PG-TRB-MATHS

IMPORTANT

STUDY MATERIAL

UNIT-1

5/4/12.

UNIT-1

ALGEBRA (Queen of Mathematics)

Notations:-

* N - Set of all Natural numbers
* Z - Set of all integers
* W - Set of all whole numbers
* Z^+ - Set of all +ve integers.
* $Q = \{\pm p/q, q \neq 0\}$ - Set of all rational numbers.
* Q^+ - Set of all +ve rational number.
* Q^* - Set of all non-zero rational number $[Q - \{0\} = Q^*]$
* R - Set of all real numbers.
* R^+ - Set of all +ve real numbers.
* R^* - Set of all non-zero real numbers.
* C - Set of all Complex numbers
* C^* - Set of all non-zero Complex numbers.

Binary Operation:-

Let S be any non-empty set, a operation $*$ is said to be binary operation on S if

$$\forall a, b \in S \Rightarrow a * b \in S.$$

then '$*$' is said to be a binary operation on S.

Ex:

1. $+, *, -,$ are binary operation on R.
2. $+, *, -$ are binary operation on Z.
3. $\div$ is not an " " on Z.
4. $+$ is not an binary operation on R^*, C^*, Q^*.
5. $\div$ is a binary operation on R^*.

Group :-

Let G be a non-empty set and $*$ be a binary operation on G if

$\forall\ a, b, c \in G$.

(i) Closure :

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

(ii) Associative :-

$\forall\ a, b, c \in G \Rightarrow (a * b) * c = a * (b * c)$

(iii) Identity :-

$\exists$ an element $e \in G$ s.t $a * e = e * a = a$

$\Rightarrow e$ is an identity element of a.

iv) Inverse :-

Let $a \in G$ $\exists$ an element $\bar{a} \in G$ s.t $a * \bar{a} = \bar{a} * a = e$

$\Rightarrow \bar{a}$ is inverse element of a.

$\therefore G$ is a group under binary operation $*$.

(OR) $(G, *)$ is a group.

Ex:

1. $(\mathbb{Z}, +)$ is a group.
2. $(\mathbb{N}, +)$ is not a group.
3. $(\mathbb{R}, \cdot)$ is not a group.
4. $(\mathbb{N}, \cdot)$ is not a group.
5. $(\mathbb{R}, +)$ is a group.
6. $(\mathbb{R}^*, +)$, $(\mathbb{C}^*, +)$, $(\mathbb{Q}^*, +)$ is not a group.
7. $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, $(\mathbb{Q}^*, \cdot)$ is a group.
8. $(\mathbb{R}, \cdot)$ $(\mathbb{Q}, \cdot)$, $(\mathbb{C}, \cdot)$ is not a group.
9. $(\mathbb{Q}, +)$, $(\mathbb{Q}, +)$ is a group.
10. Set of even integers $(\mathbb{Z}_e, +)$ is a group. ✓
11. Set of odd integers $(\mathbb{Z}_o, +)$ is not a group. ✓

12. The set of all cube root of unity $G = \{1, \omega, \omega^2\}$ under multiplication is a group.

13. The set of all four root of unity $G = \{1, -1, i, -i\}$ und multiplication is a group.

14. The set of all n^{th} root of unity under x^{ion} is a group.
ie., $G = \{1, \omega, \omega^2 \ldots \omega^{n-1}\}$.

✓15. The set of all 2×2 real number matrix under addition is a group.
ie., $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in R \right\}$

✓16. The set of all 2×2 real number matrix under x^{ion} is not a group [except non-singular ie, $ad - bc \neq 0$]

✓17. $G = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \right\}$ form a group, under x^{ion}.

Problems:

① If $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in R \right\}$ form a group under addition, find identity and inverse element.

Soln

$$I = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$ is an identity element (matrix)

$$E = A^{-1} = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$$ is an inverse matrix.

② If $(Z, *)$ form a group, $*$ is defined by $a * b = a + b + 2$ find identity & Inverse element.

Soln:

$$a * b = a + b + 2$$

(i) WKT, $a * e = e * a = a$

$$a + e + 2 = a$$

$$e + 2 = 0$$

$$\boxed{e = -2}$$

(ii) $a^{-1} * a = a * a^{-1} = e$

$$\therefore a^{-1} + a + 2 = -2 \Rightarrow \boxed{a^{-1} = -(4 + a)}$$

(3) If $(Q, *)$ form a group, $*$ is defined by $a*b = a+b-ab$, find identity & inverse.

