4th Sem Maths

1st unit Groups & cyclic groups

Most important Questions for pass Aspirants of this chapter

(1) Fundamental theorem of cyclic groups

(1) State and prove Two step Subgroup Test and ST $H=\{x \in G / x^r=e\}$ is Subgroup of G when G is abelian

(2) State and prove finite Subgroup Test

(3) Define Centre of group G ST Centre $Z(G)$ is Subgroup of G.

(4) ST every Subgroup of cyclic group is cyclic.

(5) State and prove fundamental theorem of cyclic groups

(6) G is a group and $a \in G$ then
$a^i=a^j$ if and only if
(i) a has infinite order then
$a^i=a^j$ if and only if $i=j$
(ii) If a has finite order then
$a^i=a^j$ if and only if n divides $i-j$

(7) State & prove 2 step Subgroup Test

Remaining Imp Q's of chapter

(1) prove the following,

(i) Intersection of subgroups is again a subgroup.

(ii) Identity element is unique in groups

(iii) Inverse uniqueness " " "

(iv) Socks-shoes property i.e $(ab)^{-1} = b^{-1}a^{-1}$

(v) Cancellation laws

(vi) H and K are 2 subgroups of G $\Rightarrow$ ST $HK = \{hk \mid h \in H, k \in K\}$ is subgroup of G or product of 2 subgroups is again a SG

(vii) every subgroup of cyclic group is abelian

(2) a and b are 2 elements a abelian group G if n is any integer $\Rightarrow$ ST $(ab)^n = a^n b^n$ and $(ab)^{-1} = a^{-1}b^{-1}$

is it true for non abelian group?

(3) prove that $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is group under matrix multiplication

(4) If $*$ defined on Q^+ by $a * b = \frac{ab}{2}$ $\Rightarrow$ ST $(Q^+, *)$ is a group

(5) S is set of real number except -1 define $*$ on S by $a * b = a + b + ab$ $\Rightarrow$ ST $(S, *)$ is abelian group

(6) a be an element of order n in group $\Rightarrow$ PT $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ & $|a^k| = \frac{n}{\gcd(n,k)}$ (k is the number)

Date __/__/__
Page
MY BEST BOOK

① Binary operations

group G is a set * is a operation
and for any 2 elements a, b ∈ G a*b ∈ G

operation → (×, ∘, +) denoted by symbols.

Groups

A non empty set ⟨G, *⟩ said to be group under * binary operation (*) if it satisfies following properties

- Closure property: ∀ a, b ∈ G. ∃ [a*b ∈ G]
- Inverse: a, a' ∈ G that [a*a' = a'*a = e]
- Identity: e ∈ G ∀ a ∈ G [a*e = e*a = a]
- Associativity: [(a*b)*c = a*(b*c) ∀ a, b, c ∈ G]

Properties of Groups

- Uniqueness of Identity & Inverse
  - → In G ∃ only one Identity element
  - → for every element its inverse is unique
- Cancellation laws
  - a, b, c ∈ G
  - ba = ca
  - [b = c] (Right Cancellation law)
  - [ab = ac]
  - [b = c] (left Cancellation)
- Socks-shoes property
  - a, b ∈ G
  - $(ab)^{-1} = b^{-1}a^{-1}$

Types of Groups

Abelian Group
$(G, *)$ is group
$a, b \in G$
$a * b = b * a$
is abelian

Finite Group
Group with finite number of elements

Sub Group (SG)
G is a group
H is subset of G and H → group under same operation of G
H is subgroup ($H \leq G$)

Cyclic Group (CG)
G is a group
$a \in G$ group G written using a
i.e $G = \{a^n : n \in Z\}$
→ a is generator of G

→ order of Group :- Number of elements of G ⇒ denoted by $|G|$

→ order of element :- $|a| = n$ if $a^n = e$
n is smallest +ve integer of $a^n = e$

→ Center of group :- The set of $a \in G$, where $ax = xa$ $\forall x \in G$
denoted by $Z(G)$

properties
$|a| = |\langle a \rangle|$
→ SG of CG is cyclic

1. Binary Operations

(i) A binary operation $(*)$ on any set 'G' is a mapping $* : G \times G \to G$ is the Cartesian product of G i

itself. It is as denoted by $0, ., \oplus$ etc.

(ii) $+, -, *$ are the binary operations on integers.

(iii) Division is not a binary operation.

2. Groups

A group $< G, * >$ can be defined as non empty a set 'G' which is closed under a binary operation $(*)$, su

that, at it satisfies the following properties.

(i) Associativity

$(a * b) * c - a * (b * c), \forall\ a, b, c \in G.$

(ii) Identity

There exists an element 'e' in the set 'G', such that, $e * a = a * e = a\ \forall\ a \in G$. Where e is the identity in G.

(iii) Inverse

There exists an element a' in G for each $a \in G$ such that $a * a' = a' * a = e$.

Where a' is the inverse of a.

3. Elementary Properties of Groups

(i) Uniqueness of the Identity

It states that "In a group G, there exists only one identity element".

(ii) Cancellation Laws

Let, $a, b\ c$ be the elements of a group G.

$ba = ca \Rightarrow b = c$ (Right cancellation law)

$ab = ac \Rightarrow b = c$ (Left cancellation law).

(iii) Uniqueness of Inverse

It states that "For each element a in a group G, there is a unique element b in G such that $ab = ba = e$".

(iv) Socks-Shoes Property

If a, b are the elements of a group G, then
$(ab)^{-1} = b^{-1}a^{-1}$.

4. Abelian Group

A group $(G, *)$ is said to be an abelian if it satisfies commutative property.

i.e., $a * b = b * a, \forall\ a, b \in G$.

5. Order of a Group

The order of a group is the number of elements of a group G. It is denoted as $| G |$.

6. Order of an Element of a Group

The order of an element of a group G is the smallest positive integer 'n' such that $a^n = e$.

