Order of an element

Prepared by Dr. A.K. Maiti

Semester-II (UG)

Paper: C201

Course- Mathematics (H)

Prepared by Dr. A. K. Maiti

order of an element

Let G be a group and $a \in G$. We define $a^1 = a$, $a^2 = a.a$, $a^3 = a.(a.a) = a.a.a$. In the same way we define a^m, where m is a positive integer. The product is independent of the manner in which the factors are grouped.

If m be a negative integer say $m = -p$ where p is positive integer, then we define a^m by $(a^{-1})^p$

ie $(a^{-1})^p = a^{-1}.a^{-1} \ldots a^{-1}$ (p times).

Defn: Let $(G, \circ)$ be a group and let a be an element of G. a is said to be of finite order if there exists a positive integer n such that $a^n = e$. The order of a is the least positive integer n such that $a^n = e$ and is denoted by $o(a)$.

Note: In additive notation, the order of an element is denoted by na which n is the least positive integer.

Ex (i) $o(\omega) = 3$ $o(\omega^2) = 3$

(ii) In $(\mathbb{Z}_6, +)$, $o(\bar{1}) = 6$ $o(\bar{2}) = 3$, $o(\bar{3}) = 2$, $o(\bar{4}) = 3$, $o(\bar{5}) = 6$

(iii) In the group $(\mathbb{Z}, +)$, the order of each non-zero element is infinite.

Note: The order of the identity element in a group is 1 and no other element in a group is of order 1.

Theorem: Let a be an element of a group $(G, \circ)$. Then

(i) $o(a) = o(a^{-1})$

(ii) If $o(a) = n$ and $a^m = e$ then n is a divisor of m. V.H-11

(iii) If $o(a) = n$ then $a, a^2, \ldots, a^n (= e)$ are distinct elements of G.

(iv) If $o(a) = n$ then for a positive integer m, $o(a^m) = \frac{n}{\gcd(m,n)}$.

(v) If $o(a) = n$ then $o(a^p) = n$ iff p is prime to n.

(vi) If $o(a)$ is infinite and p is a positive integer then $o(a^p)$ is infinite.

Proof: (i) Case-I Let $o(a) = n$ Then $a^n = e$, n is the least positive integer.

Again, m be the order of a^{-1}. Then we have

$$o(a) = n$$
$$\Rightarrow a^n = e$$
$$\Rightarrow (a^n)^{-1} = e \Rightarrow (a^{-1})^n = e \Rightarrow o(a^{-1}) \le n$$
$$\Rightarrow m \le n. \quad (i)$$

Also, $o(a^{-1}) = m$
$$\Rightarrow (a^{-1})^m = e$$
$$\Rightarrow (a^m)^{-1} = e \Rightarrow a^m = e$$
$$\Rightarrow o(a) \le m$$
$$\Rightarrow n \le m \quad (ii)$$

$\therefore$ From (i) and (ii), $m = n$
$$\Rightarrow o(a^{-1}) = o(a) \quad \text{(Proved)}.$$

Otherwise: Let $o(a) = n$, $a^n = e$, n is the least positive integer.

$\therefore a^n = e \Rightarrow (a^{-1})^n = e$

If possible, let there be another positive integer $m < n$ s.t.

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

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

Since $n - m < n$, this contradicts $o(a) = n$

$\therefore o(a^{-1}) = n$.

Case-II: Let $o(a)$ be infinite, we assert that $o(a^{-1})$ is infinite. If not, let $o(a^{-1}) = m$, where m is a positive integer. Then $(a^{-1})^m = e \Rightarrow (a^m)^{-1} = e$
$$\Rightarrow a^m = e$$
$$\Rightarrow a \text{ is of finite order, a contradiction.}$$

Therefore, $o(a^{-1})$ is infinite.

Hence the proof.

Scanned with CamScanner

(ii) Since $o(a) = n$, n is the least positive integer such that $a^n = e$. By division algorithm, there exist integers q and r such that $m = qn + r$, $0 \le r < n$.

Then $e = a^m = a^{qn+r} = (a^n)^q \cdot a^r = e \cdot a^r = a^r$.

