GROUP THEORY

INTRODUCTION
DEFINITIONS – EXAMPLES
ELEMENTARY PROPERTIES OF A GROUP
THEOREMS - PROBLEMS
CONCLUSION

PREPARED BY

S.Lt / Dr.D.CH.PAPARAO. M.Sc, Ph.D, PGDCA
Head, Dept. of Mathematics
S.K.B.R.COLLEGE, AMALAPURAM
East Godavari Dist. Andhra Pradesh
Mail ID: dchp876@gmail.com

"If you are not certain where you are going, you may very well end up somewhere else and not even know it"

By MAGER

INTRODUCTION

Group theory is the study of algebraic structures called groups. This introduction will rely heavily on set theory and modular arithmetic's as well. Later on it will require an understanding of mathematical induction, functions, bisections, and partitions.

Group Theory can be viewed as the mathematical theory that deals with symmetry, where symmetry has a very general meaning.

BINARY OPERATION

Let A be a non empty set. **Any mapping** $*$ **from** *A x A* into *A* is known as a Binary Operation.

$\textbf{If } * \textbf{ is a binary operation in A then}$

$\forall\, \mathbf{a, b} \in \mathbf{A} \Rightarrow \mathbf{a * b}$ **is a unique element in A.**

$\textbf{Let}\quad \mathbf{a, b} \in \mathbf{A} \quad \Rightarrow (\mathbf{a, b}) \in \mathbf{A\,x\,A}$

$\textbf{The image of } *(\mathbf{a, b}) \textbf{ is written as } \mathbf{a * b}$

$\therefore \quad *(\mathbf{a, b}) = \mathbf{a * b}$

Example :

Let C be the set of Complex numbers

$\textbf{Let } \mathbf{2, 3} \in \mathbf{C} \Rightarrow 2 + 3 = 5 \in \mathbf{C} \;\&\; 2.3 = 6 \in \mathbf{C}$

$\therefore + \textbf{ and } \bullet \textbf{ are binary operations in C.}$

ALGEBRAIC STRUCTURE (A. S)

Let A be a non empty set **and B is the set of all binary operations on A. Then (A, B)** is known as A.S.

If $*$ is a binary operation on A then $(A, *)$ is an Algebraic Strecture.

Example: We know that

$+$ and $\cdot$ are two binary operations in R

then $(R, +)$ and $(R, \cdot)$ are Algebraic Structures.

Moreover $(N, +), (N, \cdot), (Z, +), (Z, \cdot), (Q, +), (Q, \cdot)$ $(C, +), (C, \cdot)$ are all algebraic structures.

SEMIGROUP

Let S be a non empty set and $*$ is the binary operation on S. Then the algebraic structure $(S, *)$ is said to be a Semi Group if

$$\mathbf{a} * (\mathbf{b} * \mathbf{c}) = (\mathbf{a} * \mathbf{b}) * \mathbf{c} \quad \forall \mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbf{S}$$

$\Rightarrow *$ **is an associative binary operation on S.**

$\therefore (\mathbf{S}, *)$ **is a Semigroup.**

Example : 1. $(\mathbf{N}, +)$ **is a Semigroup.**

2. $(\mathbf{Z}, +)$ **is a Semigroup.**

IDENTITY ELEMENT

Let (S, $*$) be a Semi Group and a, b belongs to S. An element $e \in S$ is said to be Left Identity of S if $e * a = a \ \forall a \in S \ \Rightarrow$ e is the <u>Left Identity</u> element in S

Similarly

$a * e = a \ \forall a \in S \ \Rightarrow$ e is the <u>Right Identity</u> element in S

If $a * e = a = e * a \ \forall a \in S \ \Rightarrow$ e is the <u>Identity Element</u> in S

In general,

if $a + e = a = e + a \ \forall a \in S$

$\Rightarrow$ e is the Additive Identity element in S

Example: 0 is the additive identity element in $(Z, +)$

If $a \bullet e = a = e \bullet a \;\; \forall\, a \in S$

$\Rightarrow$ 'e' is the <u>Multiplicative Identity</u> in S

Example:

'1' is the Multiplicative Identity in the Semi Group $(C, \bullet)$.

NOTE: If $(S, *)$ is the Semi Group with Identity e then

'e' is the unique element in S.

Let e and e' are two <u>Identity Elements</u>

in a Semigroup $(S, *)$, then we have $e = e'$.