It is denoted by $|a| = n$

7. Center of a Group

The set of all $a \in G$ that commute with every element of G is called center of a group G. It is denoted by

Example:- $G = \{\ldots -4, -2, 0, 2, 4, 8, \ldots\}$
Set of even Integers
$(G, +)$ is group under addition

G

Closure
$-4, 2 \in G$
$-4+2 = -2 \in G$

Identity
$0 \in G$
$-2+0 = -2$
$-4+0 = -4$

Inverse
$-2, 2 \Rightarrow$
$-2+2 = 0$
$-4, 4 \Rightarrow$
$-4+4 = 0$

Associativity

$-2, 4, 6$
$-2+(4+6) = (-2+4)+6$
$-2+10 = 2+6$
$8 = 8$

G group

properties ① unique Identity '0' exists
② for every element inverse exists in a way their operation results in identity

Cancellation:- $-2, 4, 6$
$(-2)(4) = (-2)(+4) \Rightarrow -2 = -2$

Shoe socks:-
$(4 \cdot 6)^{-1} = 24^{-1} = \frac{1}{24}$
$4^{-1} \cdot 6^{-1} = \frac{1}{4} \cdot \frac{1}{6} = \frac{1}{24}$
So $(ab)^{-1} = a^{-1} b^{-1}$

Subgroup of $G = \{\ldots -2, 0, 2, 4, 6 \ldots\}$
$(G, +)$

$\Rightarrow$

$+1 = \{0, 2, 4, 6\}$

$2+2 = 4$.
$2+4 = 6$ ... is subgroup
$(-2)+2 = 0$

$G = \{-4, -2, 0, 2, 4, 6, \ldots\}$

$2+(-2) = 0$
$2+2 = 4$
$2+0 = 2$
$2+2+2 = 6$
$2+2+2+2 = 8$
$2+(-2)+(-2) = -2$
$2+(-2)+(-2)+(2)+-2 = -8$

$\langle 2 \rangle$ is generators

$G = [2+(2n) : n \in Z]$

(1) State and prove 2 step Subgroup Test

(or)

prove → [A non-empty subset of H of a Group G is subgroup of G if and only if
(i) $\forall a,b \in H \Rightarrow ab \in H$
(ii) $\forall a \in H \Rightarrow a^{-1} \in H$]

statement.లో [ ] బ్రాకెట్ లో

proof:- let $G(G,*)$ is group under binary ($*$) operation and let H be a (nonempty) subset of G.

Necessary Condition :-

let H is a Subgroup of G.

then by the definition Subgroup $(H,*)$ is group and $H \leq G$.
then H is called as Subgroup of G.

→ so H should be a group itself

If H is a group.
then it satisfies closure, Identity Inverse and Associative properties

If $a, b \in H$
$ab \in H$ since H is group so by
↳ closure property — (1)

The group H has Identity element such that $a, e \in H$
$a * e = e * a = a \in H$

By Inverse law $\exists\ a^{-1} \in H$. — (2)
$aa^{-1} = a^{-1}a = e$.

Hence from (1) and (2)
$a, b \in H \Rightarrow ab \in H$
$\forall a \in H \quad a^{-1} \in H$ if H
H is subgroup of G.

Sufficient condition

if $a, b \in H$ and $ab \in H$
also $\forall a \in H \quad a^{-1} \in H$

⇒ (i) closure property i.e for $a, b \in H$
$a * b \in H$

(ii) Associative law :- $a, b, c \in H$
$\Rightarrow (a * b) * c = a * (b * c)$

If $a \in H$ and $a^{-1} \in H$

$aa^{-1} \in H$

$e \in H$

Identity element in G e exists

$a \cdot e = e \cdot a = a \in H$

Inverse law :- $a \in H$ and $e \in H$

from $a^{-1} \in H$ & $a \in H$

$aa^{-1} \in H \Rightarrow aa^{-1} \in H$ by closure

and $\circ$ we have identity element

$aa^{-1} = a^{-1}a = e$

$\therefore$ $(H, *)$ satisfies ~~addition~~

closure, Associative, Inverse and Indentity properties

Hence we can say when $a^{-1} \in H$ and $ab \in H$

H is a subgroup.

2 Step Subgroup test Imp Question

ST $H = \{x \in G : x^2 = e\}$ is a subgroup of G if G is abelian.

Given that G is is abelian

$\Rightarrow$ if $a, b \in G$ $a * b = b * a$

and also given $H = \{x \in G / x^2 = e\}$

let if $e \in G \Rightarrow e^2 = e$

$\Rightarrow e \in G$.

H is non-empty.

Let $a, b \in H$

$a^2 = e$ and $b^2 = e$ from $x^2 = e$

consider

$ab^{-1} \Rightarrow (ab^{-1})^2$ from x^2

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

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

$(ab)^{-1} = e \cdot e^{-1} = e$

Hint

H

↓

SG

↓

inverse & closure

Date __/__/__
Page
MY BEST BOOK

So here $(ab^{-1})^2 = e$

it means according to $x^2 = e$ if $x \in H$

we can say. $ab^{-1} \in H$

Hence H is Subgroup of G.

కొన్ని theorem statement మరియు proof మాత్రమే ఇవ్వడం జరిగింది.