This relation holds only when $r = 0$, because, otherwise it will contradict that $o(a) = n$.

Therefore, $m = qn$ and the theorem is proved.

(iii) If possible let $a^r = a^s$ for some positive integers r, s such that $1 \le r < s \le n$. Then $a^s \cdot a^{-r} = e \Rightarrow a^{s-r} = e$

Since $0 < s - r < n$, this contradicts the assumption that $o(a) = n$. This establishes that, $a, a^2, a^3, \ldots, a^n (= e)$ are all distinct.

(iv) Let $o(a^m) = k$. Then $a^{mk} = e$

Again $o(a) = n \Rightarrow n / mk$.

Let $\gcd(m, n) = d$. Then $m = du$, $n = dv$ where $\gcd(u, v) = 1$

$\because n / mk \Rightarrow dv / duk \Rightarrow v / uk$

$\Rightarrow v / k$ Since $\gcd(u, v) = 1$. (i)

Again $(a^m)^v = (a^{du})^v = a^{duv} = (a^u)^n = e$

$o(a^m) = k$ and $(a^m)^v = e \Rightarrow k / v$ (ii)

From (i) and (ii) we have $k = v$

$\Rightarrow k = \frac{n}{d}$

Therefore, $o(a^m) = \frac{n}{\gcd(m, n)}$.

(v) ~~Given that $o(a) = n$.~~

Let p be prime to n. Then $\gcd(p,n) = 1$.

Since $o(a) = n$, $o(a^p) = \dfrac{n}{\gcd(p,n)}$ [by ~~thm~~ (iv)]

Therefore $o(a^p) = n$, $\gcd(p,n) = 1$.

Conversely, $o(a^p) = n$

We have $o(a^p) = \dfrac{n}{\gcd(p,n)}$ [by (iv)]

Therefore $\gcd(p,n) = 1$

$\Rightarrow$ p be prime to n.

(vi) If possible let $o(a^p)$ be finite say m.

$\therefore$ $o(a^p) = m \Rightarrow a^{pm} = e$,

$\Rightarrow$ a is of finite order, a contradiction.

Therefore $o(a^p)$ is infinite.

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

Proof: Let G be a finite group, the composition being denoted by multiplication. Let $a \in G$. Consider all positive integral powers of a i.e. $a, a^2, a^3, \ldots$, all these are elements of G, by closure axiom.

Since ~~G~~ G is finite, so G has finite number of elements, therefore all these integral powers of a cannot be distinct elements of G. Let us suppose that $a^r = a^s$ ($r > s$

$\Rightarrow a^r \cdot a^{-s} = a^s \cdot a^{-s}$ [$\because a^{-s} \in G$]

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

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

$\Rightarrow a^m = e$ where $m = r - s$

Since $r > s$, therefore m is a positive integer. Thus there exists a positive integer m such that $a^m = e$.

But we know that every set of positive integers has a least number. Therefore, the set of all those positive integers m such that $a^m = e$ has least ~~member~~ number n (say).

Thus, there exists a least positive integer n such that $a^n = e$. Therefore $o(a)$ is finite.

2nd Part: We have to prove that $o(a) \leq o(G)$.

Let $o(a) = n$ where $n > o(G)$. Since $a \in G$, therefore by closure property, $a, a^2, \ldots, a^n$ are elements of G. No two of these equal.

For if possible, let $a^r = a^s$, $1 \leq s < r \leq n$. Then

$a^{r-s} = e$.

Since $0 < r - s < n$. Therefore, $a^{r-s} = e$.

$\Rightarrow$ the order of a is less than n.

This is a contradiction. Hence, $a, a^2, \ldots, a^n$ are n distinct elements of G. Thus $n > o(G)$ is not possible.

Hence we must have $o(a) \leq o(G)$.

(Ex) For a group (G, o), a is an element of order 30. Find the order of a^{18}.

Ans. Since $o(a) = 30$. $\therefore a^{30} = e$.

Let $o(a^{18}) = m$. Then $a^{18m} = e$ where m is the least positive integer. Since $o(a) = 30$, 30 is a divisor of $18m$.

