Set-I (ii)

Addition Modulo m:

Let $a, b \in \mathbb{Z}$ and m be a fixed +ve integer. If r is the remainder $(0 \le r < m)$ when $a+b$ is divided by m, we define $a +_m b = r$.

Ex: (1) $20 +_6 5 = 1$

Since $20+5 = 25$
$= 4(6)+1$

$\therefore$ 1 is the remainder when $20+5$ is divided by 6.

(2) $24 +_5 4 = 3$

(3) $2 +_7 3 = 5$

(4) $-32 +_4 5 = 1$ $(\because -32+5 = -27 = (-7)(4)+1)$

(5) $-9 +_2 (-18) = 1$ $(\because -9-18 = -27 = (-14)(2)+1)$

(6) $0 +_5 (-3) = 2$ $(\because 0-3 = -3 = (-1)(5)+2)$

Note:

$$a +_m b = b +_m a$$

Congruences:

Let $a, b \in \mathbb{Z}$ and m be any fixed +ve integer if $a-b$ is divisible (divided) by m.

We say that a is congruent to b modulo m and we write it as $a \equiv b \pmod m$

This relation between integers a & b is called Congruence modulo m.

i.e, $a \equiv b \pmod m \iff m / a-b$

(or) $m / b-a$ (or) $\frac{a-b}{m} = q$ (i.e. $a-b = mq$ for $q \in \mathbb{Z}$).

and $a \not\equiv b \pmod m \Leftrightarrow m/(a-b)$ (or) $a-b \neq km$ for $k \in z$.

Note: [1]. If $a \equiv b \pmod m$ then we get the same remainder if a & b are separately divided by m.

Ex(1): If $22 \equiv 13 \pmod 3$

then 1 is the remainder when 22 & 13 are seperately divided by m.

(2) If $-7 \equiv 17 \pmod 6$

then 5 is the remainder when -7 & 17 are seperately divided by 6.

[2]. $a +_m b \equiv a+b \pmod m$

Ex: 1) $9 +_4 5 = 2$ and $9+5 = 14$

Now $14 \equiv 2 \pmod 4$

2) $12 +_4 7 = 3$ and $12+7 = 19$

Now $3 \equiv 19 \pmod 4$

→ If $a \equiv b \pmod m$, then $a +_m c = b +_m c$

Sol'n: For $a \equiv b \pmod m \Rightarrow m/a-b$

$\Rightarrow m/(a+c)-(b+c)$ for $c \in z$

$\Rightarrow a+c \equiv b+c \pmod m$

$\Rightarrow a +_m c = b +_m c$

Equivalence classes (or) Equivalence Sets:

Let A be a non-empty set and let R be an equivalence relation in A.

Further let 'a' be an arbitrary element of A. The elements $x \in A$ satisfying $x R a$ constitute a subset A_a of A, called an equivalence class of 'a' w.r.t R. we shall denote this equivalence class by A_a or by $[a]$ or by $\bar{a}$

i.e, A_a or $[a]$ or $\bar{a} = \{ x / x \in A$ and $(x, a) \in R$ i.e $xRa \}$

Ex: Let us determine the equivalence classes in the set I of all integers w.r.t the equivalence relation congruence modulo 5.

$I = \{ \ldots\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\ldots \}$

$x \in I$ is congruent to $0 \in I \pmod 5$ form an equivalence class I_0.

Here $x \equiv 0 \pmod 5$

$\Rightarrow 0 \equiv 0 \pmod 5$

$5 \equiv 0 \pmod 5$

$10 \equiv 0 \pmod 5$

$15 \equiv 0 \pmod 5$ etc.

$\therefore I_0 = \{ \ldots\ldots -10, -5, 0, 5, 10, \ldots\ldots \}$

$= \{ 5k / k \in I \}$

$= 5I.$

The integers $(x \in I)$ congruent to 1 modulo 5 form another equivalence class I_1.

Here $x \equiv 1$ (modulo 5)

$\Rightarrow 1 \equiv 1 \pmod 5$, $6 \equiv 1 \pmod 5$, $11 \equiv 1 \pmod 5$

$16 \equiv 1 \pmod 5$ etc.

$\therefore I_1 = \{ \ldots\ldots -9, -4, 1, 6, 11, 16, \ldots\ldots \}$

$= \{ 5k+1 / k \in I \}$

Similarly $I_2 = \{ 5k+2 / k \in I \}$

$= \{ \ldots\ldots -8, -3, +2, 7, 12, \ldots\ldots \}$

$I_3 = \{ 5k+3 / k \in I \}$

$= \{ \ldots\ldots -7, -2, 3, 8, 13, \ldots\ldots \}$

and $I_4 = \{ 5k+4 / k \in I \}$

$= \{ \ldots\ldots -6, -1, 4, 9, 14, \ldots\ldots \}$

These classes have the following properties.

(i) The set I is the union of these five non-empty classes

(ii) Integers in each class have a relation of congruence modulo 5 with one another.

(iii) Integers in different classes donot have a relation of congruence modulo 5 with one another.

(iv) The classes are mutually disjoint.
i.e, no two of them have any elements in common.

Partition of a set:

Let S be a non-empty set. A set $P = \{A, B, C \ldots\}$ of non-empty subsets of S will be called a partition of S if

(i) $A \cup B \cup C \cup \ldots\ldots = S$

(ii) the intersection of every pair of distinct subsets of $S \in P$ is the null set.
i.e, if $A, B \in P$ then $A \cap B = \phi$.

Ex: Let I be the set of all integers and $x \equiv y \pmod 5$ is an equivalence relation in I. consider the set of five equivalence classes

I_0, I_1, I_2, I_3 & I_4

where $I_0 = \{ \ldots\ldots -10, -5, 0, 5, 10, \ldots\ldots \}$

$I_1 = \{ \ldots\ldots -9, -4, 1, 6, 11, \ldots\ldots \}$

$\bar{I}_2 = \{ \ldots\ldots -8, -3, 2, 7, 12, \ldots\ldots \}$

$\bar{I}_3 = \{ \ldots\ldots -7, -2, 3, 8, 13, \ldots\ldots \}$

$\bar{I}_4 = \{ \ldots\ldots -6, -1, 4, 9, 14, \ldots\ldots \}$

we observe that

(i) the sets $I_0, \bar{I}_1, \bar{I}_2, \bar{I}_3$ & I_4 are non-empty.

(ii) the sets I_0, I_1, I_2, I_3 & I_4 are pair wise disjoint.

(iii) $I = I_0 \cup I_1 \cup I_2 \cup I_3 \cup \bar{I}_4$.

$\therefore \{ I_0, I_1, I_2, I_3, \bar{I}_4 \}$ is a partition of $\bar{I}$.