Date ___/___/___
Page _____
MY BEST BOOK

(a) State and prove Finite Subgroup Test

Statement: If H is a non empty finite subgroup test subset of a group G if H is closed under the operation of G $\Rightarrow$ pT H is subgroup of G.

proof :- Given H is non empty finite subset of a group G

→ and also given H is closed under operation * G

$a, b \in H$

$ab \in H$ (closed)

Case (i) $a = e$

$a.a = e$

$a^{-1} = a \in H$

$\therefore$ H Subgroup of H

case (ii) $a \neq e$

$a, a^2, a^3, \ldots \ldots \in H$

H is finite

$a^i = a^j \quad i > j$

$a^{i-j} = a^{j-j}$

$a^{i-j} = e \quad [i-j > 1]$

$a\,a^{i-j-1} = a^{i-j}$

$a^{i-j-1} = a^{-1}$

i

Hint

H Sub group

$H \leq G$

→ closure

→ Identity

→ Inverse

→ Associativity

$aa^{-1} = e$

$ae = ea = a$

$a = e$

$a = e \quad a \neq e$

$a^{i-j-1} = a^{-1}$

$i-j-1 \geq 1 \quad [i-j \geq 1]$

$a^{-1} = a^{i-j-1}$

$a^{-1} \in H$ for any $a \in H$

$\therefore H$ is Sgroup

State and prove that Center of a group is a subgroup of that group

Statement :- If G is a group ⇒ Center of G. i.e Z(G) is a subgroup of G

Center of group G :-

Let a be an element of a group G the Centre of G is set of all $a \in G$ That commute with every element of G i.e denoted by Z(G)

if $a \in G$

$Z(G) = \{ ax = xa \text{ if } x \in G \}$

RTP :-

Center Z(G) is subgroup of G

Let Z(G) be Center of group G

Let $a, b \in Z(G) \Rightarrow$

Z(G) is said to be a subgroup if

(2 step SG Test ద్వారా)

$a \in Z(G) \Rightarrow a^{-1} \in Z(G)$ $ab \in Z(G)$

(i) The Center of group,

$$Z(G) = \{a \in G : ax = xa \ \forall x \in G\}$$

Consider $x \in G$, $a \in Z(G)$

$$ax = xa$$

$$a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1} \qquad [aa^{-1} = e]$$

$$(a^{-1}a) \cdot xa^{-1} = (a^{-1}x)(aa^{-1})$$

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

$$a^{-1} \in Z(G)$$

(in form $a \in G$, $ax = xa$, here $x = a^{-1}$)

(ii) $(ab)x = (a(bx))$

$= a(xb)$

$= (ax)b$

$(ab)x = xab$

$(ab)x = x(a,b)$ ← $[ax = xa$ at $a \in Z(G)]$

[if $bx = xb$]

$\Rightarrow ab \in Z(G)$

$a, b \in Z(G)$

from (i) & (ii)

$a \in (Z(G)) \Rightarrow a^{-1} \in Z(G)$

$a, b \in Z(G) \Rightarrow ab \in Z(G)$

So by 2-step SG Test

we can set that

$Z(G)$ is a Subgroup of G.

Here Center of a group is its Subgroup.

Cyclic Groups

Date / /
Page
MY BEST BOOK

(4) State and prove fundamental theorem of cyclic groups.

(or)

(Statement మాత్రమే చాలు)

Statement:- fundamental theorem of cyclic groups states that

(i) Every subgroup of a cyclic group is cyclic

(ii) If $|\langle a \rangle| = n$ then the order of any subgroup of $\langle a \rangle$ is divisor of n.

(iii) for each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k namely $\langle a^{n/k} \rangle$

Cyclic Group:-

A group G is cyclic if there exists an element $a \in G$ such that

$G = \{a^n / n \in Z\}$ => 'a' is generator of G

$\Rightarrow G = \langle a \rangle = \{a^n / n \in Z\}$ is cyclic group

(5) **Proof**

(i) let G be cyclic group Generated by 'a'

$\Rightarrow G = \langle a \rangle$

(ఇక్కడ మొదట (i) point every SG of CG is a cyclic దీన్ని chance ఇవ్వండి).

Prove that every subgroup of a cyclic group is cyclic.

Answer :

Cyclic Group

A group 'G' is cyclic if there exists an element $a \in G$ such that $G = \{a^n | n \in Z\}$, where 'a' is a generator of G. i.e., $G = \langle a \rangle = \{a^n | n \in Z\}$ is a cyclic group.

Proof

Let, 'G' be the cyclic group generated by 'a'.

$\Rightarrow \quad G = \langle a \rangle$ to prove SG is cyclic

let, → 'H' be a subgroup of 'G'

Every element of H is also an element of G

$\Rightarrow \quad a^n \in H$ for some $n \in Z^+$

Let q be the smallest integer in Z^+ such that $a^q \in H$

$b \in H \Rightarrow b \in G$

$\Rightarrow b = a^d$ for $d \in Z$

From division algorithm, there exist two unique integers 's' and 'r' such that,

$$d = qs + r, \text{ for } 0 \le r < q$$

$$\Rightarrow \quad a^d = a^{qs+r}$$

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

But $a^q \in H \Rightarrow (a^q)^s \in H$

$\Rightarrow \quad a^{qs} \Rightarrow a^{-qs} \in H \qquad [\because a \in H, a^{-1} \in H]$

$a^d, a^{-qs} \in H$

$\Rightarrow \quad a^d . a^{-qs} \in H$

$\Rightarrow \quad a^{d-qs} \in H$

$\Rightarrow \quad a^r \in H$ for $0 \le r < q$

This is a contradiction unless $r = 0$

$\therefore \quad d = qs$

Thus, $b = a^d = (a^q)^s \Rightarrow b \in (a^q)$

$\Rightarrow \quad H = \langle a^q \rangle$

$\therefore \quad H$ is cyclic.