It follows that 5 is divisor of $3m$.

Since m is the least positive integer, $m = 5$.

Therefore $o(a^{18}) = 5$.

Another method: Since $o(a) = 30$, $\therefore o(a^{18}) = \dfrac{30}{\gcd(30, 18)} = \dfrac{30}{6} = 5$.

Ex : Find the elements ~~of order~~ 8 in the group $(\mathbb{Z}_{24}, +)$.

Ans. The elements of $\mathbb{Z}_{24}$ is $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{23}$. $o(\bar{0}) = 1$, $o(\bar{1}) = 24$

Let $o(\bar{m}) = 8$ where $0 < m < 24$.

$o(\bar{1}) = 24$, $o(\bar{m}) = o(m \cdot \bar{1}) = \dfrac{24}{\gcd(24, m)}$.

$\therefore o(\bar{m}) = 8 \Rightarrow \gcd(24, m) = 3$.

Therefore $\frac{m}{3}$, $\frac{24}{3}$ are prime to each other i.e. $m/3$ is less than 8 and prime to 8 i.e. $\frac{m}{3} = 1, 3, 5, 7$.

Hence the elements of order 8 are $\bar{3}, \bar{9}, \overline{15}, \overline{21}$.

Ex : In a group $(G, \circ)$, the elements a and b commute and $o(a)$ and $o(b)$ are prime to each other. Show that

$o(a \circ b) = o(a) \cdot o(b)$.

Ans : Let $o(a) = m$, $o(b) = n$ and let $o(a \circ b) = k$.

Then $a^m = e$, $b^n = e$ and $(ab)^k = e$.

Now, $(a \circ b)^{mn} = a^{mn} \circ b^{mn}$ $[\because a \circ b = b \circ a]$

$= e \circ e = e$

Therefore k is a divisor of mn — (1).

Again, $(a \circ b)^k = e$

$\Rightarrow a^k \circ b^k = e$ $[\because a \circ b = b \circ a]$

$\Rightarrow a^k = b^{-k}$

$\Rightarrow a^{nk} = e$ $[\because b^{-nk} = e]$

Scanned with CamScanner

$\Rightarrow$ m is a divisor of nk, since $\gcd(m,n)=1$.

$\Rightarrow$ m is a divisor of k,

Also, $(a \circ b)^k = e \Rightarrow b^k = a^{-k}$

$\Rightarrow b^{mk} = e$ $[\because a^{-mk} = e]$

$\Rightarrow$ n is a divisor of mk

$\Rightarrow$ n is a divisor of k since $\gcd(m,n)=1$.

Therefore mn is a divisor of k, since $\gcd(m,n)=1$. (ii)

From (i) and (ii), $k = mn$

$\Rightarrow O(a \circ b) = O(a) \circ O(b)$. (Proved)

<u>Conjugate element:</u> Let $(G, \circ)$ be a group and $a \in G$.

An element b in G is said to be conjugate of a if there exists an element $x \in G$ such that $b = x \circ a \circ x^{-1}$.

Ex: Prove that the orders of the elements a and $x^{-1}ax$ are the same where a, x are any two elements of a group.

<u>Ans</u>: Let n and m be the orders of a and $x^{-1}ax$ respectively.

$\therefore O(a) = n$ and $O(x^{-1}ax) = m$.

Now, $(x^{-1}ax)^2 = (x^{-1}ax)(x^{-1}ax)$

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

$= x^{-1}aeax = x^{-1}a^2x$

In general, $(x^{-1}ax)^n = x^{-1}a^nx$

$= x^{-1} \cdot e \cdot x$ $[\because O(a) = n \Rightarrow a^n = e]$

$= e$

$\therefore O(x^{-1}ax) \le n \Rightarrow m \le n$ (I).