→ The operation congruence modulo 'm' is an equivalence relation in the set of integers. So the operation congruence modulo 'm' partitions $\mathbb{Z}$ into disjoint equivalence classes called residue classes modulo 'm' or congruence modulo 'm'.

→ $\{0, 1, 2, 3, \ldots\ldots (m-1)\}$ is called the complete set of least positive residues modulo 'm' or simply set of residues modulo 'm'.

→ Let $m \in \mathbb{N}$ and $r \in \mathbb{Z}$. Let $\bar{r} = \{ x / x \in \mathbb{Z}, x \equiv r \pmod{m} \}$

Then the set $\mathbb{Z}_m = \{ \bar{0}, \bar{1}, \bar{2}, \ldots\ldots (\overline{m-1}) \}$ is called the complete set of least +ve residue classes modulo 'm'. (or) simply set of residue classes modulo 'm'.

Addition of residue classes:

For $\bar{a}, \bar{b} \in \mathbb{Z}_m$, we define addition of residue classes, denoted by $+$, as $\bar{a} + \bar{b} = \overline{a+b}$

Note [1] $+$ on the RHS is ordinary addition.

[2] If r is the remainder $(0 \le r < m)$ when

$a+b$ is divided by m then $\overline{a+b} = \bar{r}$

i.e, $\bar{a} + \bar{b} = \bar{r}$

3. The set $G = \{0, 1, 2, \ldots, (m-1)\}$ of first m non-negative integers is an abelian group w.r.t addition modulo 'm'.

Problems:

→ P.T the set $G = \{0, 1, 2, 3, 4\}$ is an abelian group of order 5 w.r.t addition modulo 5.

Sol^n: Construct composition table

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Now we can easily prove all the axioms of abelian group.

$\therefore (G, +_5)$ is an abelian group.

→ P.T the set $G = \{0, 1, 2, 3, 4, 5\}$ is an abelian group w.r.t $+_6$.

Note: The set of residue classes modulo 'm' is abelian group of order 'm' w.r.t addition of residue classes.

Multiplication modulo p:

→ If a and b are integers and p is a fixed +ve integer if ab is divided by p such that r is the remainder $(0 \le r < p)$, we define $a \times_p b = r$.

Ex: (1) $20 \times_6 5 = 4$

since $20 \times 5 = 100$
$= 16(6) + 4$

i.e, 4 is the remainder when 20×5 is divided by 6.

(2) $24 \times_5 4 = 1$

(3) $3 \times_7 3 = 2$

(4) $(-32) \times_4 5 = 0$

since $-32 \times 5 = -160$
$= (-40)(4) + 0$

(5) $0 \times_5 (-3) = 0$

$(\because 0 \times (-3) = 0$
$= 0(5) + 0)$

Note: 1) $a \times_p b \equiv ab \pmod p$

Ex: $7 \times_5 3 \equiv 21 \pmod 5$

$(\because 7 \times_5 3 = 1$ and $1 - 21 = (-4)5$

2) $a \times_m b = b \times_m a$

Ex: $3 \times_7 6 = 6 \times_7 3$

(3) If $a \equiv b \pmod p$, then $a \times_p c = b \times_p c$

Ex: If $3 \equiv 23 \pmod 5$

then $3 \times_5 4 = 23 \times_5 4$

$(\because 3 \times_5 4 = 2$ & $23 \times_5 4 = 2)$

prime integer:

→ An integer p is said to be a prime integer if $p \neq 0$, $p \neq \pm 1$ and the only divisors of p are $\pm 1, \pm p$.

Ex: $\pm 2, \pm 3, \pm 5, \pm 7, \ldots\ldots$ are prime integers.

Note: 1. If p is a prime integer and $a, b \in I$ such that $p \mid ab$ then $p \mid a$ or $p \mid b$.

Multiplicative group of integers modulo p where p is prime:

- The set $G = \{1, 2, 3, \ldots\ldots p-1\}$ where p is prime,

form a finite abelian group of order $p-1$ w.r.t multiplication modulo p.

Note: [1]. Suppose in the set G, p is not prime but p is composite

then $\exists$ two integers a and b such that $1 < a \leq p-1$, $1 < b \leq p-1$ and $a \cdot b = p$

$\therefore a \times_p b = 0$ and $0 \notin G$.

$\therefore G$ is not closed w.r.t composition multiplication modulo p.

$\therefore G$ is not group.

[2]. If we include 0 in the set G then for this composition G is not a group ($\because$ inverse of 0 is not exist).

[3]. **Multiplicative group of non-zero residue classes modulo a prime integer p:**

→ The set of non-zero residue classes modulo a prime integer p forms an abelian group of order $(p-1)$ w.r.t multiplication of residue classes.

Problems:

→ P.T the set $G = \{1, 2, 3, 4, 5, 6\}$ is a finite abelian group order 6 w.r.t $\times_7$.

→ P.T $G = \{1, 2, 3, 4\}$ is abelian group of order 4 w.r.t $\times_5$.

→ P.T $G = \{1, 3, 5, 7\}$ is an abelian group of order 4 w.r.t $\times_8$

→ Show that the set of integers $\{1, 5, 7, 11\}$ form an abelian group w.r.t $\times_{12}$.

→ In a group $(G,\cdot)$, for $a \in G$, a is idempotent $\Leftrightarrow a = e$ (20)

Soln: $(G,\cdot)$ is a group.

Let $a \in G$, a is idempotent.

$\Leftrightarrow a \cdot a = a$

$\Leftrightarrow a \cdot a = ae.$

$\Leftrightarrow a = e.$ (By LCL)

Note: If a is an element in a group $(G,\cdot)$ such that $a \cdot a = a$ then a is called an idempotent element.

→ If a, b are any two elements of a group $(G,\cdot)$ which commute. Show that (i) $\bar{a}^1$ and b commute (ii) $\bar{b}^1$ and a commute and (iii) $\bar{a}^1$ and $\bar{b}^1$ commute.

Soln: Given that $(G,\cdot)$ is a group such that

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

(i) we have

$ab = ba \Rightarrow \bar{a}^1(ab) = \bar{a}^1(ba)$

$\Rightarrow (\bar{a}^1 a)b = \bar{a}^1(ba)$

$\Rightarrow eb = \bar{a}^1(ba)$

$\Rightarrow b = (\bar{a}^1 b)a$

$\Rightarrow b\bar{a}^1 = [(\bar{a}^1 b)a]\bar{a}^1$

$\Rightarrow b\bar{a}^1 = (\bar{a}^1 b)(a\bar{a}^1)$

$\Rightarrow b\bar{a}^1 = (\bar{a}^1 b)e$

$\Rightarrow \boxed{b\bar{a}^1 = \bar{a}^1 b}$

$\therefore \bar{a}^1$ & b commute:

Similarly (ii) can be proved.