(ii) Let,

$$|<a>| = n$$

Let H be any subgroup of $<a>$

$\Rightarrow \quad H = <a^m>$

Where,

m is the least positive integer such that $a^m \in H$

From the property of cyclic group i.e.,

If $|<a>| = n$ then $a^n = e$

Let b be any arbitrary member of H

Let $b = a^k$ for some k

From division algorithm,

$$k = mq + r$$

$\Rightarrow \quad k = mq \qquad [\because r = 0]$

$\Rightarrow \quad a^k = a^{mq}$

As, $\quad b = e = a^k = a^n$

$\Rightarrow \quad a^n = a^{mq}$

$\Rightarrow \quad n = mq$

Hence, the order of any subgroup of $<a>$ is a divisor of n

(iii) Let k represents the positive divisor of n

From the property of cyclic groups i.e., if a is an element of order n in a group and k is a positive integer, then

$$<a^k> = <a^{\gcd(n,k)}> \quad \text{and}$$

$$|a^k| = \frac{n}{\gcd(n,k)}$$

$<a^{\frac{n}{k}}>$ has order

$$\frac{n}{\gcd\left(n, \frac{n}{k}\right)} = \frac{n}{\frac{n}{k}} = k$$

Let H is a subgroup of $<a>$

But $H = <a^m>$

Where,

m is a divisor of n

Then,

$$m = \gcd(n, m)$$

$$k = |a^m|$$

$$= |a^{\gcd(n,m)}| = \frac{n}{\gcd(n,m)}$$

$$k = \frac{n}{m}$$

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

$$\Rightarrow H = <a^m> = <a^{\frac{n}{k}}>$$

Hence, the group $<a>$ has exactly one subgroup of order k i.e., $<a^{\frac{n}{k}}>$ for each positive divisor k of n.

Q64. Prove that n^{th} roots of unity form a cyclic group of order 'n'.

Answer :

From the standard identities of trigonometry,

$$1 = \cos 0 + i \sin 0$$

$$\Rightarrow \quad 1 = \cos(2\pi k) + i \sin(2\pi k)$$

Where,

$$k = 0, 1, 2, \ldots, (n-1)$$

$$\Rightarrow \quad 1^{1/n} = [\cos(2\pi k) + i \sin(2\pi k)]^{1/n}$$

$$\Rightarrow \quad 1^{1/n} = \cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n}$$

$$\Rightarrow \quad 1^{1/n} = e^{i2\pi k/n} \qquad [\because \cos\theta + i\sin\theta = e^{i\theta}]$$

$\therefore$ The n^{th} root of unity is given as,

$e^{i2\pi k/n}$ where, $k = 0, 1, 2, \ldots, (n-1)$

Let, $G = \{\omega^0 = 1, \omega^1, \omega^2, \ldots, \omega^{n-1}\}$, where

$\omega^k = e^{2k\pi i/n}$ for $k = 0, 1, 2, \ldots, (n-1)$

$\Rightarrow$ 'G' is a group under multiplication.

Moreover, $\omega^0 = 1 = e$

$$\omega^1 = \omega$$

$$\omega^2 = \omega.\omega$$

$$\omega^{n-1} = \omega, \omega.\omega \ldots \omega, (n-1) \text{ times}$$

Therefore, every element of G is a power of ω

$\Rightarrow \quad G = <\omega>$

$\therefore$ 'G' is a cyclic group of order 'n'.

⑥ If G is a group and let $a \in G$ then

$a^i = a^j$ $\quad$ $a^i = a^j$

(a) if a has infinite order

$\Rightarrow$ $a^i = a^j$ if and only if $i = j$

(b) If a has finite order lets say n then,

$\langle a \rangle = \{e, a^1, a^2, \ldots a^{n-1}\}$

and $a^i = a^j$ if and only if

n divides $(i-j)$

(a) The order of a is infinite $[a^\alpha = e]$

There is non zero n such that

$a^n = e$

if $a^i = a^j$

$\frac{a^i}{a^j} = 1$

$a^{i-j} = e$

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

$i - j = 0$

$i = j$

Reason

$[\because a^\alpha = e = a^0$

Since a has infinite order

hence $a^i = a^j$ if & only if $i = j$ if a has

Comparing the exponential terms on both sides,

$i - j = 0$

$\Rightarrow \quad i = j$

$\Rightarrow \quad a^i = a^j$ if and only if $i = j$ when a has infinite order.

(ii) **Case (i) :** $< a > = \{e, a, a^2, ..., a^{n-1}\}$

Let, n be the order of a.

$\Rightarrow \quad |a| = n \Rightarrow n$ is the least positive integer such that.

$$a^n = e \qquad \text{... (1)}$$

Let a^k represents an arbitrary member of cyclic group $< a >$.

From division algorithm,

$k = nq + r$ with $0 \leq r < n$ ... (2)

$a^k = a^{nq+r}$ [$\because$ From equation (2)]

$= a^{nq} \cdot a^r$

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

$= e^q \cdot a^r$ [$\because$ From equation (1)]

$= e \cdot a^r$

$= a^r \; 0 \leq r < n$

$\Rightarrow a^k = a^r$

k lies between 0 and n i.e., 1, 2, 3, 4, 5, ... n

$\Rightarrow \quad \{a^0, a^1, a^2, a^3, ... a^{n-1}\}$

$\Rightarrow \quad \{e, a, a^2, a^3, ... a^{n-1}\}$

$\Rightarrow \quad <a> = \{e, a, a^2, a^3, ... a^{n-1}\}$

$\therefore \quad <a> = \{e, a, a^2, a^3, ... a^{n-1}\}$

Case (ii) : n divides $(i - j)$

Let, $a^i = a^j$ and $i > j$

$\Rightarrow \quad \frac{a^i}{a^j} = e$

$\Rightarrow \quad a^{i-j} = e$

$i - j = nq + r$, with $0 \leq r < n$ ... (3)

[$\because$ From equation (2)]

$\Rightarrow \quad a^{nq+r} = e$

$\Rightarrow \quad a^{nq} \cdot a^r = e$

$\Rightarrow \quad (a^n)^q \cdot a^r = e$

$\Rightarrow \quad (e)^q \cdot a^r = e$ [$\because$ From equation (1)]

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

$\Rightarrow \quad a^r = e$

$\Rightarrow \quad a^r = a^0$

$\Rightarrow \quad r = 0$

Substituting $r = 0$ in equation (3),

$i - j = nq + 0$

$\Rightarrow \quad i - j = nq$ where, $q \in Z$

$\Rightarrow \quad n$ divides $i - j$

$\therefore \quad a^i = a^j$ if and only if n divides $i - j$ when 'a' has finite order

Lets do Remaining questions they are easy and unique interesting

(7) Define Subgroup → G → subset + group properties
pT intersection of 2 subgroups is again a subgroup
let G
⇒ let H, K be SG of G $H \leq G$, $K \leq G$, $H \cap K \leq G$

e be identity G.
$e \in H$ and $e \in K$
$\therefore e \in H \cap K$
$H \cap K$ non empty set, $H \cap K \leq G$

$a, b \in H \cap K$

$a, b \in H$ $a, b \in K$
$ab \in H$ $ab \in K$ [H, K SG closure]
$ab \in H \cap K$
$a^{-1} \in H \cap K$
$a^{-1} \in H$, $a^{-1} \in K$ [H ⊆ K SG every element has its Inverse]
$\therefore H \cap K$ SG
Asso Identity, Inverse
$H \cap K$ SG.

