Defi: order of an element in a group:

Let $a \in G$ and if $\exists$ a positive integer n such that

$a^n = e$ (where e is the identity in G).

then a is said to be of finite order.

If $\exists$ no such positive integer, then a is said to be of infinite order.

It may happen that there are many such integers exist for which $a^m = e$

then, let the least positive integer among such type of integers m be n, then

$a^n = e$ is obvious and the n is called order of an element a of G and we denote it by $o(a)$ i.e. $\boxed{o(a) = n}$

Ex Let us consider a multiplicative group

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

Here identity element $e = 1$.

and $(1)^1 = 1$ $\qquad (i)^4 = 1$

$(-1)^2 = 1$ $\qquad (-i)^4 = 1$

$\Rightarrow o(1) = 1, \quad o(-1) = 2, \quad o(i) = 4, \quad o(-i) = 4$

Ex In klein's 4 group. i.e.

$G = \{e, a, b, c\}$.

where Table is

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Here $o(e) = 1$ and $o(a) = 2 = o(b) = o(c)$

$\Rightarrow$ order of every element except identity is 2.

Property:- The order of the identity of every group is 1 and it is the only element of order 1.

1. Theorem Prove that the order of every element of a finite group is finite and less than or equal to the order of the group.

Proof:- Let G be a group of finite order n

$\Rightarrow$ Number of distinct elements in G are n.

Again let $a \in G$, then consider the elements

$a^0 = e$, and $a^1, a^2, a^3, \dots\dots a^n$ ——— ①

All these elements belong to G, because any element, operated with himself will ~~again~~ give a new element, which must be again member of G, due to closure property.

Here in ① they are $n+1$ in number

$\Rightarrow$ They are more than the order of group i.e. n. So they all can't be distinct

$\Rightarrow$ At least two elements must be same

Let us suppose

$$a^i = a^j \quad \text{where } 0 \le i \le j \le n$$

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

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

$$\Rightarrow a^{j-i} = e \qquad \text{let } j-i = l$$

$$\Rightarrow a^l = e \qquad \text{this } l \le n.$$

$$\Rightarrow o(a) \le l$$

$$\Rightarrow o(a) \le n \qquad \because l \le n$$

$\Rightarrow$ order of an element $\le$ order of G.

Proved

2. Th Prove that if order of an element a of a group G is n, then $a^m = e$ iff m is a multiple of n.

Proof:- case (i) Let us consider first that $a^m = e$ — (i)

~~So~~ Since m and n are integers, so m can be written as

$$m = nq + l \qquad ; 0 \le l < n$$

$$\Rightarrow a^m = a^{nq+l} = e \qquad \text{from (i)} \qquad \text{Ex } 15 = 2(7)+1$$

$$\Rightarrow a^{nq+l} = e$$

$$\Rightarrow a^{nq} \cdot a^l = e \Rightarrow (a^n)^q \cdot a^l = e$$

$$\boxed{\because (a^m)^n = a^{mn}}$$

$(e)^q \cdot a^r = e$

$\Rightarrow e \cdot a^r = e$

$\Rightarrow a^r = e$ Here $0 \le r < n$

$\because$ Order of $a = n$

So no number exist, which is less than n and for which $a^r = e$

It is only possible when $r = 0$

$\Rightarrow m = nq$

$\Rightarrow m$ is a multiple of n. H.P.

Case(ii) Here let us consider that m is a multiple of n

$\Rightarrow \exists\, q \in \mathbb{Z}$ s.t. $m = nq$

$\Rightarrow a^m = a^{nq}$

$\Rightarrow a^m = (a^n)^q = (e)^q = e$.

$\Rightarrow \boxed{a^m = e}$ where m is a multiple of n.

H.P.

Prop:- The order of any integral power of an element a of a group G cann't be more than the order of the element.

Means If $o(a) = n$, then $o(a^k)$ cann't be more than n. It will be less than or equal to n.

Th. If G is a group then prove that $o(a) = o(a^{-1})$ where $a \in G$.

Proof:- Let us take $o(a) = n$ and $o(a^{-1}) = m$ then we are to prove that $m = n$

Now a^{-1} is nothing but some integral power of a ~~So~~ by the property that order of any integral power of a cann't be more than $o(a)$. Means may be less than or equal to $o(a)$. So by this property

$$o(a^{-1}) \le o(a) \quad \text{——— (i)}$$

$$\Rightarrow \boxed{m \le n}$$

Again a can be considered as integral power of a^{-1} i.e. $a = (a^{-1})^{-1}$

~~$\Rightarrow$~~ $\cancel{o(a) \le o(a^{-1})}$

$$\Rightarrow o((a^{-1})^{-1}) \le o(a^{-1})$$

$$\Rightarrow o(a) \le o(a^{-1}) \qquad \because (a^{-1})^{-1} = a.$$

$$\Rightarrow \boxed{n \le m} \quad \text{——— (ii)}$$

from (i) & (ii) $\boxed{m = n}$

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

H.P.