② Theorem- Prove that the order of a every cyclic group is equal to the order of its ~~generator~~ generator.

Ans:- Let $G = \{a\}$ be a cyclic group generated by a which is of finite order n. Then n is the least (+) ve integer such that $a^n = e$

To prove G is of order n

Since G is cyclic hence each element of G is some integral power of 'a' and by closure property, Each integral power of a belongs to G. we claim that G contains n distinct elements as $a, a^2, a^3, \ldots, a^n = e$ → ①

First we shall prove that all the elements of ① are distinct. Let i and j be the two distinct integers.

Such that

$$1 \leq i < j \leq n$$

Where, $a^i = a^j$

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

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

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

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

Which is impossible since $j-i<n$ and n is the least positive integer such that $a^n = e$. Hence all the elements of ① are distinct. It remains to prove that any integral power of a greater than n of a is one of the element of ①

Let $m > n$

We can write $m = nq + r$

where q is the integer and $0 \leq r < n$

Now,

$a^m = a^{nq+r} = a^{nq} a^r$
$= (a^n)^q a^r = e^q a^r = ea^r = a^r$ $(\because e^q = e)$
$= a^r$ ~~belongs to (r)~~

As $0 \le r < n$ so a^r and so a^m is one of the elements of ①
Hence G contains only n distinct elements which are in ①
Thus order of G is n
Hence the order of a cyclic group is equal to the order of its generator.

Note see page → (34) Remember Theorem → (45) page

Complex of group → Any subset of group is called complex of a group.

Sub-group of a group - If H be a subset of a group G. Then H is called sub group of G, if H is also a group under the same operation of G.

Theorem - If "H" be the subset of a group G then prove that H is subgroup of G iff $a, b \in H$
$\Rightarrow ab^{-1} \in H$

OR, Prove that necessary and sufficient condition that a subset H of a group G is subgroup if $a, b \in H$
$\Rightarrow ab^{-1} \in H$

Ans The ~~ness~~ necessary part :-
Let H be the sub-group of G
to prove that $a, b \in H \Rightarrow ab^{-1} \in H$

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

If $b \in H \Rightarrow b^{-1} \in H$ ($\because H$ is subgroup, so invertiable)
again,

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

$\Rightarrow ab^{-1} \in H$ [by closure property on H]

Which is the necessary condition for sub-group.

<u>The sufficient part</u>:—

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

To prove H is a sub-group.

we verify the following group ~~axioms~~ properties:

i) Replacing b by a in ①

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

$\Rightarrow e \in H$ {where e is identity element of G}

$\Rightarrow$ identity element exists in H.

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

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

~~$\Rightarrow eb^{-1} \in H \Rightarrow eb^{-1} \in H \Rightarrow b^{-1} \in H$~~

$\therefore$ Inverse of any element of H exists.

iii) ~~$a, b \in H \Rightarrow ab^{-1} \in H$~~

~~$\Rightarrow e, b \in H \Rightarrow eb^{-1} \in H \Rightarrow b^{-1} \in H$~~

~~Inverse of any element of H exists.~~ X

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

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

$a.b \in H$

(iii) $a, b \in H \Rightarrow a.b^{-1} \in H$
$\Rightarrow a(b^{-1})^{-1} \in H$
$\Rightarrow ab \in H$
i.e closure property hold in H.

(iv) Since, H is subset of G and G is a group and so all the elements of H must obey associative law.
from (i) to (iv), it follows that H is a group
So, H is sub-group of G.

V.I. (2) Theorem: A non empty subset H of a group G is a sub-group of G iff (i) $a, b \in H \Rightarrow ab \in H$
(ii) $a \in H \Rightarrow a^{-1} \in H$
Where a^{-1} is the inverse of a in G.

$\Rightarrow$ Let H be a non-empty subset of a group G such that (i) and (ii) hold. To prove that H is a sub group of G. for this we must show that H is a group.
(i) Closure property $\forall a, b \in H \Rightarrow ab \in H$ {by virtue of (i)}
(ii) Associatively $(ab)c = a(bc)$ $\forall a, b, c \in H$
$\forall a, b, c \in H \Rightarrow a, b, c \in G$ { $\because H \subseteq G$ }
$\Rightarrow (ab)c = a(bc)$ $\because$ {by Associative in G}

(iii) Existence of identity: If e be the identity in G then identity for H.
$a \in H \Rightarrow a^{-1} \in H$ by (ii)
$a \in H$, $a^{-1} \in H$ $\Rightarrow aa^{-1} \in H \Rightarrow e \in H$
~~$\Rightarrow e = aa^{-1} \in H$ by (i)~~

$\Rightarrow e \in H$ Thus identity element $e \in H$

(iv) Existence of Inverse → Each element of H is invertiable by virtue of (ii).