MY BEST BOOK

(2) State and prove one step Subgroup Test

Statement:- A non empty subset H of group G is subgroup of G if and only if $ab^{-1} \in H$ for all $a, b \in H$

Given,

H is a non empty subset of G

Let, $ab^{-1} \in H \; \forall \; a, b \in H$

(i) $a, b \in H$

$\Rightarrow \quad ab^{-1} \in H$

Let, $b = a$

$\Rightarrow \quad aa^{-1} \in H$

$\Rightarrow \quad e \in H$

$\therefore \quad e \in H$

(ii) $e \in H, a \in H$

$\Rightarrow \quad ea^{-1} \in H$

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

$e \in H, b \in H$

$\Rightarrow \quad eb^{-1} \in H$

$\Rightarrow \quad b^{-1} \in H$

(iii) $a \in H, b \in H \Rightarrow a\,b^{-1} \in H$

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

$\Rightarrow a(b^{-1})^{-1} \in H$

$\Rightarrow \quad ab \in H$

$\therefore$ The closure property is satisfied in H

(iv) $a, b, c \in H \quad \Rightarrow a, b, c \in G$

$\Rightarrow a(bc) = (ab)C$

i.e., All elements of H are in G and the composition is associative in G and H.

Hence, H forms a group with the same operation in G

$\therefore \quad H$ is a subgroup of G.

Converse: Let H be a subgroup.

(i) By closure axiom: $a, b \in H \Rightarrow a\,b \in H$

(ii) By inverse axiom: $a, b \in H \Rightarrow a^{-1} \in H, b^{-1} \in H$

$\therefore \quad a \in H, b^{-1} \in H \Rightarrow ab^{-1} \in H.$

(3) State and prove uniqueness of the identity theorem in group

Stt:- In a group G there is only one identity elmt

proof:- Let e and e' identity $\in G$

$a \in G$

$ae = ea = a$ — (1)

$a.e' = e'a = a$ — (2) $\forall a \in G$

$a = e' \Rightarrow e'.e = e.e' = e'$ — (4)

$a = e$

$a = e.e' = e'e = e$ — (3)

$\therefore$ (3) and four clear

$$\boxed{e' = e}$$

(4) State and prove Cancellation laws

a, b, c elements a group & binary opⁿ —

(i) $ba = ca \Rightarrow b = c$ [Right Cancellation law]

(ii) $ab = ac \Rightarrow b = c$ [left cancellation law]

Proof :- RCL :-

a^{-1} be an inverse of a

$$(ba)a^{-1} = (ca)a^{-1}$$
$$baa^{-1} = c.aa^{-1}$$
$$b.e = c.e$$
$$\boxed{b = c}$$

LCL :-

a^{-1} be inverse a

$$a^{-1}(ab) = a^{-1}(ac)$$
$$a^{-1}ab = a^{-1}a.c$$
$$eb = ec$$
$$\boxed{b = c}$$

State and prove uniqueness of inverse theorem in group

⇒ Statement :-
for each element in group there is unique element
$a, b \in G$
$ab = ba = e$

Proof :- Let b, c be inverse of a where $a \in G$

$ab = ba = e$ ... ①
$ac = ca = e$ ... ②

e identity element in G

$ab = ac$ or $ba = ca$
$b = c$ $b = c$

every
∴ element has its unique inverse

(5) for any 2 elements a, b in G
pt $(ab)^{-1} = b^{-1}a^{-1}$.
(or) =
state and prove shoes & socks property

Proof: Given that

$a, b \in G \Rightarrow ab \in G$ } closure
$a^{-1}, b^{-1} \in G \Rightarrow$ ~~$a^{-1}b^{-1} \in G$~~ } property

$$(ab)(b^{-1}a^{-1}) = a.bb^{-1}a^{-1}$$
$$= a.ea^{-1}$$
$$= aa^{-1}$$
$$(ab)(b^{-1}a^{-1}) = e \quad -(1)$$

$$(b^{-1}a^{-1})(ab) = b^{-1}.a^{-1}ab$$
$$= b^{-1}.eb$$
$$= b^{-1}.b$$
$$(b^{-1}a^{-1})(ab) = e \quad -(2)$$

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

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

Q49. Let G be a group and H,K be two subgroups of G. Then show that HK = {hk|h ∈ H, k∈K} is a subgroup of G.

Answer : **(OU) June-18, Q9(a)(i)**

Given,

G is a group

H,K are two subgroups of G

$HK = \{hk | h \in H, k \in K\}$

Let a, b be any two elements of HK

i.e., $a,b \in HK$

$\Rightarrow \quad a = h_1 k_1, \quad b = h_2 k_2$

Where,

$h_1, h_2 = h \in H$

$k_1, k_2 = k \in K$

Condition 1

The product of the two elements of H is itself an element of H.

$$ab = h_1 k_1 . h_2 k_2$$
$$= h_1 h_2 k_1 k_2$$
$$= hk \in HK$$

$\therefore \quad ab \in HK$

Condition 2

The identity element, $e \in HK$

Condition 3

The inverse of an element of H, K is itself an element of H, K

Since,

$$h_1 h_2 \in H \text{ and } k_1 k_2 \in K$$

Also $a^{-1} = (h_1 k_1)^{-1} = k_1^{-1} h_1^{-1}$

$$b^{-1} = (h_2 k_2)^{-1} = k_2^{-1} h_2^{-1}$$

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

$$= k_1^{-1} h_1^{-1} \; k_2^{-1} h_2^{-1}$$

$$\in KH = HK$$

$\therefore$ HK is a subgroup of G.