Also, $o(x^{-1}ax) = m \Rightarrow (x^{-1}ax)^m = e$

$$\Rightarrow x^{-1}a^m x = e$$

$$\Rightarrow x^{-1}a^m x = x^{-1}x \quad [\because x^{-1}.x = e]$$

$$\Rightarrow a^m x = x \quad [\text{left Cancellation law}]$$

$$\Rightarrow a^m = e \quad [\text{right Cancellation law}]$$

$$\Rightarrow o(a) \leq m$$

$$\Rightarrow n \leq m \quad (2)$$

From (1) and (2), $n = m$

$$\Rightarrow o(a) = o(x^{-1}ax) \quad \text{(Proved)}$$

Deduction: Deduce that $o(a\circ b) = o(b\circ a)$ for $a, b \in G$.

Ans: $a\circ b$ can be expressed as $a\circ b = b^{-1}\circ(b\circ a)\circ b$.

This shows that $a\circ b$ and $b\circ a$ are conjugate of each other.

so, $o(a\circ b) = o(b\circ a)$.

Another way: $\boxed{\text{See Page-7}}$

Ex: Given that $axa = b$ in G. Find x.

Ans: We have $axa = b$

$$\Rightarrow a^{-1}(axa) = a^{-1}b \quad [\because a\in G \Rightarrow a^{-1}\in G]$$

$$\Rightarrow a^{-1}a(xa) = a^{-1}b \quad [G \text{ is associative}]$$

$$\Rightarrow exa = a^{-1}b \quad [a^{-1}.a = e]$$

$$\Rightarrow xa = a^{-1}b \quad [\because e.a = a]$$

$$\Rightarrow xaa^{-1} = a^{-1}ba^{-1}$$

$$\Rightarrow x = a^{-1}ba^{-1} \quad [aa^{-1} = e]$$

Ex: If G is a group of even order. Prove that it has an element $a \neq e$ satisfying $a^2 = e$ 'C.H-06 V.H-09.

Ans: Let G be a group of even order $2n$, n is the positive integer. We shall prove that G must have an element $a \neq e$ such that $a^{-1} = a$. We shall prove it by contradiction.

Suppose G has no element, other than identity element e, which is its own inverse. Now in a group, every element possesses a unique inverse. The identity element e is its own inverse. Further, if b is the inverse of c then c is the inverse of b. So, excluding the identity element e, the remaining $2n-1$ elements of G must be divided into pairs of two such that each pair consists of an element and its inverse. But we can not do so because the odd integer $2n-1$ is not divisible by 2. Hence our assumption is wrong. So in G, there exists an element $a \neq e$ satisfying $a^2 = e$.

Otherwise: Let $A = \{g \in G \mid g \neq g^{-1}\} \subseteq G$. Then $e \notin A$. If $g \in A$ then $g^{-1} \in A$. i.e elements of A occurs in pairs.

Therefore, the number of elements in A is even. This implies that the number of elements in $\{e\} \cup A$ is odd. Since the number of elements in G is even and $\{e\} \cup A \subseteq G$, there exists $a \in G$ such that $a \notin \{e\} \cup A$.

But then $a \neq e$ and $a \notin A$. Hence there exists $a \in G$ such that $a \neq e$ and $a = a^{-1}$ i.e $a^2 = e$.

Ex: If in the group G, $a^5 = e$, $aba^{-1} = b^2$ for $a, b \in G$. Find $o(b)$.

Ans : We have $aba^{-1} = b^2$ [given]

Now $(aba^{-1})^2 = aba^{-1}aba^{-1}$

$= ab^2a^{-1}$ $[a^{-1}a = e]$

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

$= a^2ba^{-2}$.

$\therefore (aba^{-1})^4 = \{(aba^{-1})^2\}^2 = (a^2ba^{-2})^2$

$= a^2ba^{-2}.a^2ba^{-2}$

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

$= a^3ba^{-3}$.

$\therefore (aba^{-1})^8 = a^4ba^{-4}$

$(aba^{-1})^{16} = \{(aba^{-1})^8\}^2 = \{a^4ba^{-4}\}^2$

$= a^4ba^{-4}.a^4ba^{-4}$

$= a^4b^2a^{-4} = a^4(aba^{-1})a^{-4}$

$= a^5.ba^{-5}$

$= ebe$ $[\because a^5 = e]$

$= b$.