(iii) we have $ab = ba$

$\Rightarrow (ab)^{-1} = (ba)^{-1}$

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

$\Rightarrow \bar{a}^1$ & $\bar{b}^1$ commute.

Law of Integral exponents:

Let $(G,\cdot)$ be a group. Let $a \in G$. Then by closure law $a, aa, aaa, \ldots\ldots$ are all elements of G.

Since the composition in G obeys general associative law. $aaa\ldots\ldots a$ (n times) is independent of the manner in which the elements are grouped.

For any integer 'n', we define a^n as follows:

(i) $a^0 = e$ is the identity element.

(ii) $a^1 = a$

(iii) for $n \geq 1$, $a^{n+1} = a^n \cdot a$

(iv) for $n > 0$, $\bar{a}^n = (\bar{a}^1)^n$

Ex: $a^2 = a^1 \cdot a = a \cdot a$

$a^3 = a^2 \cdot a = (aa)a$ etc.

$\bar{a}^4 = (\bar{a}^1)^4 = (\bar{a}^1)^3 (\bar{a}^1)^1$

$= \left[(\bar{a}^1)^2 (\bar{a}^1)^1\right] \bar{a}^1$

$= \left[(\bar{a}^1)^1 (\bar{a}^1)^1\right] \bar{a}^1 \cdot \bar{a}^1$

$= \bar{a}^1 \bar{a}^1 \bar{a}^1 \bar{a}^1$ etc.

Note:

(1) $a^n = a \cdot a \cdot \ldots \cdot a$ (n times) and $a^n \in G$

(2) $\bar{a}^n = (\bar{a}^1)(\bar{a}^1)(\bar{a}^1)\ldots\ldots(\bar{a}^1)$ (n times) and $\bar{a}^n \in G$

(3) If additive operation $+$ is taken as the operation, then a^n in multiplication notation becomes na in additive notation.

Identity element $= 0$

and inverse of a is $-a$.

$na = a + a + \ldots\ldots + a$ (n times) and

$-na = (-a) + (-a) + \ldots\ldots + (-a)$ (n times)

when n is +ve integer.

Also $na \in G$ & $-na \in G$.

→ Let G be a group and $a \in G$. If n is any +ve integer, then (i) $a.a^n = a^n.a$ and (ii) $a^n, \bar{a}^n$ are inverse elements to one another. (21)

Soln: we prove the statements by using mathematical induction.

(i) Let S(n) be $a.a^n = a^n.a$ for $n \in Z^+$

put n=1

$\therefore aa' = a.a = a'.a$

$\therefore$ S(1) is true.

Suppose for n=k S(k) is true.

$\therefore aa^k = a^k.a$ —— (1)

NOW $aa^{k+1} = a(a^k a)$

$= (aa^k)a$ (by asso.)

$= (a^k.a).a$ (by (1))

$= a^{k+1}a$

$\therefore$ S(k+1) is true.

$\therefore$ By induction S(n) is true for every +ve integer 'n'.

(ii) Let S(n) be that a^n and $\bar{a}^n$ are inverse to one another.

Let e be the identity element in G.

Since $a\bar{a}^1 = e = \bar{a}^1 a$.

$\Rightarrow a^1\bar{a}^1 = e = \bar{a}^1 a^1$

$\Rightarrow$ S(1) is true.

Let S(k) be true.

$\therefore a^k \bar{a}^k = e = \bar{a}^k a^k$. —— (2)

NOW $a^{k+1}.\bar{a}^{(k+1)} = a^{k+1}(\bar{a}^1)^{k+1}$

$= a^k.a\,(\bar{a}^1)^k\,\bar{a}^1$

$= a.a^k.a^{-k}.\bar{a}^1$ (by (i))

$= a(a^k.\bar{a}^k)\bar{a}^1$ (by asso.)

$= a e \bar{a}^1$ (by (2))

$= a \bar{a}^1 = e$

Similarly $\bar{a}^{(k+1)} a^{k+1} = e$

$\therefore a^{k+1} \bar{a}^{(k+1)} = \bar{a}^{(k+1)} a^{k+1} = e$

$\therefore S(k+1)$ is true.

By induction $S(n)$ is true for every +ve integer n.

Note: If $n \in N$, $(a^n)^{-1} = \bar{a}^n$ and $(\bar{a}^n)^{-1} = a^n$.

→ Let G be a group. Let $a, b \in G$ then

(i) $a^m a^n = a^{m+n}$ for $m, n \in N$

(ii) $(a^m)^n = a^{mn}$ for $m, n \in N$

(iii) $(ab)^n = a^n b^n$ when G is abelian and $n \in N$.

(iv) $e^n = e$ for $n \in N$.

Soln: we prove the statements by using the principle of mathematical induction.

(i) Let $S(n)$ be $a^m \cdot a^n = a^{m+n}$ for $m, n \in N$.

put $n = 1$

$\therefore a^m \cdot a^1 = a^{m+1}$ (by defn)

$\therefore S(1)$ is true.

Let $S(k)$ be true.

$\therefore a^m \cdot a^k = a^{m+k}$ ——(1)

Now $a^m \cdot a^{k+1} = a^m (a^k \cdot a)$

$= (a^m \cdot a^k) a$

$= a^{m+k} \cdot a^1$ (by (1))

$= a^{m+k+1}$ (by defn)

$\therefore S(k+1)$ is true.

$\therefore$ By induction, $S(n)$ is true for $n \in N$.

Note: $a^m a^n = a^n \cdot a^m$.

Since $a^m a^n = a^{m+n}$

$= a^{n+m} = a^n a^m$.

(ii) Let $S(n)$ be

$(a^m)^n = a^{mn}$ for $m, n \in N$.

put $n = 1$

$\therefore (a^m)^1 = a^m = a^{m \cdot 1}$ (by defn)

$\therefore S(1)$ is true.

Let $S(k)$ be true.

$\therefore (a^m)^k = a^{mk}$ —— (1)

Now $(a^m)^{k+1} = (a^m)^k \cdot (a^m)^1$

$= a^{mk} \cdot a^m$ (by (1))

$= a^{mk+m}$

$= a^{m(k+1)}$

$\therefore S(k+1)$ is true.

$\therefore$ By Induction, $S(n)$ is true for $n \in N$.

Note: $(a^m)^n = (a^n)^m$

Since $(a^m)^n = a^{mn} = (a^n)^m$ for $m, n \in N$.

(iii) Let $S(n)$ be

$(ab)^n = a^n b^n$ for $n \in N$

and G is abelian.

put $n = 1$

$\therefore (ab)^1 = ab = a^1 \cdot b^1$

$\therefore S(1)$ is true.