Abelian → $(ax = xa) \forall x \in G$

prove that every cyclic group is abelian

· cyclic gp defn or any of

G ⇒ $G = \langle a \rangle = \{a^n \quad n \in Z\}$

let us consider

$x, y \in G$

$x = a^r, \quad y = a^s \quad r, s \in Z$

$xy = a^r a^s$

$xy = a^{r+s}$

$= a^{s+r}$

$xy = a^s . a^r$

$xy = y . x$

$xy = yx$.

∴ G is abelian

Let a and b be two elements of an abelian group and let n be any integer. Show that $(ab)^n = a^n b^n$ and hence deduce that $(ab)^{-1} = a^{-1} b^{-1}$. Is it true for non-abelian?

Answer :

Let, G be an abelian group

Let, a, b are the elements of G.

$\Rightarrow \quad a, b \in G$

Let, n be any integer,

(i) **n is a Positive Integer**

Let, $(ab)^n = a^n b^n$ ... (1)

Substituting, $n = 1$ in equation (1),

$(ab)' = ab$

$= a'b' \ \forall \ a, b \in G$

$\therefore$ Equation (1) is true for $n = 1$

Let, equation (1) is true for $n = k$,

$\Rightarrow \quad (ab)^k = a^k b^k$

Consider,

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

$= a^k b^k ab$

$= a^k (b^k a) b$ [$\because$ Using associativity in G]

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

$= a^k a . b^k b$

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

$\therefore \quad (ab)^{k+1} = a^{k+1} b^{k+1}$

Hence, equation (1) is true for $n = k + 1$

From mathematical induction,

$(ab)^n = a^n b^n$ is true $\forall \ n \in N$

(ii) n is a Negative Integer

If n is a negative integer, then $-n$ is a positive integer.

Consider,

$$(ab)^n = (ba)^n \qquad [\because G \text{ is abelian}]$$

$$= ((ba)^{-1})^{-n} \qquad [\because n = (-1)(-n)]$$

From the property of groups,

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

$$\Rightarrow \quad ((ba)^{-1})^{-n} = (a^{-1}b^{-1})^{-n}$$

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

$$= a^n b^n$$

$$\therefore \quad (ab)^n = a^n b^n \; \forall \; a, b \in G$$

Substituting, $n = -1$ in above equation,

$$(ab)^{-1} = (ba)^{-1} \qquad [\because G \text{ is abelian}]$$

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

$\therefore$ $(ab)^{-1} = a^{-1}b^{-1}$ when G is abelian.

The condition is not true for non-abelian group.

$$\Rightarrow \quad (ab)^n \neq a^n b^n$$

$\therefore$ $(ab)^n = a^n b^n$ when G is abelian and $(ab)^n \neq a^n b^n$ when G is non abelian.

Q37. **Prove that the set $GL(2, R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in R, ad - bc \neq 0 \right\}$ is a non abelian group with respect to matrix multiplication.** **(OU) May/June-19, Q1**

OR

Show that GL(2, R) is a non-abelian group under matrix multiplication. **(KU) PP-1, Q1**

OR

Show that the set

$$GL(2,R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}; a, b, c, d \in R, ad - bc \neq 0 \right\}$$

forms a group under matrix multiplication.

Answer : **(MGU) May/June-18, Q1**

Given set is,

$$GL(2, R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in R, \ ad - bc \neq 0 \right\}$$

Let, $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in GL(2, R)$

$\Rightarrow \quad \det A = a_1 d_1 - b_1 c_1 \neq 0$

$\Rightarrow \quad \det B = a_2 d_2 - b_2 c_2 \neq 0$

$$AB = \begin{vmatrix} a_1 & b_1 \\ c_1 & d_1 \end{vmatrix} \begin{vmatrix} a_2 & b_2 \\ c_2 & d_2 \end{vmatrix}$$

$$AB = \begin{vmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{vmatrix}$$

$\therefore$ Multiplication is closed in $GL(2, R)$

Then $\det(AB) = (\det A)(\det B)$

$\neq 0$

$\therefore$ $\det(AB) \neq 0$

i.e., product of two matrices with non-zero determinant is also a matrix with non-zero determinant.

Associativity of matrices can also be proved.

The identity is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

i.e., $\det \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1 - 0 = 1 \neq 0$

The inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

$\therefore$ $GL(2, R)$ is a group under matrix multiplication.

Non-Abelian:

$GL(2, R)$ is said to be an abelian group if it satisfies the following condition

$$AB = BA$$

$$AB = \begin{bmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{bmatrix} \quad \ldots (1)$$

Consider,

$$BA = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$$

$$\therefore \quad BA = \begin{bmatrix} a_2 a_1 + b_2 c_1 & a_2 b_1 + b_2 d_1 \\ c_2 a_1 + d_2 c_1 & c_2 b_1 + d_2 d_1 \end{bmatrix} \quad \ldots (2)$$

From equations (1) and (2),

$$AB \neq BA$$

$\Rightarrow$ $GL(2, R)$ is non-abelian

$\therefore$ The set $GL(2, R)$ is a non abelian group under matrix multiplication.

PT matrix of 2×2 ... and is non abelian group

Answer :

Given that,

$$SL(2, F) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \begin{array}{l} \text{with } ad - bc = 1, \\ \text{where } a, b, c, d \in Q \end{array} \right\} \quad \ldots (1)$$

Where F in a field of real, rational or complex numbers i.e., $F = R$, $F = Q$, $F = C$ (or) $F = Z_p$ where p is prime.

Claim: $SL(2, Q)$ is non-abelian group

Since,

Q^+ forms a group under multiplication.

