Subgroup

$H \subseteq G$ is subgroup if H itself form a group under the operation of G.

$G = \mathbb{Z}_{10} = \{0, 1, 2, 3, \dots 9\}$

$H_1 = \{0\}$

$H_2 = \mathbb{Z}_{10}$

$\cancel{H_2} = \{0, 1, 2, 3, \dots 9\} = \mathbb{Z}_{10}$

$H_3 = \{0, 2, 4, 6, 8\}$

$H_2 = \cancel{H_4} = \{0, 3, 6, 9, 5, 4, 1, 2, 7, 8\} = \mathbb{Z}_{10}$

$H_4 = \{0, 5\}$

$H_3 = \cancel{H_5} = \{0, 4, 8, 2, 6\} = H_3$

Subgroup Tests

Thm ① One step Subgroup Test:

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

Proof:

First, let H be a subgroup of G and $a, b \in H$

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

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

$\Rightarrow ab^{-1} \in H$ (H is closed)

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

TS H is a subgroup

① Associativity

$\because H \subseteq G$

$\therefore$ elements of H are elements of G

$\because$ G is a group

$\therefore$ elements of G are associative

$\Rightarrow$ elements of H are associative

Example. $(\mathbb{Z}, +)$,

H = set of even integers $= 2\mathbb{Z}$.

$2, 4, 6 \in H \Rightarrow 2, 4, 6 \in \mathbb{Z}$

$(2+4)+6 = 2+(4+6)$ ⊄ Possible in $\mathbb{Z}$ but not in $2\mathbb{Z}$.

② Identity

$\because$ H is non empty

let $a \in H$

Now $a \in H, a \in H \Rightarrow a a^{-1} \in H$ $\left(\because ab^{-1} \in H\ \forall a, b \in H\right)$

$\Rightarrow e \in H$

$\therefore$ Identity exists

③ Inverse

Now $e \in H$, $a \in H \Rightarrow e a^{-1} \in H$ $\left[\because ab^{-1} \in H \ \forall a, b \in H\right]$

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

$\Rightarrow$ Inverse of a exists

$\because$ a is an arbitrary element of H

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

④ Closedness (Closure Property)

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

Now $a, b \in H \Rightarrow a \in H, b \in H$

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

$\Rightarrow a(b^{-1})^{-1} \in H$ $\left[\because ab^{-1} \in H \ \forall a, b \in H\right]$

$\Rightarrow ab \in H$

$\left[\because (b^{-1})^{-1} = b\right]$

a^{mn}
$= (a^m)^n$

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

$\Rightarrow$ H is a subgroup of G.

② Two Step Subgroup Test

let G be a group and H be a nonempty subset of G. Then H is a subgroup of G iff

(i) $ab^{-1} \in H \quad \forall a, b \in H$ (closedness)

(ii) $a^{-1} \in H \quad \forall a \in H$ (Inverse)

Proof: same as one-step subgroup test.
① Associative ② Identity ③ Inverse (given)
④ Closedness (given)

Identity
(let $b = a^{-1}$)

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

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

③ Finite Subgroup Test

let G be a group and H be a nonempty finite subgroup of G. Then H is a subgroup of G iff H is closed under the operation of G.

Proof: let H be a subgroup of G
then H is closed under the operation of G

Then H is closed under the operation of G

$\Rightarrow ab \in H \;\; \forall a, b \in H$

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

i.e. $ab \in H \;\; \forall a, b \in H$

TS H is a subgroup

① Closedness (given)

② Associativity (same 4-5 lines)

③ Identity:

$\because$ H is nonempty set

$\therefore a \in H$. If $a = e$, then we are done

$a^0 = e \;\; \forall a \in G$

If $a \neq e$, then $a \in H$,

$a^2 \in H$

$a^3 \in H$

$\vdots$

$a^i \in H$

$a^{i+1} \in H$

$\vdots$

$a^j \in H$

$a^{j+1} \in H$

$\vdots$

$\therefore$ The elements $a, a^2, a^3, \ldots, a^i, a^{i+1}, \ldots, a^j, a^{j+1}, \ldots$

are elements of H

$\because$ H is a finite set

$\because$ H is a finite set

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

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

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

$\because a \in H \Rightarrow a^{j-i} \in H$ [$\because (j-i) > 0$ & using closedness]

$\Rightarrow e \in H.$

$\therefore$ Identity exists in H

$\mathbb{Z}_4 = \{0,1,2,3\}$
$H = \{0,2\}$
$2^0 = 0, 2^1 = 2,$
$2^2 = 0, 2^3 = 2, 2^4 = 0$
$2^5 = 2$

Inverse:

Let $a \in H$

if $a = e$, then $a^{-1} = e^{-1} = e \in H$

If $a \neq e$,

then the elements $a, a^2, a^3, \cdots a^i, a^{i+1}, \cdots$
$\cdots a^j, a^{j+1}, \cdots$

are elements of H

$\because$ H is finite set

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

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

$\Rightarrow a^{j-i} = e$ —— (1)

$\therefore (j-i) > 1$ [$\because (j-i) \neq 0$, $(j-i) \neq 1$]

$\Rightarrow (j-i)-1 > 0$

$\Rightarrow j-i-1 > 0$

$\Rightarrow a^{j-i-1} \in H$

Now $a \cdot a^{j-i-1} = a^{j-i} = e$ (from eqn (1))

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

$\therefore$ Inverse of $a = a^{j-i-1}$ exists in H

$\therefore$ a is an arbitrary elements of H

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

Q. Let G be an abelian group under multiplication with identity e. ~~Then~~ ~~these~~ show that the set $H = \{x^2 \mid x \in G\}$ is a subgroup of G.

Soln

$e \in G$.

and $e^2 = e \Rightarrow e \in H$

$\therefore$ H is nonempty.

Two step subgroup test

(1) Closedness

let $a \in H$, $b \in H$

Then $a = x^2$, $b = y^2$ where $x, y \in G$

$ab = x^2 y^2 = xxyy$

$= x(xy)y$ [$\because G$ is associative]

$= x(yx)y$ [G is abelian, $xy = yx$]

$= (xy)(xy)$

$= (xy)^2 \in H$ [$\because x \in G, y \in G \Rightarrow xy \in G$]

$\Rightarrow ab \in H$

$\therefore H$ is closed.

② **Inverse**

Let $a \in H$ and $a = x^2$, where $x \in G$.

$a^{-1} = (x^2)^{-1} = x^{-2} = (x^{-1})^2 \in H$

$\Rightarrow a^{-1} \in H$ [$\because x \in G \Rightarrow x^{-1} \in G$]

$\Rightarrow$ Inverse of a exists in H.

$\because a$ is an ~~arbit~~ arbitrary element of H

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

From two-step subgroup test

H is a subgroup of G.