cdot a^{i-j-1} = e$

$\Rightarrow a^{i-j-1} = a^{-1} \in H \qquad \left[\begin{array}{l} \because i-j-1 > 0 \\ \Rightarrow i-j-1 \geq 1 \end{array}\right]$

$\therefore a^{-1} \in H$ for $a \in H$

$\Rightarrow$ Inverse of each element of H exists in H

Thus, H is a subgroup of G according to two-step subgroup test.

Example:

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

$H = \{0, 4\}$ is a subgroup of G

$\because H$ is finite and closed.

$K = \{0, 2, 4, 6\}$ is a subgroup of G

$\because K$ is finite and closed.

Cyclic subgroup:

Thm: Let G be a group and let a be any element of G. Then $\langle a \rangle$ is a subgroup of G.

where, $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

This subgroup $\langle a \rangle$ is called the cyclic subgroup of G generated by a.

Proof: $\because a \in \langle a \rangle \Rightarrow \langle a \rangle$ is non-empty.

Now, let $x, y \in \langle a \rangle$

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

Now, $xy^{-1} = (a^n)(a^m)^{-1} = a^n a^{-m} = a^{n-m} \in \langle a \rangle$ $(\because n-m \in \mathbb{Z})$

Thus, $x, y \in \langle a \rangle \Rightarrow xy^{-1} \in \langle a \rangle$

Therefore, $\langle a \rangle$ is a subgroup of G. (One-step subgroup test)

Example:

① Consider $U(12) = \{1, 5, 7, 11\}$

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

$\because 5^1 = 5, \quad 5^2 = 25 \pmod{12} = 1, \quad 5^3 = 5, \quad 5^4 = 1, \ldots$

② Consider $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$\langle 1 \rangle = \{1, 2, 3, 4, 5, 0\} = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}_6.$

$\langle 2 \rangle = \{2, 4, 0\} = \{0, 2, 4\}.$

$\because 2^1 = 2, \quad 2^2 = 2 +_6 2 = 4, \quad 2^3 = 2 +_6 2 +_6 2 = 6 \pmod 6 = 0.$

Center of a group:

The center of a group G is the subset of elements in G that commute with every element of G. In symbols,

$$Z(G) = \{a \in G \mid ax = xa \quad \forall\, x \in G\}$$

Theorem:

The center of a group G is a subgroup of G.

Proof:

Clearly, $ae = ea = a \quad \forall a \in G$

$\Rightarrow e \in Z(G)$

$\Rightarrow Z(G)$ is nonempty.

Now, let $a, b \in Z(G)$ and $x \in G$ be any arbitrary element of G.

Then $(ab)x = a(bx)$

$= a(xb)$ $\quad (\because b \in Z(G))$

$= (ax)b$ $\quad$ (Associativity)

$= (xa)b$ $\quad (\because a \in Z(G))$

$= x(ab)$

$\therefore ab \in Z(G)$ for $a, b \in Z(G)$.

Now we shall show that $a^{-1} \in Z(G)$ for $a \in Z(G)$

Let $a \in Z(G) \Rightarrow \quad ax = xa \quad \forall x \in G$.

$\Rightarrow a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1}$ $\quad (\because a \in Z(G) \Rightarrow a \in G \Rightarrow a^{-1} \in G$

$\Rightarrow (a^{-1}a)xa^{-1} = (a^{-1}x)(aa^{-1})$ $\quad$ (Associativity)

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

$\Rightarrow xa^{-1} = a^{-1}x \quad \forall x \in G$.

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

Thus, according to two step subgroup test, $Z(G)$ is a subgroup of G.

Example:

(1) $G=\{1,-1,i,-i\}$

$Z(G)=\{1,-1,i,-i\}$.

Note: For any abelian group G,

$Z(G)=G$.

(2) Quaternion Group (Q_8)

$$Q_8=\left\{\pm 1, \pm i, \pm j, \pm k \;\middle|\; \begin{array}{l} i^2=j^2=k^2=-1, \\ ij=k,\ jk=i,\ ki=j, \\ ji=-k,\ kj=-i,\ ik=-j \end{array}\right\}$$

$Z(Q_8)=\{1,-1\}$.

Centralizer of an element:

Let a be a fixed element of a group G. The centralizer of a in G is the set of all elements in G that commute with a.

In symbols, $C(a)=\{g\in G \mid ga=ag\}$.

Theorem:

For each a in a group G, the Centralizer of a is a subgroup of G.

Proof:

$$C(a) = \{g \in G \mid ga = ag\}.$$

Let $x, y \in C(a) \Rightarrow xa = ax$ and $ya = ay$

Now $(xy)a = x(ya)$
$= x(ay)$
$= (xa)y$
$= (ax)y = a(xy)$

$\therefore xy \in C(a)$ for $x, y \in C(a)$

Now, we shall show $x^{-1} \in C(a)$ for $x \in C(a)$

$\because x \in C(a) \Rightarrow xa = ax$

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

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

$= e(ax^{-1}) = (x^{-1}a)e$

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

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

$\Rightarrow x^{-1} \in C(a)$

Thus, using two step subgroup test, $C(a)$ is a subgroup of G.

Example:

(1) let $G = \{1, -1, i, i\}$

$C(i) = \{1, -1, i, -i\} = G$

Note: for any abelian group G,

$C(a) = G \quad \forall a \in G$.

(2) $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

$C(i) = \{1, -1, i, -i\}$

$C(j) = \{1, -1, j, -j\}$

$C(-1) = \{\pm 1, \pm i, \pm j, \pm k\} = Q_8$.

Cyclic group:

let G be a group ~~and a ∈~~ If $G = \langle a \rangle$ for some $a \in G$, we say that G is cyclic and a is a generator of G.

Example: $U(10) = \{1, 3, 7, 9\}$ is a cyclic group.

$\langle 3 \rangle = \{3, 9, 7, 1\} = \{1, 3, 7, 9\} = U(10)$

$\therefore 3$ is the generator of $U(10)$

$3^1 = 3,\ 3^2 = 9,\ 3^3 = 27 \pmod{10} = 7,\quad 3^4 = (7)(3) = 21 \pmod{10} = 1$.