Let $S(k)$ be true for some $k \in N$

$\therefore (ab)^k = a^k b^k$. —— (1)

Now $(ab)^{k+1} = (ab)^k (ab)$

$= (a^k b^k)(ab)$ (by (1))

$= (a^k b^k)(ba)$ ($\because$ G is abelian i.e, $ab = ba$)

$= a^k (b^k b) a$

$= a^k (b^{k+1}) a$

$= a^k (b^{k+1} a)$

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

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

$= a^{k+1} b^{k+1}$

$\therefore$ S(K+1) is true.

$\therefore$ By the induction S(n) is true for $n \in N$

(iv) Let S(n) be $e^n = e$ for $n \in N$

Put $n=1$, $\therefore e^1 = e$

$\therefore$ S(1) is true

Let S(K) be true for some $K \in N$.

$\therefore e^K = e$ —— (1)

Now $e^{K+1} = e^K \cdot e$

$= e \cdot e = e$.

$\therefore$ S(K+1) is true.

$\therefore$ By induction method S(n) is true for $n \in N$.

Note: If G is an additive group, the above properties can be stated as

(i) $-(na) = (-n)a$ for $n \in Z$.

(ii) $ma + na = (m+n)a$

$= (n+m)a = na + ma$ for $m, n \in Z$.

(iii) $n(ma) = (nm)a$

$= (mn)a = m(na)$ for $m, n \in Z$

(iv) $m(a+b) = ma + mb$ for $m \in Z$.

→ In a group G for every $a \in G$, $a^2 = e$ prove that G is an abelian group.

Soln: Let $(G, \cdot)$ be the given group.

$\forall a, b \in G \Rightarrow ab \in G$

Since $a \in G$, $a^2 = e$

we have $(ab)^2 = e$

$\Rightarrow (ab)(ab) = e$

$\Rightarrow$ inverse of ab is ab.

$\therefore (ab) = (ab)^{-1}$

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

$\therefore (ab) = b^{-1}a^{-1}$ —— (1)

But $a^2=e \Rightarrow aa=e$

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

Similarly $b^2=e \Rightarrow b^{-1}=b$

① $\equiv ab=ba$

$\therefore G$ is abelian

→ Show that in a group G for $a,b \in G$, $(ab)^2=a^2b^2 \Leftrightarrow G$ is abelian.

Sol^n:

Part 1:

Let $(G,\cdot)$ be the given group.

$\forall a,b \in G$ and $(ab)^2=a^2b^2$

TO prove that G is abelian.

NOW $\forall a,b \in G$

$\Rightarrow (ab)^2=a^2b^2$

$\Rightarrow (ab)(ab)=aabb$

$\Rightarrow a(ba)b=a(ab)b$

$\Rightarrow ba=ab$ (By LCL & RCL)

$\Rightarrow G$ is abelian.

Part 2:

Let G be abelian.

TO prove that $(ab)^2=a^2b^2$

NOW we have

$(ab)^2=(ab)(ab)$

$=a(ba)b$

$=a(ab)b$ ($\because G$ is abelian)

$=(aa)(bb)$

$=a^2b^2$

$\therefore (ab)^2=a^2b^2$.

→ If G is a group of even order, prove that it has an element $a \neq e$ satisfying $a^2=e$.

Sol^n: In a group every element possesses its inverse and the identity element e is its own inverse.

since the number of elements in G is even (Given)

∴ there is atleast one more element of G which is its own inverse.

∴ In G, there is an element $a \neq e$ such that

$$a = a^{-1}$$
$$\Rightarrow aa = aa^{-1}$$
$$\Rightarrow a^2 = e.$$

→ If G is a group such that $(ab)^m = a^m b^m$ for three consecutive integers m for all $a, b \in G$, show that G is abelian.

Soln: Let $a, b \in G$

Let $m, m+1, m+2$ be three consecutive integers.

By hypothesis, $(ab)^m = a^m b^m$ —①

$$(ab)^{m+1} = a^{m+1} b^{m+1} \text{ —②}$$

and $$(ab)^{m+2} = a^{m+2} b^{m+2} \text{ —③}$$

NOW $(ab)^{m+2} = (ab)^{m+1}(ab)$ (by defn)

$\Rightarrow a^{m+2} b^{m+2} = a^{m+1} b^{m+1} ab.$

$\Rightarrow a \cdot a^{m+1} b^{m+1} b = a\, a^m b^m ba\, b$

$\Rightarrow a^{m+1} b^{m+1} = a^m b^m ba$

$\Rightarrow (ab)^{m+1} = (ab)^m ba$

$\Rightarrow (ab)^m (ab) = (ab)^m ba$

$\Rightarrow ab = ba$

$\Rightarrow$ G is abelian

Order of an element of a group:-

Let $(G, \cdot)$ be a group. $a \in G$ then the order of the element 'a' is defined as the least +ve integer 'n' such that $a^n = e$.

– If there exist no +ve integer 'n' such that $a^n = e$ then we say that a is of infinite order or zero order. and the order of a is denoted by $o(a)$.

Note: If $(G,+)$ is a group then $na = e$ where n is the least +ve integer and $a \in G$

Examples:

(1) $G = \{1, -1, i, -i\}$ is a multiplicative group.

Now $1^1 = 1 = 1^2 = 1^3 = 1^4 = \cdots\cdots$

$\therefore o(1) = 1$

$(-1)^1 = -1$; $(-1)^2 = 1 = (-1)^4 = (-1)^6 = \cdots\cdots$

$\therefore o(-1) = 2$

$(i)^1 = i$; $(i)^2 = -1$, $(i)^3 = -i$, $(i)^4 = 1 = (i)^8 = (i)^{12} = \cdots\cdots$

$\therefore o(i) = 4$

and $(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$, $(-i)^4 = 1 = (-i)^8 = \cdots\cdots$

$\therefore o(i) = 4$

(2) $G = \{1, \omega, \omega^2\}$.

$1^1 = 1$ $\quad \omega^1 = \omega$ $\quad (\omega^2)^1 = \omega^2$

$\therefore o(1) = 1$ $\quad \omega^2 = \omega^2$ $\quad (\omega^2)^2 = \omega$

$\omega^3 = 1$ $\quad (\omega^2)^3 = 1$

$\therefore o(\omega) = 3$ $\quad \therefore o(\omega^2) = 3$.

(3) $G = \{1, 3, 5, 7\}$ is a group w.r.t $\times_8$.