Soln:

(i) $a*e = e*a = a$

$a*e = a+e-ae = a$

$\Rightarrow e(1-a) = 0$

$\Rightarrow \boxed{e = 0}$

(ii) $a*a^{-1} = a^{-1}*a = e$

$a+a^{-1} - aa^{-1} = 0$

$a + a^{-1}(1-a) = 0$

$\boxed{a^{-1} = \frac{-a}{1-a}}, \quad a \neq 1$

(4) If $G = \left\{ \begin{pmatrix} x & x \\ x & x \end{pmatrix} / x \in R^* \right\}$ form a group under $\times$ then find identity and inverse.

Soln:

$$G = \left\{ \begin{pmatrix} x & x \\ x & x \end{pmatrix} / x \in R^* \right\}$$

(i) $\begin{pmatrix} x & x \\ x & x \end{pmatrix} \begin{pmatrix} e & e \\ e & e \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$

$\begin{pmatrix} 2xe & 2xe \\ 2xe & 2xe \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$

$2xe = x \Rightarrow 2e = 1$

$e = 1/2$

$\therefore E = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$ is an identity matrix.

(ii) $\begin{pmatrix} x & x \\ x & x \end{pmatrix} \begin{pmatrix} y & y \\ y & y \end{pmatrix} = \begin{pmatrix} e & e \\ e & e \end{pmatrix}$

$\begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix} = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$

$2xy = 1/2 \Rightarrow y = \frac{1}{4x}$ $\therefore A^{-1} = \begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix}$ is inverse matrix.

(5) If $G = \{f_1, f_2, f_3, f_4\}$ form a group under Composite function where $f_1(x) = x$, $f_2(x) = -x$, $f_3(x) = 1/x$, $f_4(x) = -1/x$

Soln:

(i) $f(x) = x \Rightarrow f_1$ is an identity function.

ie., $f_1(x) = x$

(ii) $f_1 \circ f_2(x) = f_1(-x) = -x = -f_1(x)$ f_1 is inverse of f_1

$f_1 \circ f_3(x) = f_1(1/x) = 1/x = f_3(x)$ f_2 is inverse fun of f_2

f_3 is inverse function of f_3

f_4 " " of f_4

$\therefore f_3$ is an inverse function.

Commutative Group (or) Abelian group:-

A group satisfies Commutative property then the group is called an Abelian group.

ie., G is Commutative iff $\forall a, b \in G \Rightarrow a * b = b * a$.

Ex:

① $(\mathbb{Z}, +)$ is an infinite abelian group.

② The set of 2x2 matrix $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right\}$ Commutative not satisfi in matrix multiplication

Semi-group:-

A non-empty set G is a semigroup under binary operation if it satisfies closure & Associative property.

* Every group is a semi-group $\Rightarrow$ Converse is not true.

Ex: 1. $(N, +)$ is a semi-group but not a group.

2. $(\mathbb{Z}, \cdot)$ " " "

Monoid:-

A Semi-group satisfies a identity element is called a monoid.

Ex: i) $(\mathbb{Z}, \cdot)$ is monoid

ii) $(\mathbb{Z}, +)$ is monoid ; iii) $(N, +)$ is not monoid.

Order of a group:-

The number of distinct elements of a group G is called a Order of a group.

⇒ It is denoted by $o(G)$. finite group ⇒ order group

Ex: 1. $G = \{1, 2, 3, 4\}$ then $o(G) = 4$

2. $(Z, +)$ is a group but $o(G)$ = infinite.

Residue classes:-

Residue class of mod n is set of all Congruence value from 0 to n-1.

ie., Res of (mod n) = $\{[0], [1] \ldots\ldots [n-1]\}$

* Z_n - Set of all Congruence class under mod n.

ie, $Z_n = \{[0], [1] \ldots [n-1]\}$

* Z_n is form an abelian group under addition modulo n.

* $[a] +_n [b] = \begin{cases} a+b < n \Rightarrow [a+b] \\ a+b \geq n \Rightarrow [r] \end{cases}$, $0 \leq r < n$

$[a] \cdot_n [b] = \begin{cases} [ab] & , ab < n \\ [r] & , ab \geq n \end{cases}$ $0 \leq r < n$.