The above facts prove that H is a group.

Conversly —

Let H be a sub-group of G.

To prove that (i) and (ii) Hold.

Our assumption ⇒ H is a group.

⇒ (i) and (ii) hold.

Remark-

(1) A non empty subset H of a group $(G, *)$ is a group of G iff.

$a b \in H \Rightarrow a * b \in H$

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

(3) A necessary and sufficient condition for a non-empty subset H of a ~~finite~~ group G to be a group is that $a \in H, b \in H \Rightarrow ab \in H$

OR

The above theorem can also be expressed as prove that a non empty subset H of a finite group G is a sub-group iff ~~ab∈H~~ $ab \in H$ ~~⇒ a,b∈H~~ $\forall a, b \in H$

Ans → Let H be a non empty subset of a finite group G and H is also a subgroup of G.

To prove that $a, b \in H \Rightarrow ab \in H$

H is a sub-group of G ⇒ H is a group.

⇒ H is closed ~~with respect to operation~~

from this the required result follows.

Conversely – Suppose that H is a non-empty subset of a finite group G such that $a, b \in H \Rightarrow ab \in H$

We have to prove that H is a subgroup of G, i.e. to prove

(i) Closure property → $\forall a, b \in H \Rightarrow ab \in H$ [given]

(ii) Existence of identity element –

Let e be the identity of G and $a \in H$. Since H is finite

$\therefore$ Order of a is finite, say n.

[G is a finite group ⇒ every element of G is of finite order]

$\Rightarrow o(a) = n \Rightarrow a^n = e$

$\Rightarrow a, a \in H \Rightarrow aa \in H$ [by given condition]

$\Rightarrow a^2 \in H$

$\because a, a^2 \in H \Rightarrow aa^2 \in H \Rightarrow a^3 \in H$

Repeating this process, we see that $a^n \in H \Rightarrow e \in H$

Thus identity element $e \in H$

(iii) Associativity → ~~$(ab)c = a(bc)$ $\forall a, b, c \in H$~~

~~$\forall a, b, c \in H \rightarrow a, b, c \in G$~~

~~$\Rightarrow (ab)c = a(bc)$ [By Associative law in G]~~

$\because H \subseteq G$, and so all elements of H must obey associative law.

(iv) Existence of inverse – Let $a \in H$. ~~such that~~

$\because o(a) = n$, $\Rightarrow a^n = e$

By the given condition.

$a, a \in H \Rightarrow a^2 = aa \in H \Rightarrow a^2 \in H$

$\Rightarrow a^3 = a^2 a \in H \Rightarrow a^3 \in H$

Repeating this process, we observe that $a^{n-1} \in H$

But $a^{n-1} = a^n a^{-1} = e a^{-1} = a^{-1}$

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

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

Hence every elements of H is investiable.

from what has been done it follows that H is a group.

Theorem ④ A necessary and sufficient condition for a non empty finite subset of a group G to be a subgroup is that H must be closed.

Ans:- Let H be a nonempty finite subset of a group G. Such that H is a sub-group of G.

To prove that H is closed

$\because$ H is a sub-group of G $\Rightarrow$ H is a group

$\Rightarrow$ H is closed w.r. to operation of G.

Conversly - Suppose that H is a nonempty finite sub-set of a group G and

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

To prove that H is a sub-group of G.

For this we must show that H is a group.

(i) Closure property - $\forall a, b \in H$

$\Rightarrow ab \in H$ (given)

(ii) Associativity - ~~a(bc) = (ab)c $\forall a,b,c \in H$~~

$\because H \subseteq G$, and so all elements of H must obey associative ~~(by Associativity)~~

(iii) Existence of identity element ÷ Let e be the identity in H. By the given condition

$a \in H$, $a \in H \Rightarrow a^2 = aa \in H$

$\Rightarrow a^3 = a^2 a \in H$

$\Rightarrow a^4 = a^3 a \in H$

Proceeding in this way we see that all the elements $a, a^2, a^3, a^4, \ldots$ belong to H if $a \in H$. But H is a finite set consequently, ~~all~~ these elements are not distinct. ~~that is there must be repeatition in this collection of elements~~

Let $a^r = a^s$ where $r, s \in N$

such that $r > s$

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

$\Rightarrow a^{r-s} = e$ (also $r-s$ is a (+ve) integer)

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

(iv) Existence of inverse:-

Again $r-s \geq 1$

$\Rightarrow r-s-1 \geq 0$

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

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

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

This shows that every element of H is inversiable. The above facts prove that H is sub-group of G.