$1^1 = 1$ $\quad 3^1 = 3$ $\quad 5^1 = 5$ and $7^1 = 7$

$o(1) = 1$ $\quad 3^2 = 3 \times_8 3 = 1$ $\quad 5^2 = 5 \times_8 5 = 1$ $\quad 7^2 = 7 \times_8 7 = 1$

$\therefore o(3) = 2$ $\quad \therefore o(5) = 2$ $\quad \therefore o(7) = 2$

(4) $G = (Q - \{0\}, \cdot)$ is a group.

$1^1 = 1$ $\quad (-1)^1 = -1$

$o(1) = 1$ $\quad (-1)^2 = 1$

$o(-1) = 2$

The order of every other element of G is infinite

since $3 \in G$ and $3^m \neq 1$ for any +ve integer m.

(5) $G = \{0, 1, 2, 3, 4, 5\}$ is a group w.r.t $+_6$

$1(0) = 0$ $\quad$ $1(1) = 1$

$O(0) = 1$ $\quad$ $2(1) = 2 = 1 +_6 1 = 2$

$3(1) = 3 = 1 +_6 1 +_6 1 = 3$

$4(1) = 4 = 1 +_6 1 +_6 1 +_6 1 = 4$

$5(1) = 5 = 1 +_6 1 +_6 1 +_6 1 +_6 1 = 5$

$6(1) = 6 = 1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 = 0$

$\therefore O(1) = 6$

Similarly we can easily see

$O(2) = 3$, $O(3) = 2$, $O(4) = 3$, $O(5) = 6$.

(6) $G = (I, +)$ is a group.

$1(0) = 0$

$\therefore O(0) = 1$

If $a(\neq 0) \in \mathbb{Z}$ then there exists no +ve integer $n \in I^+$ such that $na = e$

$\therefore O(a) = \infty$ or 0.

Note: [1] The order of an identity element is 1

[2] If $a^m = e$ in group G where m is a +ve integer then the order of 'a' is finite.

Also $O(a) \leq m$

Observe that, by definition $O(a) \neq m$.

→ 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 $(G, \cdot)$ be the given finite group.

Let $a \in G$

By closure property

$a \cdot a = a^2 \in G$

$a \in G,\ a^2 \in G \Rightarrow a \cdot a^2 = a^3 \in G$ etc.

$\therefore a, a^2, a^3, \ldots \in G$

Since G is finite, all these elements cannot be different.

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

Now $a^r a^{-s} = a^s a^{-s}$ $(\because a^s \in G \Rightarrow a^{-s} \in G)$

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

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

$\Rightarrow a^m = e$ where $r - s = m > 0$ $(\because r > s \Rightarrow r - s > 0)$

$\therefore \exists$ a +ve integer m such that $a^m = e$

$\therefore$ every collection of +ve integers has least element say 'n'.

$\therefore \exists$ a least +ve integer 'n' such that $a^n = e$

$\therefore o(a) = n$

$\therefore$ order of 'a' is finite.

Now to prove that $o(a) \leq o(G)$

If possible let $o(a) > o(G)$.

Let $o(a) = n$ i.e $a^n = e$

By closure property,

we have $a^1, a^2, a^3, \ldots a^n \in G$.

No two of these elements are equal.

because if possible, let $a^r = a^s$, $1 \leq s < r \leq n$

$1 \leq 1 < 2 \leq 2$

$0 < 2-1 < 2$

$o(a) \leq (r-s) < n$

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

since $0 < r - s < n$

$\therefore a^{r-s} = e \Rightarrow o(a) \leq r - s < n$

$\Rightarrow o(a) < n$ which is contradiction.

$\therefore$ The n elements $a^1, a^2, \ldots a^n$ are distinct elements of G.

$\therefore o(a) > o(G)$ is wrong.

$\therefore o(a) \leq o(G)$

→ In a group G, if $a \in G$ then $o(a) = o(a^{-1})$.

proof: Let $o(a)=n$ & $o(a^{-1})=m$

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

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

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

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

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

$\Rightarrow m \leq n$ ——①

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

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

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

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

$\Rightarrow a^m = e$

$\Rightarrow o(a) \leq m$

$\Rightarrow n \leq m$ ——②

from ① & ② we have $n = m$

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

→ The order of any +ve integral power of an element 'a' in a group G cannot exceed the order of an element 'a'.

i.e, $o(a^r) \leq o(a)$ for $a \in G$ and $r \in N$.

proof: Let $o(a^r) = m$ & $o(a) = n$

Since $o(a^r) = m$

i.e, m is the least +ve integer such that $(a^r)^m = e$.

Since $o(a) = n$

i.e, n is the least +ve integer such that $a^n = e$

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

$\Rightarrow (a^n)^r = e^r$; $r \in N$

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

$\Rightarrow o(a^r) \leq n$

$\Rightarrow m \leq n$.

i.e, $o(a^r) \leq o(a)$

Sup → The orders of a & $b^{-1}ab$ are same, where $a, b \in G$

i.e, $o(a) = o(b^{-1}ab)$

Proof: Let $o(a) = m$ & $o(b^{-1}ab) = n$

Since $o(a) = m$

i.e, m is the least +ve integer such that $a^m = e$

Since $o(b^{-1}ab) = n$.

i.e, n is the least +ve integer such that $(b^{-1}ab)^n = e$.

Now we have

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

$$(b^{-1}ab)^2 = (b^{-1}ab)(b^{-1}ab)$$

$$= b^{-1}a(bb^{-1})ab. \quad \text{(By asso)}$$

$$= b^{-1}aeab \quad \text{(by inverse)}$$

$$= b^{-1}aab \quad \text{(by identity)}$$

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

In general, we get

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

$$= b^{-1}eb \quad (\because a^m = e)$$

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

$$= e$$

$\therefore o(b^{-1}ab) \leq m$

$\Rightarrow n \leq m$ ——— (1)

Again, $(b^{-1}ab)^n = b^{-1}a^nb$

$e = b^{-1}a^nb \quad (\because (b^{-1}ab)^n = e)$

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

$\Rightarrow e = a^n$ (by LCL & RCL)

$\Rightarrow a^n = e$

$\Rightarrow o(a) \leq n$

$\Rightarrow m \leq n$ ——— (2)

from (1) & (2) we have

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

→ The order of ab is same as that of ba where a, b are elements of a group G.

proof: WKT $o(a) = o(b^{-1}ab)$

we have

$$o(ba) = o(b^{-1}(ba)b)$$

$$\Rightarrow o(ba) = o((b^{-1}b)ab)$$

$$= o(eab)$$

$$= o(ab)$$

$\therefore o(ba) = o(ab)$

$\therefore$ The orders of ab & ba are same.

→ If a is an element of order n (i.e, $o(a) = n$) and p is prime to 'n' then a^p is also of order 'n'.