MONOID

Let $(s, \ast)$ be a Semigroup with identity element e then S is called the Monoid.

Examples :

1. $(\mathbf{Z}, +)$ **is a Monoid,** 0 **is the identity element.**

2. $(\mathbf{Q}, \cdot)$ **is a Monoid,** 1 **is the identity element.**

3. $(\mathbf{N}, +)$ **is not a Monoid, where** $\mathbf{N} = \{1, 2, 3, 4, \cdots\cdots\}$

$\therefore$ **additive identity element** 0 **does not exists in N.**

Give an example of Semigroup which is not a Monoid

Example: (N, +) is a Semigroup but not a Monoid.

INVERSE ELEMENT

Let $(S, *)$ be a Semigroup with identity element *e*.

An element $a \in S$ is said to be <u>left inverse</u>
if there exists an element $b \in S$ such that
$\underline{b * a = e} \Rightarrow$ **b is the left inverse of a.**

An element $a \in S$ is said to be <u>right inverse</u>
if there exists an element $c \in S$ such that
$\underline{a * c = e} \Rightarrow$ **c is the right inverse of a.**

'a' is invertible element in S if a is both left and right invertible.

$\therefore\ a * b = e = b * a \Rightarrow$ **a is invertiable**
and the inverse of 'a' is unique.

THEOREM

Let (S, *) be a Semigroup with identity element *e* and a $\in S$. If b is the left inverse and c is the right inverse of a then b = c.

$\mathbf{Let\ (S,*)\ be\ a\ semigroup\ and\ e\ is\ identity\ in\ S.}$

$\mathbf{Let\ a,\ b,\ c \in S}$

$\because$ **b is the left inverse of a** $\Rightarrow b * a = e \rightarrow (1)$

$\because$ **c is the right inverse of a** $\Rightarrow a * c = e \rightarrow (2)$

Claim : $\underline{\textbf{we prove that } b = c}$

$\because$ **e is the identity element in S** $\Rightarrow a * e = e * a = a \rightarrow (3)$

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

Hence proved

GROUP

Let G be a nonempty set and $*$ is a binary operation on G. The algebraic structure $(G, *)$ is said to be group if G satisfies the following three axioms

1. **Associative**

$$\mathbf{a * (b * c) = (a * b) * c \quad \forall\ a, b, c \in G}$$

2. **Existence of identity**

$$\mathbf{a * b = b * a = a \quad \Rightarrow b = e \text{ is the identity in } G.}$$

$$\mathbf{\text{i.e., } a * e = e * a = a \quad \Rightarrow e \text{ is the identity in } G.}$$

3. **Existence of inverse**

$$\mathbf{a * b = b * a = e \quad \Rightarrow b = a^{-1} \text{ is the inverse of } a}$$

$$\mathbf{\text{i.e., } a * a^{-1} = a^{-1} * a = e \Rightarrow a^{-1} \text{ is the inverse of } a}$$

$$\mathbf{\therefore (G, *) \text{ is a group}}$$

Examples for GROUPS

1. $(\mathbf{Z},+),(\mathbf{Q},+),(\mathbf{R},+),(\mathbf{C},+)$ **are additive groups,**

0 **is the additive identity.**

2. $(\mathbf{Q}^*,\bullet),(\mathbf{R}^*,\bullet),(\mathbf{C}^*,\bullet)$ **are multiplicative groups,**

1 **is the multiplicative identity. Here** $\mathbf{X}^* = \mathbf{X} - \{0\}, \mathbf{X} = \mathbf{Q},\mathbf{R},\mathbf{C}.$

3. $(\mathbf{Z}^*,\bullet)$ **is not a Group, where** $\mathbf{Z} = \{\cdots -3,-2,-1,0,1,2,3,\cdots\}$

$\because$ **Multiplicative inverses of non – zero elements does not exists in Z.**

i.e., Multiplicative inverse of a is $\frac{1}{\mathbf{a}}(\mathbf{a} \neq 0)$

$\because$ **Multiplicative inverse of** 2 **is** $\frac{1}{2}$**, but** $\frac{1}{2} \notin \mathbf{Z}$

COMMUTATIVE GROUP

Let $(G, *)$ be a group and $a, b \in G$. G is said to be a commutative group if $a * b = b * a \ \forall a, b \in G$

In additive Group $\Rightarrow a + b = b + a \ \forall a, b \in G$

In multiplicative Group $\Rightarrow a \cdot b = b \cdot a \ \forall a, b \in G$

1. $(Z, +), (Q, +), (R, +), (C, +)$ are commutative groups w.r.t addition.