Order of a element:-

Let G be a group and $a \in G$, $\exists$ an least +ve integer n' $\ni$ $a^n = e$ then n' is called $o(a)$.

ie., $o(a) = n$.

Ex: ① $G = \{1, \omega, \omega^2\}$ form a gp under $\times^{ion}$, find $o(\omega)$

$\omega \in G \Rightarrow \omega^3 = 1$ $(a^n = e)$

$\therefore$ $\boxed{o(\omega) = 3}$ ($\because$ 1 is an identity)

7) (A) Find the solution of equation $ax = b$, in S_3 where S_3 = set of all permutations

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Soln:

$$ax = b \quad ; \quad S_3 = (a, b)$$

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

$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 3 & 2 & 1 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 3 & 2 & 1 \\ 1 & 3 & 2 \end{pmatrix}$$

$$x = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ or } (1\ 2\ 3)$$

5. Every element of a group G is of order 2, then G is abelian.

6. If every element in G which has own inverse then G is abelian.

7. Inverse of identity element is itself.

8. If G is a group and $a, b \in G$, $(a*b)^2 = a^2 * b^2$ then G is abelian.

9. If G is abelian then $(a*b)^n = a^n * b^n$ $\forall$ integer n.

10. If $o(G) = 2n$, where $n > 3$, then G is non-abelian.

Ex: $o(G) = 8 = 2 \times 4 \quad (4 > 3)$

$\therefore G$ is non-abelian.

$o(G) \leq 6$, G is abelian.

11. If G is a group and $o(a) = n$ $\exists$ an $m \ni a^m = e$ then $n \mid m$.

12. Every group of order 4 is abelian.

13. Group of order ≤ 6, then the group is abelian.

ie, $o(G) \leq 6$, G is abelian.

Idempotent element:-

Let G be a group and $a \in G$ if $a^2 = a$ then a is called idempotent element.

In every group, idempotent element is identity element.

Periodic group (or) Torsion Group:-

A group is said to be periodic group if every element of a group is finite order.

Ex: 1. $G = \{1, -1, i, -i\}$

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

Subgroup:-

Let G be a group and H is a subset of G, if H form a group under binary operation of G then H is said to be subgroup of G.

Ex:

1. Let $(z, +)$ be a group.

   And $2e = \{0, \pm 2, \pm 4 \ldots\} \subset z$

   $\Rightarrow (2e, +)$ is a group

   $\therefore (2e, +)$ is a subgroup of $(z, +)$

   (set of all even integers)

2. $I \subset z$. But $(I, +)$ is not a group.

   $\therefore$ A subset $(I \subset z)$ is not a subgroup of $(z, +)$.

3. (Set of all integer)^z is a subgroup under addition of set of all real numbers under addition.

4. $H = \{1, -1\}$ is a subgroup of $G = \{1, -1, i, -i\}$ under

Theorem:-

1. A non-empty subset H of a group G is subgroup of G iff $\forall\ a, b \in H \Rightarrow ab \in H$.

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

2. A non-empty subset H of a group G is subgroup of G iff $\forall a, b \in H \Rightarrow ab^{-1} \in H$.

3. The identity element of a group & subgroup are same.

4. If G is finite and H is finite, $a \in H \Rightarrow a^{-1} \in H$ then H is a subgroup of G.

5. Union of two subgroups is need not be a subgroup.
ie, If H & K are two subgroups then HUK is not a subgroup.

Ex: $H = 2Z = \{0, \pm 2, \pm 4 \ldots\}$

$K = 3Z = \{0, \pm 3, \pm 6 \ldots\}$

$HUK = \{0, \pm 2, \pm 3, \pm 4, \pm 6 \ldots\}$ is not a group.

$\because 2, 3 \in HUK \Rightarrow 2+3=5 \notin HUK$ is not a subgroup.

6. The Union of two subgroup is a subgroup if $H \subseteq K$ & $K \subseteq H$ (contained in each other)

Ex: $H = 2Z = \{0, \pm 2, \pm 4 \ldots\}$

$K = 4Z = \{0, \pm 4, \pm 8 \ldots\}$ $(\because H \subset K)$

$\therefore HUK = \{0, \pm 2, \pm 4 \ldots\}$ is a subgroup.