Proof: Let $o(a^p) = m$

i.e, m is the least +ve integer such that $(a^p)^m = e$

Since $o(a) = n$

i.e, n is the least +ve integer such that $a^n = e$

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

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

$$\Rightarrow o(a^p) \leq n$$

$$\Rightarrow m \leq n \quad \text{---} (1)$$

Since p is prime to n.

i.e, p, n are relatively prime.

$\therefore \exists$ two integers x & y such that

$$px + ny = 1$$

NOW $a = a^1$

$$= a^{px+ny}$$

$$= a^{px}\, a^{ny}$$

$$= (a^p)^x (a^n)^y$$

$$= (a^p)^x e^y$$

$$= (a^p)^x e$$

$$a = (a^p)^x.$$

$\Rightarrow a^m = [(a^p)^x]^m$

$= [(a^p)^m]^x$

$= e^x$

$= e$

$\therefore o(a) \leq m$

$\Rightarrow n \leq m$ ——— (2)

from (1) & (2) we have $m = n$

i.e., $o(a^p) = o(a)$

→ In a group, if $ba = a^m b^n$, prove that the elements $a^m b^{n-2}$, $a^{m-2} b^n$, ab^{-1} have the same order.

Soln: we have

$a^m b^{n-2} = a^m b^n b^{-2}$

$= bab^{-2}$ $(\because ba = a^m b^n)$

$= bab^{-1}b^{-1}$

$= (b^{-1})^{-1}(ab^{-1})b^{-1}$

W.K.T $o(a) = o(b^{-1}ab)$ ——— (1)

where $a, b \in G$.

$\therefore o(a^m b^{n-2}) = o((b^{-1})^{-1}(ab^{-1})b^{-1})$

$\therefore o(a^m b^{n-2}) = o(ab^{-1})$ ——— (2) (by (1))

Now we have

$a^{m-2} b^n = a^{-2} a^m b^n$

$= a^{-2} ba$

$= a^{-2} ba^{-1} a^2$

$= (a^2)^{-1}(ba^{-1})a^2$

$\therefore o(a^{m-2} b^n) = o[(a^2)^{-1}(ba^{-1})a^2]$

$= o(ba^{-1})$ (by (1))

$= o[(ba^{-1})^{-1}]$ $(\because o(a) = o(a^{-1}))$

$= o(ab^{-1})$ ——— (3)

from (2) & (3)

$o(a^m b^{n-2}) = o(ab^{-1}) = o(a^{m-2} b^n)$

IFoS-2011

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

Sol^n: we have

$$(aba^{-1})^2 = (aba^{-1})aba^{-1}$$
$$= ab(a^{-1}a)ba^{-1}$$
$$= abeba^{-1}$$
$$= ab^2a^{-1}$$
$$= aaba^{-1}a^{-1} \quad (\because aba^{-1} = b^2)$$
$$= a^2ba^{-2}$$

Now $(aba^{-1})^4 = \{(aba^{-1})^2\}^2$
$$= (a^2ba^{-2})^2$$
$$= a^2ba^{-2} \cdot a^2ba^{-2}$$
$$= a^2b(a^{-2}a^2)ba^{-2}$$
$$= a^2beba^{-2}$$
$$= a^2b^2a^{-2}$$
$$= a^2aba^{-1}a^{-2}$$
$$= a^3ba^{-3}$$

Now $(aba^{-1})^8 = \{(aba^{-1})^4\}^2$
$$= (a^3ba^{-3})^2$$
$$= a^3ba^{-3} \cdot a^3ba^{-3}$$
$$= a^3b(a^{-3}a^3)ba^{-3}$$
$$= a^3b^2a^{-3}$$
$$= a^3aba^{-1}a^{-3}$$
$$= a^4ba^{-4}$$

Now $(aba^{-1})^{16} = \{(aba^{-1})^8\}^2$
$$= (a^4ba^{-4})^2$$
$$= a^4ba^{-4} \cdot a^4ba^{-4}$$
$$= a^4b(a^{-4}a^4)ba^{-4}$$
$$= a^4b^2a^{-4}$$
$$= a^4aba^{-1}a^{-4}$$
$$= a^5ba^{-5}$$

$= ebe^{-1} \quad (\because a^5 = e)$

$= be$

$= b$

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

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

$\Rightarrow b^{32} = b$

$\Rightarrow b^{32} = b$

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

Since $b^m = e \Rightarrow o(b) / m$ i.e $\frac{31}{dy}$

$\therefore o(b) / 31$

But 31 is prime integer

$\therefore o(b) = 1$ or 31

if $b = e$ then $o(b) = 1$

if $b \neq e$ then $o(b) = 31$

Division algorithm:

Let $a, b \in I$ with $b \neq 0$ then we can divide 'a' by b to get a non-negative remainder 'r' which is smaller than b.

In other words if $a, b (\neq 0) \in I$ then there exists integers q, r such that $a = bq + r$ where $0 \leq r < |b|$.

Ex: Let $-15, -9 \in I$

then $-15 = 2(-9) + 3$

Here $0 < 3 < |-9|$

→ If a is an element of a group G such that $o(a) = n$ then $a^m = e$ iff n/m. (i.e, n is a divisor of m).

Proof: Given that a is an element of a group G such that $o(a) = n$.

i.e, n is the least +ve integer such that $a^n = e$

Let m be the +ve integer such that $a^m = e$

then we have to prove that n/m.

Since $a^m = e$

where m is the +ve integer such that

$o(a) \leq m$

$\Rightarrow n \leq m$

Case(i) : If $n = m$ then n/m

Case(ii) If $n < m$ (i.e, $n \neq m$) then by division algorithm $\exists$ two integers q & r such that $m = nq + r$ where $0 \leq r < n$

$$\Rightarrow a^m = a^{nq+r}$$
$$= a^{nq} a^r$$
$$= (a^n)^q . a^r$$
$$= e^q . a^r \quad (\because a^n = e)$$
$$= a^r$$

$\therefore a^m = a^r$.

$\Rightarrow a^m = a^r$

$\Rightarrow a^r = e \quad (\because a^m = e)$

Since $0 \leq r < n$

$\therefore a^r = e$

$\Rightarrow r$ must be equal to '0' because otherwise $o(a) \neq n$

if $o(a) = n$ then $\exists$ no +ve integer $r < n$ such that $a^r = e$

$\therefore m = nq + 0$

$\Rightarrow m = nq$

$\Rightarrow \frac{m}{n} = q$

$\Rightarrow n/m$.

Conversely Suppose that n/m then we prove that $a^m = e$

Since n/m

i.e, n is divisor of m $\exists$ an integer q such that $m = nq$.