$\therefore (aba^{-1})^{16} = b$

$\Rightarrow (b^2)^{16} = b$ $[\because aba^{-1} = b^2]$

$\Rightarrow b^{32} = b$.

$\Rightarrow b^{31} = e$.

Since $b^m = e \Rightarrow$ ~~31 is a divisor of m~~. $\therefore$

$\therefore$ ~~m is 31~~. $o(b)/m$

$\therefore$ ~~$o(b) = 31$~~. $\therefore o(b)/31$.

But 31 is prime integer, $\therefore o(b) = 1$ or 31.
So, if $b = e$ then $o(b) = 1$ and if $b \neq e$, $o(b) = 31$.

Ex : Let $(G,\circ)$ be a group and $a,b \in G$. If $o(a)=3$ and $a \circ b \circ a^{-1} = b^2$ find $o(b)$ if $b \neq e$ [Ans : $o(b)=7$]

Ans: Try yourself

Ex Let $(G,*)$ be a group and $a,b \in G$. Suppose that $a^2 = e$ and $a*b*a = b^7$. Prove that $b^{48} = e$. V. H - 2010.

Ans: Here $a*b*a = b^7$

Then $a*(a*b*a)*a = a*b^7*a$

$\Rightarrow a^2*b*a^2 = a*b^7*a$

$\Rightarrow b = a*b^7*a \quad [\because a^2=e]$

~~$\Rightarrow a*b*a = a^2*b^7*a^2$~~

$\Rightarrow b = (a*b*a)*(a*b*a)*(a*b*a)* \cdots * (a*b*a)$

$\Rightarrow b = (a*b*a)^7$

$\Rightarrow b = (b^7)^7 \quad [\because a*b*a = b^7]$

$\Rightarrow b = b^{49}$

$\Rightarrow b^{48} = e$ (Proved)

Ex Let $(G,*)$ be a group and $a,b \in G$. Suppose that $a*b = b*a^{-1}$ and $b*a = a*b^{-1}$. Show that $a^4 = b^4 = e$.

Ans: Since $a*b = b*a^{-1}$

$\Rightarrow a = b*a^{-1}*b^{-1}$

Similarly, $b*a = a*b^{-1} \Rightarrow b = a*b^{-1}*a^{-1}$.

Thus, $b*a = a*b^{-1} = (b*a^{-1}*b^{-1})*b^{-1} \quad [\because a = b*a^{-1}*b^{-1}]$

$= b*a^{-1}*b^{-2}$.

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

$\Rightarrow a = a^{-1}*b^{-2}$.

$\Rightarrow \ a^2 = b^{-2}$.

Hence $a^4 = a^2 * a^2 = a^2 * b^{-2}$

$= a * a * b^{-1} * b^{-1}$

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

$= a * (b * a) * b^{-1}$ $[\because b * a = a * b^{-1}]$

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

$= (b * a^{-1}) * a * b^{-1}$ $[\because a * b = b * a^{-1}]$

$= b * e * b^{-1}$

$= b * b^{-1} = e$.

$\therefore \ a^4 = e$.

Also, $b^4 = a^{-4} = e$.

$\therefore \ a^4 = b^4 = e$ (Proved)

(Ex) Prove that a non-commutative group of order $2n$, where n is an odd prime, must have a subgroup of order n.

Proof: Let G be a group of order $2n$ where n is odd prime. The divisors of $2n$ are $1, 2, n$ and $2n$. The possible orders of different elements of the group are 1 or 2 or n or $2n$.

No element can have order $2n$, because if there be an element of order $2n$, then G must be cyclic and therefore commutative.

The group contains only one element (the identity) of order 1.

If the order of each non-identity element be 2 then $ab = ba \ \forall a, b \in G$. So, G is commutative, a contradiction.

Therefore, there must be an element b of order n. The cyclic subgroup $\langle b \rangle$ is a subgroup of G of order n.

Ex. Prove that any conjugate of a has the same order as that of a. Deduce that $O(a \circ b) = O(b \circ a)$ for $a, b \in G$.

