Important theorems of groups.

Theorem (A) — The order of any integral power of an element of a group G is less than or equal to the order of a.

$$O(a^m) \leq O(a) \quad \forall\, a \in G \text{ and } m \in N.$$

Proof: — Let a be an element of a group G such that $O(a) = n$

So that n is a normal number, such that $a^n = e$ = identity of G ——— (1)

Let a^m be any power of a and let

$$O(a^m) = P \quad \text{——— (2)}$$

To prove that $O(a^m) \leq O(a)$, it is enough to show that

$$P \leq n. \quad \text{——— (3)}$$

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

$\Rightarrow a^{nm} = e^m = e \Rightarrow (a^m)^n = e \Rightarrow O(a^m) \leq n$

$\Rightarrow P \leq n$ (From eqn (2))

Proof Proved

Theorem (B) — The order of every element of a finite group is finite.

Proof: — Let a be an arbitrary element of a finite group G. To prove that $O(a)$ is finite.

By closure property, all the elements

$a^2 = a \cdot a$, $a^3 = a \cdot a \cdot a$ --- etc. belong to G.

That is to say a, a^2, a^3, a^4, a^5 — etc, belong to G.

But all these elements are not distinct since G is finite.

Let e be the identity in G, then $a^0 = e$.

Hence we can write

$$a^m = a^n \text{ where } m > n.$$

$$a^m = a^n \Rightarrow a^m a^{-n} = a^n a^{-n} = a^0 = e$$

$$\Rightarrow a^{m-n} = e \Rightarrow a^p = e$$

where $p = m - n$

$m > n$, $m - n = p \Rightarrow p > 0$

Also m and n are finite and hence p is a finite positive integer.

Now p is a positive integer

s.t $a^p = e$

This proves that $o(a) \leq p$ = finite number

i.e. $o(a) \leq$ a finite number

$\Rightarrow o(a)$ is finite.

Proved