7. Intersection of two subgroups is also a subgroup.

8. If H and K are two subgroups of G then the product HK is subgroup of G iff $HK = KH$.

9. If H and K are finite subgroup of G, and $G = HK$ then $o(G) = \boxed{o(HK) = \frac{o(H)\,o(K)}{o(H \cap K)}}$

If $o(H \cap K) = \{e\}$ then $o(H \cap K) = 1$

$\Rightarrow o(HK) = o(H) \cdot o(K)$

(10.) If $o(H)$ and $o(K)$ are relatively prime. Then $o(HnK) = 1$

ie., $\gcd(o(H), o(K)) = 1$ then $o(HnK) = 1$.

Also $o(HnK) = \gcd\{o(H), o(K)\}$

(1.) Let H and K are 2 subgroups of G of order 2 and 9. respectively find $o(G)$.

Soln:

$o(H) = 2,\ o(K) = 9$

$o(G) = o(HK) = \dfrac{o(H)\,o(K)}{o(HnK)}$ $\quad \left| \because o(HnK) = \gcd\{2, 9\} = 1 \right.$

$\Rightarrow o(G) = o(H)\,o(K)$

$= 2 \times 9$

$\Rightarrow \boxed{o(G) = 18}$

(2.) If the order of H and K are 5, 10 respectively, find o

Soln:

Given, $o(H) = 5,\ o(K) = 10$

$o(G) = o(HK) = \dfrac{o(H)\,(o(K)}{o(HnK)}$ $\quad \left| o(HnK) = \gcd\{5, 10\} = 5 \right.$

$= \dfrac{5 \times 10}{5}$

$\boxed{o(G) = 10}$

Centre of a Group :-

Let G be a group, the set $z(G) = \{\}$

Said to be centre of a group G defined by,

$$z(G) = \{x \mid xa = ax \ \forall\, a \in G\}$$

* Centre of G. ie., $z(G)$ is a subgroup of G.

Proper Subgroup

A subgroup of G is said to be proper if $o(H) \mid o(G)$ properly.

Improper Subgroup:-

Let G be a group and subgroup singleton set $\{e\}$ and G itself are called improper subgroup other subgroups are proper subgroup.

Cyclic group:-

A group which is generated by an element $a \in G$ then G is called cyclic group.

ie, $G = \{a^n / n \in I\}$

$G = \langle a \rangle$

Ex: $G = \{1, -1, i, -i\}$ is cyclic.

Here 'i', '-i' are the generated elements.

* A cyclic group have several generators.
* If 'a' is a generator of a cyclic group G then its inverse 'a^{-1}' also a generator of G.

Monogenic Cyclic group:-

A cyclic group has only one generator is called Monogenic cyclic group.

Ex: $G = \{1, -1\}$,

'-1' is only one generator of G.

* Order of a cyclic group is same as order of its generator.

① If $G = \{1, \omega, \omega^2\}$ is a cyclic group, find its generators.

Soln:

ω, ω^2 are the 2 generators of G.

$\therefore \omega^1 = \omega \qquad (\omega^2)^1 = \omega^2$

$\omega^2 = \omega^2 \qquad (\omega^2)^2 = \omega$

$\omega^3 = 1 \qquad (\omega^2)^3 = \omega^6 = 1 \qquad O(\omega) = O(\omega^2) = 3$

(2) The set of all integer is a cyclic group under addition find its generated elements.

Soln:

$Z = \{0, \pm 1, \pm 2 \cdots\}$

generators $-1, 1$.

(3) $G = \{0, 1, 2, 3\}$ is a cyclic group under addition modul 4, Find its generators.

Soln:

Given $G = \{0, 1, 2, 3\}$ $\Rightarrow$ 1, 3 are the generators

$(1)^4 = 1 +_4 1 +_4 1 +_4 1 = 0$ $\quad (3)^1 = 3$

$(1)^3 = 1 +_4 1 +_4 1 = 3$ $\quad (3)^2 = 3 +_4 3 = 2$

$(1)^2 = 1 +_4 1 = 2$ $\quad (3)^3 = 3 +_4 3 +_4 3 = 1$

$(1)^1 = 1 = 1$ $\quad (3)^4 = 3 +_4 3 +_4 3 +_4 3 = 0$

(4) If $O(G) = p^2$, p is prime then G is ~~abelian~~ cyclic.

$O(G) = p \Rightarrow$ Cyclic

Ex:

$O(G) = 49 = 7^2$, 7 - prime $\Rightarrow G$ is cyclic.