Ans: Case-I: Let $o(a) = m$ then $a^m = e$, Let $x \in G$.

$$\therefore (x \circ a \circ x^{-1})^m = (x \circ a \circ x^{-1}) \circ (x \circ a \circ x^{-1}) \circ \cdots \circ (x \circ a \circ x^{-1}) \quad [m \text{ times}]$$

$$= x \circ a^m \circ x^{-1}$$

$$= x \circ e \circ x^{-1} \quad [a^m = e]$$

$$= x \circ x^{-1} \quad [x^{-1} \circ x = e = x^{-1} \circ x]$$

$$= e$$

$$\therefore (x \circ a \circ x^{-1})^m = e.$$

If possible let $(x \circ a \circ x^{-1})^k = e$ where k is a positive integer less than m.

Then $(x \circ a \circ x^{-1})^k = e$

$$\Rightarrow x \circ a^k \circ x^{-1} = e$$

$$\Rightarrow a^k = x^{-1} \circ x = e$$

$$\Rightarrow a^k = e, \text{ a contradiction, since } o(a) = m.$$

So, m is the least positive integer such that $(x \circ a \circ x^{-1})^m = e$

$$\therefore (x \circ a \circ x^{-1})^m = e \Rightarrow O(x \circ a \circ x^{-1}) = m.$$

Case-II: Let $O(a) =$ infinite.

Let $o(x \circ a \circ x^{-1})$ be finite say k.

Then $(x \circ a \circ x^{-1})^k = e$

$$\Rightarrow x \circ a^k \circ x^{-1} = e$$

$$\Rightarrow a^k = x^{-1} \circ x$$

$$\Rightarrow a^k = e \Rightarrow a \text{ is of finite order. which}$$

gives contradiction. Therefore, $o(x \circ a \circ x^{-1})$ is infinite.

(Ex) In a group $(G,\circ)$, $a^{n+1}b^{n+1} = b^{n+1}a^{n+1}$ and $a^n b^n = b^n a^n$ hold for all $a,b \in G$, and for some integer n. Prove that the group is abelian.

Ans: $ab = a^{n+1}(a^{-n}b^{-n})b^{n+1}$

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

$= (a^{n+1}b^{-n})(a^{-n}b^{n+1})$ —— (i)

$(a^{n+1}b^n)^{n+1} = a^{n+1}(b^n a^{n+1})^n \cdot b^n$

$= (a^{n+1}(b^n a^{n+1})^{n+1})(b^n a^{n+1})^{-1} b^n$

$= ((b^n a^{n+1})^{n+1} \cdot a^{n+1}) a^{-(n+1)} b^{-n} b^n$

$[\because a^{n+1}b^{n+1} = b^{n+1}a^{n+1}]$

$= (b^n a^{n+1})^{n+1}$.

Also, $(a^{n+1}b^n)^n = a^{n+1}(b^n a^{n+1})^{n-1} b^n$

$= (a^{n+1}(b^n a^{n+1})^{-1})((b^n \cdot a^{n+1})^n b^n)$

$= a^{n+1} \cdot a^{-(n+1)} b^{-n}(b^n(b^n \cdot a^{n+1})^n)$

$= (b^n a^{n+1})^n$ $[\because a^n b^n = b^n a^n]$

Therefore, $a^{n+1}b^n = (a^{n+1}b^n)^{n+1}(a^{n+1}b^n)^{-n}$

$= (b^n a^{n+1})^{n+1}(b^n a^{n+1})^{-n} = b^n a^{n+1}$ (ii)

By similar steps, $b^{n+1}a^n = a^n b^{n+1}$ —— (iii)

From (ii) we have $a^{n+1}b^{-n} = b^{-n}a^{n+1}$ and from (iii), we have $b^{n+1}a^{-n} = a^{-n}b^{n+1}$.

Scanned with CamScanner

Finally from (i) we have $ab = (a^{n+1}b^{-n})(a^{-n}b^{n+1})$

$= b^{-n}(a^{n+1}b^{n+1})a^{-n}$

$= (b^{-n}b^{n+1})(a^{n+1}.a^{-n})$

$= ba$ for all $a, b \in G$.

Therefore G is an abelian group.