Now $a^m = a^{nq}$

$= (a^n)^q$

$= e^q \quad (\because a^n = e)$

$= e$

$\therefore a^m = e$

→ G is an abelian group. If $a, b \in G$ such that $o(a) = m$, $o(b) = n$ and $(m, n) = 1$ then $o(ab) = mn$.

Proof: Given that G is an abelian group and $a, b \in G$ such that $o(a) = m$ & $o(b) = n$

Since $o(a) = m$;

i.e, m is the least +ve integer such that $a^m = e$.

and $o(b) = n$

i.e, n is the least +ve integer such that $a^n = e$

Also $a, b \in G \Rightarrow ab \in G$

Let $o(ab) = p$

Now $(ab)^{mn} = a^{mn} b^{mn} \quad (\because G \text{ is abelian})$

$= (a^m)^n (b^n)^m$

$= e^n e^m$

$= e$

$\therefore (ab)^{mn} = e$

$\Rightarrow o(ab) / mn$

i.e, p / mn —— (1)

Also $(ab)^{pn} = [(ab)^p]^n$

$= e^n$

$= e$

and $(ab)^{pn} = a^{pn} b^{pn}$

$= a^{pn}(b^n)^p$

$= a^{pn} \cdot e$

$= a^{pn}$

$\therefore a^{pn} = e \quad (\because (ab)^{pn} = e)$

$\Rightarrow o(a) / pn$

i.e, m / pn.

Since $(m, n) = 1$

$\Rightarrow m / p$. ——(2)

Similarly we can prove n/p ——(3)

from (2) & (3) and $(m, n) = 1$

we have mn / p ——(4)

$\therefore$ from (1) & (4)

we have $mn = p$

$\therefore o(ab) = p = mn$

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

→ Given $axa = b$ in G, find x.

Soln: we have $axa = b$

$\Rightarrow \bar{a}^1(axa) = \bar{a}^1 b$

$\Rightarrow (\bar{a}^1 a)(xa) = \bar{a}^1 b$

$\Rightarrow exa = \bar{a}^1 b$

$\Rightarrow xa\bar{a}^1 = \bar{a}^1 b\bar{a}^1$

$\Rightarrow xe = \bar{a}^1 b\bar{a}^1$

$\Rightarrow \boxed{x = \bar{a}^1 b\bar{a}^1}$

→ Find the solution of the equation $abxax = cbx$ in a group G, where $a, b, c \in G$

Soln: we have $abxax = cbx$

$\Rightarrow \bar{a}^1 abxax = \bar{a}^1 cbx$

$\Rightarrow bxax = a^{-1}cbx$

$\Rightarrow xax = b^{-1}a^{-1}cbx$

$\Rightarrow xa = b^{-1}a^{-1}cb$

$\Rightarrow x = b^{-1}a^{-1}cb\bar{a}^1$

→ If a and b are any elements of a group G, then $(bab^{-1})^n = ba^nb^{-1}$ for any integer 'n'.

Soln: (i) $n=0$

we have $(bab^{-1})^0 = e$ (by defn)

Also $ba^0b^{-1} = beb^{-1}$

$= bb^{-1}$

$= e$

$\therefore (bab^{-1})^0 = ba^0b^{-1}$

(ii) $n>0$.

we have $(bab^{-1})^1 = bab^{-1}$

$= ba^1b^{-1}$ $(\because a^1 = a)$

$\therefore$ The result is true for $n=1$

Let us suppose that the result is true for $n=k$

then $(bab^{-1})^k = ba^kb^{-1}$

Now $(bab^{-1})^{k+1} = (bab^{-1})^k (bab^{-1})$

$= (ba^kb^{-1})(bab^{-1})$

$= ba^kb^{-1}bab^{-1}$

$= ba^keab^{-1}$

$= ba^kab^{-1}$

$= ba^{k+1}b^{-1}$

$\therefore$ The result is true for $n=k+1$

$\therefore$ By the mathematical induction the result is true for $n>0$

(iii) $n<0$

Let $n=-m$ where $m>0$

then $(bab^{-1})^n = (bab^{-1})^{-m}$

$= [(bab^{-1})^m]^{-1}$

$= (ba^mb^{-1})^{-1}$

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

$= ba^{-m}b^{-1}$

$= ba^nb^{-1}$

→ prove that a group G is abelian if every element of G except the identity element is of order two.

Sol^n: W.K.T the order of an identity element 'e' is 1. i.e, $o(e) = 1$

and given that the order of every element of the group G is 2 except the identity element.

$\therefore o(a) = 2 \quad \forall a \in G \ \& \ a \neq e.$

$\Rightarrow a^2 = e$

Let $a, b \in G \Rightarrow ab \in G$

$\therefore (ab)^2 = e \ ; \ ab \neq e$

$\Rightarrow (ab)(ab) = e$

$\Rightarrow (ab)^{-1} = ab$

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

$\Rightarrow ba = ab \quad (\because a^2 = e \Rightarrow aa = e \Rightarrow a^{-1} = a)$

$\therefore$ G is abelian

→ If every element of a group G is its own inverse, then G is abelian.

Sol^n: Let a & b be two elements of the group G then $ab \in G$

Given that every element of G is its own inverse.

$\therefore a^{-1} = a, \ b^{-1} = b$ & $(ab)^{-1} = ab$

NOW we have

$(ab)^{-1} = ab$

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

$\Rightarrow ba = ab$

$\therefore$ G is abelian.

Note [1]. All groups of order 4 and less are commutative.

[2] If a group G is of order 4 and every element of G is its own inverse then it is known as Klein-4-group

→ If 'a' is an element of a group G such that $O(a) = n$ then the set $H = \{a^1, a^2, a^3, \ldots\ldots a^n = e\}$ forms a group w.r.t the composition in G.

Soln: Let $a \in G$ such that $O(a) = n$

$\Rightarrow a^n = e$

where n is the least +ve integer & e is the identity element in G.

(i) Let $a^p, a^q \in H$

$\Rightarrow a^p \cdot a^q = a^{p+q}$

$= a^r \in H$

when $p+q \equiv r \pmod n$ as $a^n = e$.

$\therefore$ Multiplication is closed in H.

(ii) Let $a^p, a^q, a^r \in H$

$\Rightarrow (a^p \cdot a^q)\, a^r = (a^{p+q})\, a^r$

$= a^{(p+q)+r}$

$= a^{p+(q+r)}$

$= a^p \cdot a^{q+r}$

$= a^p (a^q a^r)$

$\therefore x^n$ is asso. in H.

(iii) $\forall\, a \in H \;\exists\; a^n = e \in H$ such that $ae = ea = a$

$\therefore a^n = e = a^0$ is an identity element in H.