* $O(G) = pq$, where p, q are distinct prime number $q > p$ then G is cyclic. (Thm: P cyclic)

Ex:

$O(G) = 15 = 3 \times 5$ $\quad (\because 5 > 3$

$\therefore G$ is cyclic.

* If $O(G) = pq$, $p > q$ if

i) $q \nmid p-1 \Rightarrow G$ is cyclic.

ii) $q \mid p-1 \Rightarrow G$ is non-abelian.

(OR)

If $O(G) = pq$, $p > q$ if

i) $p \nmid q-1 \Rightarrow G$ is cyclic

ii) $p \mid q-1 \Rightarrow G$ is non-abelian.

If $O(G) = 21 = 3 \times 7$ $\quad q > p$

(1) $7 \not\equiv 3-1 \Rightarrow G$ is cyclic.

(*) * If every group of order 4 is ~~cyclic but~~ abelian but not cyclic.

Ex: Keli's group $G = \{e, a, b, c\}$ is abelian but not cyclic.

* Every cyclic group is abelian Converse is not true.
* If G is cyclic and H is subgroup of G then H is cyclic.

ie, Every subgroup of cyclic group is cyclic.

∴ Every subgroup of cyclic group is abelian.

(I.M)* A cyclic group of order n then it has atleast $d(n)$ subgroups, where $d(n)$ = no. of divisors of n.

Ex:

(i) $O(G) = 10$

No. of subgroups $= d(10) = 4$

No. of divisors of $n = d(n) = (a+1)(b+1)(c+1)\ldots\ldots$

where $n = p^a q^b r^c \ldots\ldots$

(ii) Let G be a cyclic group of order 30 then find the number of subgroups of G.

Soln:

$O(G) = 30$

$= 2^1 \times 3^1 \times 5^1$

$d(30) = (1+1)(1+1)(1+1)$

$d(30) = 8$

∴ Number of subgroups $= 8$.

(iii) G is a cyclic group of order 100, find the no. of subgroups of G.

Soln: $o(G) = 100$

$= 25 \times 4$

$= 5^2 \times 2^2$

$d(n) = (2+1)(2+1) = 9$

∴ Number of subgroups = 9.

V. Imp* G be a finite cyclic group generated by 'a' is of order 'n' then G has $\phi(n)$ generated elements.

where $\phi(n)$ - no. of integer $< n$ & relatively prime to

$$\phi(n) = n\left(1-\tfrac{1}{p}\right)\left(1-\tfrac{1}{q}\right)\left(1-\tfrac{1}{r}\right)\cdots$$

* If p is prime then no. of generators is $\phi(p) = p-1$

Ex:

① Find the no. of generators of a cyclic group of order

Soln:

$o(G) = 15$ i.e., $n = 15$

$\phi(15) = 15\left(1-\tfrac{1}{3}\right)\left(1-\tfrac{1}{5}\right)$

$= 15\left(\tfrac{2}{3}\right)\left(\tfrac{4}{5}\right)$

$= 8$

∴ G has 8 generators.

(ii) If $G = \{a, a^2, a^3, \ldots, a^{15}\}$ Find no. of generators.

Soln:

$n = 15$, $o(G) = 15$

$\phi(15) = 8$

∴ G has 8 generators.

Also generated elements, $a, a^2, a^4, a^7, a^8, a^{11}, a^{13}, a^{14}$

(relatively prime to 15)

* Every Group of prime order is cyclic.

ie, $O(G) = p$, then G is cyclic.

* An infinitely cyclic groups has exactly two generators namely 'a' and 'a^{-1}'.

* A cyclic group has only one generator it has atmost two elements.

Coset of a subgroup:-

Let G be a group and H be a subgroup of G then the set,

$Ha = \{ha / h \in H, a \in G\}$ is called right coset of H in G.

Also, $aH = \{ah / h \in H, a \in G\}$ is called left Coset of H in G.

Ex:

$$G = \{0, \pm 1, \pm 2 \ldots\} = (\mathbb{Z}, +)$$

$$H = 2\mathbb{Z} = \{0, \pm 2, \pm 4 \ldots\}$$

$\because a = 1 \in G \Rightarrow H+1 = \{\pm 1, \pm 3, \pm 5 \ldots\}$ is in G.