(Ex): Let (G, o) be a group and $a, b \in G$. Prove that $(a o b o a^{-1})^n = a o b^n o a^{-1}$ for all integers.

<u>Ans</u>: Given that $(a o b o a^{-1})^n = a o b^n o a^{-1}$.

This relation is proved by mathematical induction when n is positive integer.

<u>Case-I</u>: Let n be positive integer.

$\therefore$ Put $n=1$, $(a o b o a^{-1})^1 = a o b o a^{-1}$ which is true.

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

$= a o b o (a^{-1} o a) o b o a^{-1}$ [o is associative]

$= a o b o e o b o a^{-1}$ [Inverse]

$= a o b^2 o a^{-1}$. [Identity]

Thus, the relation is true for $n = 2$.

Let, the relation is true for $n = m$, m being a positive integer.

$\therefore (a o b o a^{-1})^m = a o b^m o a^{-1}$.

Now, $(a o b o a^{-1})^{m+1} = (a o b o a^{-1})^m o (a o b o a^{-1})$

$= a o b^m o (a^{-1} o a) o b o a^{-1})$

$= a o b^{m+1} o a^{-1}$.

Thus, the result is true for $n = m+1$ if it is true for $n = m$.

$\therefore$ By mathematical induction, the result is true for every positive integer.

Case- II When n is negative i.e $n = -m$, $(m>0)$

$$\therefore (a \circ b \circ a^{-1})^{n} = (a \circ b \circ a^{-1})^{-m}$$
$$= \{(a \circ b \circ a^{-1})^{m}\}^{-1}$$
$$= (a \circ b^{+m} \circ a^{-1})^{-1} \quad [\text{using Case- I}]$$
$$= (a^{-1})^{-1} \circ b^{-m} \circ a^{-1} \quad [(a \circ b)^{-1} = b^{-1} \circ a^{-1}]$$
$$= a \circ b^{-m} \circ a^{-1} \quad [(a^{-1})^{-1} = a]$$
$$= a \circ b^{n} \circ a^{-1}.$$

$$\therefore (a \circ b \circ a^{-1})^{n} = a \circ b^{n} \circ a^{-1}.$$

Case- III : When $n = 0$, then $(a \circ b \circ a^{-1})^{0} = a \circ b^{0} \circ a^{-1}$.

Thus, $(a \circ b \circ a^{-1})^{n} = a \circ b^{n} \circ a^{-1}$, for all integers.

(Ex) If $(G, \circ)$ be a finite group with identity e, prove that there exists a positive integer m such that $a^{m} = e$ holds $\forall a \in G$.

Ans: Let a be an element of a finite group $(G, \circ)$. Then $a, a^2, a^3, \ldots\ldots$ are all elements of G. Since G is finite, all the integral powers of a can not be distinct elements of G.

Let us suppose that $a^{r} = a^{s}$ $(r > s)$

$$\Rightarrow a^{r} \cdot a^{-s} = a^{s} \cdot a^{-s} \quad [a^{-s} \in G]$$
$$\Rightarrow a^{r-s} = e$$
$$\Rightarrow a^{m} = e, \quad m = r - s.$$

Thus, there exists a positive integer m such that $a^{m} = e$, $\forall a \in G$

Hence the result.

Ex In a group G, $a^m = b^m$ and $a^n = b^n$ $[\gcd(m,n)=1]$ holds for elements a, b in G. Prove that $a=b$.

Ans : Since $\gcd(m,n)=1$, there exist integers x, y such that $mx+ny=1$.

$$\therefore a = a^{mx+ny} = a^{mx}\, a^{ny} = (a^m)^x (a^n)^y$$
$$= (b^m)^x (b^n)^y \quad \left[\because \begin{matrix} a^m = b^m \\ a^n = b^n \end{matrix}\right]$$
$$= b^{mx+ny}$$
$$= b.$$

$\therefore a = b$. (Proved)

Ex In a group G, $a^m b^m = b^m a^m$, $a^n b^n = b^n a^n$ with $\gcd(m,n)=1$ for all a, b in G. Prove that G is abelian.