(i) Closure

Let $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in SL(2, Q)$

Where, a_1, b_1, c_1, d_1 & $a_2, b_2, c_2, d_2 \in Q$ with $a_1 d_1 - b_1 c_1 = 1$ and $a_2 d_2 - b_2 c_2 = 1$

[$\because$ From equation (1)]

Consider,

$$AB = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 d_2 + d_1 d_2 \end{bmatrix} \in SL(2, Q)$$

$\Rightarrow$ $AB \in SL(2, Q)$

$\therefore$ $SL(2, Q)$ is closure.

(ii) Associative

For $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ and

Let $C = \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \in SL(2, Q)$

$\Rightarrow$ $(A.B).C = A.(B.C)$

$SL(2, Q)$ is Associative

(iii) Identity

Let, $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \in SL(2, Q)$

Then, there exist $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ such that $A.I = I.A = A$

$\therefore$ $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ in the identity matrix in $SL(2, Q)$.

(iv) Inverse

Let $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \in SL(2, Q)$

$|A| = a_1 d_1 - b_1 c_1 = 1$

Then there exist A^{-1} such that $A.A^{-1} = A^{-1}.A$

Consider,

$A.A^{-1} = I$,

Where,

$$A^{-1} = \frac{Adj(A)}{\det(A)}$$

$$\text{Adj}(A) = \begin{bmatrix} d_1 & -b_1 \\ -c_1 & a_1 \end{bmatrix}$$

$$\therefore \quad A^{-1} = \frac{\begin{bmatrix} d_1 & -b_1 \\ -c_1 & a_1 \end{bmatrix}}{1}$$

[$\because$ From equation (

$$A^{-1} = \begin{bmatrix} d_1 & -b_1 \\ -c_1 & a_1 \end{bmatrix}$$ is the inverse matrix of

$\therefore$ $SL(2, Q)$ is a group

(v) Commutative Property

Let, $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$

$$A.B = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{bmatrix}$$

$$B.A = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$$

$$= \begin{bmatrix} a_2 a_1 + b_2 c_1 & a_2 b_1 + b_2 d_1 \\ c_2 a_1 + d_2 c_1 & c_2 b_1 + d_2 d_1 \end{bmatrix}$$

$\Rightarrow$ $A.B \neq B.A$

$\therefore$ It is not a commutative

Thus, $SL(2, Q)$ does not satisfies commutative property.

$\therefore$ $SL(2, Q)$ is non-abelian group.

Q39. Show that every group G with identity e such that x * x = e for all x in G, is abelian.

Oct.-13, 02

Answer :

Given that,

'G' is a group with identity 'e' such that,

$x * x = e \ \forall \ x \in G$

Let, $a, b \in G$

$\Rightarrow$ $a * a = e$ and $b * b = e$

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

Since,

$$a,b \in G$$

$$\Rightarrow \quad a * b \in G$$

$$\Rightarrow \quad (a * b) * (a * b) = e$$

$$\Rightarrow \quad (a * b) = (a * b)^{-1} \quad [\because e \text{ is an identity element}]$$

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

$$= b * a$$

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

$\therefore$ 'G' is an abelian group.

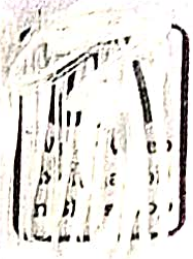
Q41. If $*$ defined on Q^+ by $a * b = \frac{ab}{2}$. Then show that $(Q^+, *)$ is a group.

Answer : [March/April-17, Q1 | March/April-14, Q1 | March-12, Q1]

Given that,

$*$ is the operation defined on Q^+ such that $a * b = \frac{ab}{2} \; \forall \; a,b \in Q^+$

Q^+ is the set of all positive rational number.



(i) Closure

For $a,b \in Q^+$

$$\frac{ab}{2} \in Q^+$$

$$\Rightarrow \quad a * b = \frac{ab}{2} \in Q^+$$

(ii) Associativity

For $a,b,c \in Q^+$

$$(a * b) * c = \left(\frac{ab}{2}\right) * c$$

$$= \left(\frac{ab}{2}\right)\left(\frac{c}{2}\right) = \frac{abc}{4}$$

$$a * (b * c) = a * \left(\frac{bc}{2}\right)$$

$$= \frac{abc}{2(2)} = \frac{abc}{4}$$

$$\therefore \quad (a * b) * c = a * (b * c)$$

(iii) Identity

For $a \in Q^+$

$$a * e = a \qquad [\because e \text{ is an identity element}]$$

$$\Rightarrow \quad \frac{ae}{2} = a$$

$$\Rightarrow \quad ae = 2a$$

$$\Rightarrow \quad e = 2 \in Q^+$$

$$\Rightarrow \quad e * a = \frac{ea}{2} = \frac{2a}{2}$$

$$= a$$

$$\Rightarrow \quad a * e = e * a = a$$

Therefore, $\forall \; a \in Q^+$, $e = 2$ is an identity element in Q^+.

(iv) Inverse

For $a \in Q^+$

$$a * a' = e$$

$$\Rightarrow \quad a * a' = 2 \qquad [\because e = 2]$$

$$\Rightarrow \quad \frac{aa'}{2} = 2$$

$$\Rightarrow \quad aa' = 4$$

$$\Rightarrow \quad a' = \frac{4}{a} \in Q^+$$

$$= \frac{4}{a}\left(\frac{a}{2}\right)$$

$$= 2 = e$$

$$\Rightarrow \quad a * a' = a' * a = e$$

Therefore, $a \in Q_0^+$ there is an element $a' = \frac{4}{a} \in Q$ such that $a' = \frac{4}{a}$ is the inverse of 'a'.

$\therefore$ $(Q_0^+, *)$ is a group.

Q42. Let S be the set of all real numbers except –1. Define $*$ on S by $a * b = a + b + ab$. Show that (S, $*$) is an abelian group.

[Oct./Nov.-17, Q1 | March/April-15, Q1

Answer :

Given that,

'S' is the set of all real numbers except -1.