Properties of Coset:-

* The Union of Cosets is a group.

ie, $G = \cup aH$ or $\cup Ha$

* If $a \in H$, the Coset $Ha = H$ (subgroup).

* Any two right or left Cosets have same no. of elements.

* Any two Cosets have distinct elements.

* The number of right Cosets of H = The no of left cosets.

Lagrange's theorem:-

Let G be a finite group and H be a subgroup of G, then order of H divides order of G. ie, $O(H) / O(G)$.

* Let G be a group and H, K are the subgroup of G and $K \subset H$ then $I_G(K)$ (index of K of G) is index of product of index of H of G and index of K of H.

ie., $$I_G(K) = I_G(H) \cdot I_H(K)$$

$$\Rightarrow \frac{o(G)}{o(K)} = \frac{o(G)}{o(H)} \cdot \frac{o(H)}{o(K)}$$

$$\Rightarrow (G:K) = (G:H) \cdot (H:K)$$

* Let G be a cyclic group of prime order then G has no proper subgroup (has only improper subgroup).

ie, improper subgroups are $\{e\}$ and G itself.

Simple group:-

A group has no proper subgroup then is called simple group.

Ex:

* If $o(G) = 23\ (=p)$ then G is simple,
* Every group of prime order is simple.
* Simple $\Rightarrow$ cyclic $\Rightarrow$ abelian.
* A group has only improper subgroups then the group is simple group.

Euler's theorem:-

If n is positive integer and 'a' is relatively prime to 'n' then,

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

where $\phi(n)$ - the number of integers $< n$ and relatively to 'n'.

Ex:

(1) find the remainder when 7^{50} is divisible by 12

Soln

$$a=7, \quad n=12, \quad \phi(12)=4$$

$$(7^4)^{12} \equiv 1^{12} \pmod{12}$$

$$7^{48} \equiv 1 \pmod{12}$$

$$7^{48}\,7^2 \equiv 7^2 \pmod{12}$$

$$7^{50} \equiv 1 \pmod{12}$$

Fermat's Theorem:-

If p is prime number and 'a' is any integer then,

$$a^{p-1} \equiv 1 \pmod{p} \quad (\text{or}) \quad a^p \equiv a \pmod{p}$$

Ex:

(1) Find If 3^{100} is divisible by 13, find the remainder.

Soln

$$a^{p-1} \equiv 1 \pmod{p} \quad \Big| \begin{array}{l} a=3 \\ p=13 \end{array}$$

$$3^{12} \equiv 1 \pmod{13}$$

$$3^{96} \equiv 1 \pmod{13}$$

$$3^{96} \cdot 3^4 \equiv 3^4 \pmod{13}$$

$$3^{100} \equiv 81 \pmod{13}$$

$$3^{100} \equiv 3 \pmod{13}$$

$\therefore$ Remainder is 3.

Normal Subgroup:-

Let G be a group and N be a subgroup of G if $\exists\ g \in G$ and $n \in N \Rightarrow gng^{-1} \in N$, then N is called a Normal Subgroup of G.

Ex: $G = \{1, -1, i, -i\}$, $H = \{1, -1\}$

$g = i$, $g^{-1} = -i$ $\quad gng^{-1} = i(-1)(-i) = -1 \in H$

(2) * If N is normal iff $\underline{gNg^{-1} = N}$ $\forall g \in G$.

Ex

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

$g = i$, $g^{-1} = -i$

$gNg^{-1} = \{i(1)(-i), i(-1)(-i)\}$

$= \{1, -1\} = N$

III by as $g = -1$, $g = 1$, $g = -i$.

Properties of Normal subgroup:-

* Every subgroup of an abelian group is Normal.
* Every subgroup of cyclic group is Normal.
* Centre of G ie, $z(G)$ is normal.
* If N is normal subgroup iff left cosets of N is equal to right cosets of N.

  ie, N is normal $\Leftrightarrow$ $aN = Na$.
* If N is a subgroup of index two then N is Normal.
* The intersection of two Normal subgroup is Normal.
* If N_1 & N_2 are Normal subgroup of G. Then their product $N_1 N_2$ is also normal.
* If N is normal iff product of any two right cosets again a right coset of N.

  ie, $Na \cdot Nb = Nab$ $\Leftrightarrow$ N is normal.

* Theorem:

If K is normal and H is any subgroup of G then $\underline{KH}$ is subgroup of G.