(iv) Let $a^p \in H$, $\exists\; a^{n-p} \in H$ such that

$a^p \cdot a^{n-p} = a^{n-p} a^p = a^n = e$.

$\therefore a^{n-p}$ is the inverse of a^p in H.

$\therefore$ every element of H is invertible.

$\therefore H = \{e = a^0, a^1, a^2, \ldots\ldots a^{n-1}\}$ is a group w.r.t composition in G

→ If G is a finite abelian group with elements $a_1, a_2, \ldots\ldots a_n$, P.T $a_1 \cdot a_2 \cdot a_3 \cdot \ldots\ldots a_{n-1} \cdot a_n$ is an element whose square is the identity.

Soln: we have $(a_1 \cdot a_2 \ldots\ldots a_n)^2 = (a_1 \cdot a_2 \ldots\ldots a_n)(a_1 \cdot a_2 \ldots\ldots a_n)$ ①

Now each element in the group is unique inverse.

$\therefore$ each of $a_1, a_2, \ldots a_n$ is the inverse of exactly one of them.

So associate each of $a_1, a_2, \ldots a_n$ with its inverse.

(1) $\Rightarrow (a_1 a_2 \ldots a_n)^2 = (a_1 a_1^{-1})(a_2 a_2^{-1}) \ldots (a_n a_n^{-1})$

$= ee \ldots$ upto n times

$= e$

$\rightarrow$ The equation $x^2 a x = \bar{a}^1$ is solvable for 'x' in a group G iff 'a' is the cube of some element in G.

Soln: Suppose $x^2 a x = \bar{a}^1$ is solvable for 'x' in G

Then $\exists\, c \in G$ such that $c^2 a c = \bar{a}^1$

Now $c^2 a c = \bar{a}^1$

$\Rightarrow ccac = \bar{a}^1$

$\Rightarrow c(ca)c = \bar{a}^1$

$\Rightarrow c(ca)ca = \bar{a}^1 a$

$\Rightarrow c(ca)(ca) = e$

$\Rightarrow (ca)(ca) = \bar{c}^1$

$\Rightarrow (ca)(ca)c = \bar{c}^1 c$

$\Rightarrow (ca)(ca)(ca) = a$

$\Rightarrow a = (ca)^3$

$\therefore$ a is the cube of some element ca in G.

conversely suppose that $a = b^3$ for some $b \in G$

Let $x = b^{-2}$ be the solution of the equation $x^2 a x = \bar{a}^1$.

for if $x = b^{-2}$ and $a = b^3$ then

$x^2 a x = (b^{-2})^2 b^3 b^{-2}$

$= b^{-4} b^3 b^{-2}$

$= b^{-3}$

$= (b^3)^{-1}$

$= a^{-1}$ $(\because b^3 = a)$

$\therefore x = b^{-2}$ is a solution of $x^2 a x = \bar{a}^1$.

→ If in a group G, $xy^2 = y^3x$ and $yx^2 = x^3y$ then $x = y = e$ where e is the identity element of G

Soln: we have $xy^2 = y^3x$

$\Rightarrow x(xy^2) = x(y^3x)$

$\Rightarrow x^2y^2 = xy^3x$

$\Rightarrow (x^2y^2)y^{-1} = xy^3xy^{-1}$

$\Rightarrow x^2y^2y^{-1} = xy^3xy^{-1}$

$\Rightarrow x^2y = xy^2yxy^{-1}$

$\Rightarrow x^2y = y^3xyxy^{-1}$ $(\because xy^2 = y^3x)$ ——— (1)

Again $yx^2 = x^3y$

$\Rightarrow yx^2 = x \cdot x^2y$

$= x(y^3xyxy^{-1})$ (by (1))

$\therefore yx^2 = xy^3xyxy^{-1}$

$\Rightarrow x^2 = y^{-1}xy^3xyxy^{-1}$

$\Rightarrow x^2y = y^{-1}xy^3xyx$ ——— (2)

from (1) & (2) we have

$y^3xyxy^{-1} = y^{-1}xy^3xyx$.

$\Rightarrow y^4xyxy^{-1} = xy^3xyx$

$\Rightarrow y^4xyx = xy^3xyxy$

$= xy^2 \cdot yxyxy$

$= y^3xyxyxy$ $(\because xy^2 = y^3x)$

$\Rightarrow yxyx = xy \cdot xy \cdot xy$ (∵ by cancelling y^3 from both sides)

$(yx)^2 = (xy)^3$ ——— (3)

Since the given relations $x^2y = y^3x$ & $y^2x = x^3y$ are symmetrical in x & y.

∴ Interchanging x & y in (3) we get $(xy)^2 = (yx)^3$ ——— (4)

from ③ & ④, we have

$$(xy)^2 = (yx)^3$$
$$= (yx)^2 (yx)$$
$$= (xy)^3 (yx)$$

$\therefore e = (xy)(yx)$ (∵ by cancelling $(xy)^2$ both sides)

$\Rightarrow e = xy^2x$

$\Rightarrow x^{-2} = y^2$ ——— ⑤

Now $xy^2 = y^3x$

$\Rightarrow x(x^{-2}) = y(x^{-2})x$

$\Rightarrow x^{-1} = yx^{-1}$

$\Rightarrow \boxed{e = y}$

Again $yx^2 = x^3y$

$ex^2 = x^3$

$\Rightarrow \boxed{e = x.}$

$\therefore x = y = e.$

→ Let G be a group and let $a \in G$ be of finite order 'n' (i.e, $O(a) = n$). Then for any integer k we have $O(a^k) = \frac{n}{(n,k)}$ where (n,k) denotes the H.C.F of n and k.

Soln: Let $(n,k) = m$ then we have

$n = pm$, $k = qm$ for some integers p and q.

such that $(p,q) = 1$

Let $O(a^k) = l$

then $(a^k)^l = e$ where l is the least +ve integer & e is the identity in G.

$\Rightarrow a^{kl} = e.$

$\Rightarrow O(a) / kl.$

$\Rightarrow n/kl \quad (\because o(a)=n)$

$\Rightarrow pm/qml$

$\Rightarrow p/ql \cdot \left(i.e, \frac{ql}{p}\right)$

$\Rightarrow p/l$ ——— (1) $(\because$ p and q are relatively prime).

Again $(a^k)^p = (a^{qm})^p$

$= a^{qmp}$

$= a^{qn}$

$= (a^n)^q$

$= e^q$

$= e$

$\therefore o(a^k)^p = e$

$\Rightarrow o(a^k)/p$

$\Rightarrow l/p$ ——— (2)

$\therefore$ From (1) & (2) we have

$l = p.$

$\Rightarrow o(a^k) = p$

$= \frac{n}{m} \quad (\because n = pm)$

$= \frac{n}{(n,k)}$