$*$ is the operation defined on S such that $a * b = a + b + ab \ \forall \ a, b \in S$

Let, $a, b, c \in S$ where $a \neq b \neq c \neq -1$.

A set is said to be an abelian group if it satisfies the following conditions.

(i) Closure

For $a, b \in S$.

$$a * b = a + b + ab \in S$$

$\therefore$ $(S, *)$ is closed under $*$.

(ii) Associativity

For $a, b, c \in S$

$$(a * b) * c = (a + b + ab) * c$$

$$= a + b + ab + c + (a + b + ab)\, c$$

$$[\because a * b = a + b + ab]$$

$$= a + b + ab + c + ac + bc + abc$$

$$= a + b + c + ab + bc + ac + abc$$

Similarly, $a * (b * c) = a * (b + c + bc)$

$$= a + b + c + bc + a\,(b + c + bc)$$

$$= a + b + c + bc + ab + ac + abc$$

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

$\therefore$ $*$ is associative.

(iii) Identity

For $a \in S$,

$$a * e = a$$

$$\Rightarrow \quad a + e + ae = a$$

$$\Rightarrow \quad e + ae = 0 \qquad \Rightarrow \quad e\,(1 + a) = 0$$

$$\Rightarrow \quad e = 0 \qquad [\because a \neq -1]$$

Similarly,

$$e * a = e + a + ea$$

$$= 0 + a + 0.a$$

$$= a$$

$$\Rightarrow \quad a * e = e * a = a$$

$\therefore \forall\, a \in S,\ e = 0$ is an identity element for $*$.

(iv) Inverse

For $a \in S$,

$$a * a' = e$$

$$\Rightarrow \quad a * a' = 0$$

$$\Rightarrow \quad a + a' + aa' = 0 \qquad [\because\ a * b = a + b + ab]$$

$$\Rightarrow \quad a'(1 + a) + a = 0 \qquad \Rightarrow \quad a'(1 + a) = -a$$

$$\Rightarrow \quad a' = \frac{-a}{1+a} \text{ where, } a \neq -1$$

Similarly,

$$a' * a = a' + a + a'a$$

$$= \frac{-a}{1+a} + a + \frac{-a}{1+a}(a)$$

$$= \frac{-a}{1+a}(1+a) + a$$

$$= -a + a = 0 = e$$

$$\Rightarrow \quad a * a' = a' * a = e$$

$\therefore$ $\forall\, a \in S$, there is an element $a' = \dfrac{-a}{1+a} \in S$ such that $a' = \dfrac{-a}{1+a}$ is the inverse of 'a'.

(v) Commutativity

$$a * b = a + b + ab = b + a + ab = b * a$$

$\therefore$ $(S, *)$ is an abelian group.

Q70. Let a be an element of order n in a group and let k be a positive integer. Then prove that $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = \frac{n}{\gcd(n,k)}$.

[(MGU) July/Aug.-22, Q8 | (KU) May/June-18, Q2(b)]

OR

Let G be a group G and a $\in$ G such that $|a| = n$. If K is a positive integer then prove that,

$\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = \frac{n}{\gcd(n,k)}$.

(OU) Jan.-21, Q10

OR

If a is an element of order n in a group and k be a positive integer, then show that $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = \frac{n}{\gcd(n,k)}$.

(KU) PP-1, Q9(b)

OR

Let G be a group and a$\in$G is such that O(a) = n then show that $O(a^k) = \frac{n}{\gcd(n,k)}$ (where k is a positive integer).

Answer : (OU) June-18, Q9(a)(ii)

Given that,

The element a has order n i.e.,

$|a| = n$

$\Rightarrow$ n is the least positive integer such that,

$$a^n = e \quad \ldots (1)$$

(i) Let, the gcd of n, k be d.

i.e., $d = \gcd(n, k)$

Let, $k = \gcd(n, k).r$

$\Rightarrow$ $k = dr$

Consider,

$$a^k = a^{dr}$$
$$= (a^d)^r$$

$$\Rightarrow \langle a^k \rangle \subseteq \langle a^d \rangle \quad \ldots (2)$$

From the property of gcd of two numbers, i.e., for any two integers n, k there exist integers s and t such that, $\gcd(n, k) = ns + kt$

$\Rightarrow$ $d = ns + kt$

Consider,

$$a^d = a^{ns + kt}$$
$$= a^{ns} \cdot a^{kt}$$
$$= (a^n)^s \cdot (a^k)^t$$
$$= e^s (a^k)^t \quad [\because \text{From equation (1)}]$$
$$= (a^k)^t$$

$$\Rightarrow \langle a^d \rangle \subseteq \langle a^k \rangle \quad \ldots (3)$$

From equations (2) and (3),

$$\langle a^k \rangle \equiv \langle a^d \rangle$$

$$\equiv \langle a^{\gcd(n, k)} \rangle$$

$$\therefore \langle a^k \rangle \equiv \langle a^{\gcd(n, k)} \rangle$$

(ii) To prove $|a^d| = \frac{n}{d}$

Consider,

$$(a^d)^{\frac{n}{d}} = a^{\frac{nd}{d}}$$

$$= a^n$$

$$= e$$

$$\Rightarrow \quad (a^d)^{\frac{n}{d}} = e$$

$$\Rightarrow \quad |a^d| \leq \frac{n}{d} \qquad \ldots (4)$$

If 'i' is a positive integer less than $\frac{n}{d}$ then,

$$(a^d)^i \neq e \qquad [\because |a| = n]$$

$$\Rightarrow \quad |a^k| = |\langle a^k \rangle|$$

$$= |\langle a^d \rangle|$$

$$= |\langle a^{\gcd(n, k)} \rangle|$$

$$= |a^{\gcd(n, k)}|$$

$$= \frac{n}{\gcd(n, k)} \quad [\because \text{From equation (4)}]$$

$$\therefore \quad |a^k| = \frac{n}{\gcd(n, k)}.$$