Remark:- Observe the difference between the theorem ③ and ④

Remember: Let G be a cyclic group and $o(G) = n$ (finite). Let 'a' be the generator, so $o(a) = o(G) = n$.

How many generators:-

$a^m \in G$ is also a generator if g.c.d of m and $n = (m,n) = 1$

2014

① Q: How many (Find) generators are of a cyclic group of order 10.

Ans: Let $G = \{a\}$ be a cyclic group of order 10.

$\therefore o(a) = o(G) = 10$

$\therefore G = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10} = e\}$

$\because (1,10) = 1,\ (3,10) = 1,\ (7,10) = 1,\ (9,10) = 1$

$\therefore$ there are four generators of G namely a, a^3, a^7, a^9.

~~(2) Q: Find the generators of a cyclic group of order 8.~~

Ans. Do same as above. (Ans. a, a^3, a^5, a^7)

Theorem (5) If H_1 and H_2 be any two sub-groups of G, then prove that $H_1 \cap H_2$ is also a sub-group. OR

Prove that intersection of two sub-groups of a group is again a subgroup

Ans: H_1 and H_2 are two subgroups of G

$$\therefore x_1, x_2 \in H_1 \Rightarrow x_1 x_2^{-1} \in H_1$$

$$\text{and } x_1, x_2 \in H_2 \Rightarrow x_1 x_2^{-1} \in H_2$$

To prove $H_1 \cap H_2$ is a sub group of G

$$\because H_1 \cap H_2 \subseteq H_1 \subseteq G$$

$$\Rightarrow H_1 \cap H_2 \subseteq G$$

Let x_1, x_2 be any two elements of $H_1 \cap H_2$

$$\because x_1, x_2 \in H_1 \cap H_2$$

$$\Rightarrow x_1, x_2 \in H_1 \text{ and } x_1, x_2 \in H_2$$

$$\Rightarrow x_1 x_2^{-1} \in H_1 \text{ and } x_1 x_2^{-1} \in H_2$$

$\{\because H_1$ and H_2 are sub-groups$\}$

$$\Rightarrow x_1 x_2^{-1} \in H_1 \cap H_2$$

$\Rightarrow H_1 \cap H_2$ is a sub-group of G

Hence intersection of two group is also sub-group.

P.T. intersection of sub-groups is also a sub-group.

Ans:- Let $H_1, H_2, H_3, H_4, \ldots$ be sub groups of a group G

To prove that $H_1 \cap H_2 \cap H_3 \cap H_4 \ldots$ is also a sub-group of G.

$\because H_1, H_2, H_3 \ldots$ are sub-group

$\therefore x_1, x_2 \in H_i \Rightarrow x_1 x_2^{-1} \in H_i \quad \forall\, i = 1, 2, 3, \ldots$

Now,

$$H_1 \cap H_2 \cap H_3 \cap \ldots \subseteq H_i \subseteq G$$

$\Rightarrow H_1 \cap H_2 \cap H_3 \cap \ldots \subseteq G$

Let x_1, x_2 be any two elements of $H_1 \cap H_2 \cap H_3 \ldots$

$\because x_1, x_2 \in H_1 \cap H_2 \cap H_3 \cap \ldots$

$\Rightarrow x_1, x_2 \in H_i \quad \forall\, i = 1, 2, 3, \ldots$

$\Rightarrow x_1 x_2^{-1} \in H_i \quad \forall\, i = 1, 2, 3, \ldots$ [H_i is sub-group]

$\therefore x_1 x_2^{-1} \in H_1 \cap H_2 \cap H_3 \cap \ldots$

$\Rightarrow H_1 \cap H_2 \cap H_3 \ldots$ is a sub-group G

Hence intersection of sub-groups of a group is also a subgroup.

Note:-

① Find the necessary and sufficient condition for sub-group of a group.

Ans: The necessary and sufficient condition for subgroup H of a group G is

$a, b \in H \Rightarrow ab^{-1} \in H$ → [Do theorem ①]

② State and prove that necessary and sufficient condition for sub-group of a finite group.

Ans Statement - The necessary and sufficient condition that a subset H of a group G is a sub group is

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

[Do theorem ③]

③ Find the necessary and sufficient condition for it a finite subset H of a group is sub group.

Ans→ The necessary and sufficient condition for sub-group of a finite subset H of a group G is $a, b \in H \Rightarrow ab \in H$

[Do theorem (4)]