Ans : We 1st prove that a^m commutes with b^n and a^n commutes with b^m i.e. $a^m b^n = b^n a^m$ and $a^n b^m = b^m a^n$ for all $a, b \in G$.

$$(a^m b^n)^m = a^m (b^n a^m)^m a^{-m}$$
$$= (b^n a^m)^m a^m a^{-m}, \text{ (by given condition)}$$
$$= (b^n a^m)^m \quad \text{--- (i)}$$

$$(b^n a^m)^n = b^n (a^m b^n)^n b^{-n}$$
$$= (a^m b^n)^n b^n b^{-n} \text{ (By given condition)}$$
$$= (a^m b^n)^n$$

$$\therefore (b^n a^m)^n = (a^m b^n)^n \quad \text{--- (ii)}$$

Since $\gcd(m,n)=1$, using (i) & (ii) we have $a^m b^n = b^n a^m$ by the previous example.

Similarly, $a^n b^m = b^m a^n$.

Since $\gcd(m,n)=1$, $\exists$ integers x, y such that $mx+ny=1$

$$\therefore ab = a^{mx+ny} \cdot b^{mx+ny}$$

$$= (a^x)^m\left[(a^y)^n (b^x)^m\right](b^y)^n$$

$$= (a^x)^m \left[(b^x)^m (a^y)^n\right] (b^y)^n \quad \left[\because a^n b^m = b^m a^n \ \forall a, b \in G\right]$$

$$= \left[(a^x)^m (b^x)^m\right]\left[(a^y)^n (b^y)^n\right]$$

$$= \left[(b^x)^m (a^x)^m\right]\left[(b^y)^n (a^y)^n\right] \quad \left[\text{By given condition}\right]$$

$$= (b^x)^m \left[(a^x)^m (b^y)^n\right](a^y)^n$$

$$= (b^x)^m \left[(b^y)^n (a^x)^m\right](a^y)^n \quad \left[\because a^m b^n = b^n a^m \ \forall a, b \in G\right]$$

$$= (b^m)^x\left[(b^n)^y (a^m)^x\right](a^n)^y$$

$$= \left[(b^m)^x (b^n)^y\right]\left[(a^m)^x (a^n)^y\right]$$

$$= b^{mx+ny} \cdot a^{mx+ny}$$

$$= ba \quad \forall a, b \in G$$

$\therefore$ G is an abelian group.

EX Let $(G, \circ)$ be a group and $a \in G$. Prove that $o(a) = o(x \circ a \circ x^{-1})$ for every element $x \in G$. If a be the only element of order 2 in G, deduce that a commutes with every element of G.

Proof: Case-I: Let $o(a) = m$. Then $a^m = e$.

Now, $(x \circ a \circ x^{-1})^m = (x \circ a \circ x^{-1}) \circ (x \circ a \circ x^{-1}) \cdots \circ (x \circ a \circ x^{-1})$ [m times]

$= x \circ a^m \circ x^{-1}$ [Associative, inverse and identity]

$= x \circ x^{-1}$ $[a^m = e]$

$= e.$

Let $(x \circ a \circ x^{-1})^k = e$ for some positive integer $k < m$.

$\therefore (x \circ a \circ x^{-1})^k = e \Rightarrow x \circ a^k \circ x^{-1} = e$

$\Rightarrow a^k = x^{-1} \circ x = e$, a contradiction since $o(a) = m$.

So, m is the least positive integer such that $(x \circ a \circ x^{-1})^m = e$ $\therefore o(x \circ a \circ x^{-1}) = m$.

Case-II: Let $o(a)$ be infinite. Let $o(x \circ a \circ x^{-1}) = k$ (say).

$\Rightarrow (x \circ a \circ x^{-1})^k = e \Rightarrow x \circ a^k \circ x^{-1} = e \Rightarrow a^k = e$; showing that a is of finite order, a contradiction. $\therefore o(x \circ a \circ x^{-1})$ is infinite.

2nd Part: Since $o(a) = o(x \circ a \circ x^{-1}) = 2$ $\therefore a = x \circ a \circ x^{-1}$ $\forall x \in G$

$\Rightarrow x \circ a = a \circ x$ $\forall x \in G$.