2. $(Q^*, \cdot), (R^*, \cdot), (C^*, \cdot)$ are commutative groups w.r.t multiplication. Here $X^* = X - \{0\}, X = Q, R, C.$

3. $(Z^*, \cdot)$ is not a Commutative Group.

PROBLEMS

If $G = Q - \{1\}$ and $*$ is defined on G as $a * b = a + b - ab$ then show that $(G, *)$ is an abelian group.

$1.$ $\underline{\text{Closure Property}}$

$\text{Let } a, b \in G \quad \Rightarrow a \neq 1, b \neq 1 \text{ and } a + b, ab \in G$

$\Rightarrow a + b - ab \in G \quad \Rightarrow a * b \in G$

$\Rightarrow *$ is a binary operation on G.

$2.$ $\underline{\text{Associative Property}}$

$$\text{LHS} = a * (b * c) = a * (b + c - bc)$$

$$= a + (b + c - bc) - a(b + c - bc)$$

$$= a + b + c - ab - bc - ca + abc$$

$$\text{RHS} = (a * b) * c = (a + b - ab) * c$$

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

$$= a + b + c - ab - bc - ca + abc$$

$\therefore (a + b - ab) = (a * b) * c \Rightarrow *$ is associative in G.

3. <u>Identity Property</u>

$$\text{Let } a,b \in G \text{ and } a*b = a \quad \Rightarrow a+b-ab = a$$

$$\Rightarrow b(1-a) = 0 \qquad \Rightarrow b = 0 \qquad \because a \neq 1$$

$$\therefore b = 0 = e \text{ is the identity element in } G$$

4. <u>Inverse Property</u>

$$\text{Let } a,b \in G \text{ and } a*b = e \quad \Rightarrow a+b-ab = 0$$

$$\Rightarrow b(1-a)+a = 0 \Rightarrow b = \frac{a}{a-1}\left(=a^{-1}\right)$$

$$\Rightarrow b = \frac{a}{a-1} \text{ is the inverse element of } a \text{ in } G.$$

$$\therefore (G,*) \text{ is a group}$$

5. <u>Abelian Property</u>

$$\text{Let } a,b \in G$$

$$a*b = a+b-ab = b+a-ba = b*a$$

$$\therefore (G,*) \text{ is an abelian group.}$$

SOME EXAMPLE PROBLEMS

1. If $G = R - \{-1\}$ and $*$ is defined on G, as $a * b = a + b + ab \ \forall a, b \in G$ then show that $(G, *)$ is an abelain group.

2. If $*$ is defined on Z, as $a * b = a + b - 3$ then show that $(Z, *)$ is an abelain group.

3. If o is defined on Q^+, as $aob = \frac{ab}{3} \ \forall a, b \in Q^+$ then show that (Q^+, o) is an abelain group.

4. Show that the $G = \{x / x = 2^a 3^b \text{ and } a, b \in Z\}$ is an abelain group w.r.t. multiplication.

Cancellation laws are hold in a group G

$\textbf{Let G be a group and } a,b,c \in G$

$\textbf{Take } ab = ac \qquad \left(\because a^{-1}a = aa^{-1} = e\right)$

$$\Rightarrow a^{-1}(ab) = a^{-1}(ac) \Rightarrow \left(a^{-1}a\right)b = \left(a^{-1}a\right)c$$

$$\Rightarrow (e)b = (e)c \Rightarrow b = c\left(\because ae = ea = a\right)$$

$\therefore$ **Left cancellation law hold in G.**

$\textbf{Let G be a group and } a,b,c \in G$

$\textbf{Take } ba = ca \qquad \left(\because a^{-1}a = aa^{-1} = e\right)$

$$\Rightarrow (ba)a^{-1} = (ca)a^{-1} \Rightarrow b\left(a^{-1}a\right) = c\left(a^{-1}a\right)$$

$$\Rightarrow b(e) = c(e) \qquad \Rightarrow b = c\left(\because ae = ea = a\right)$$

$\therefore$ **Right cancellation law hold in G.**

Elementary Properties of a group G

In a group G, Identity element is unique

Proof : Let G be a group and e and e' are two identity elements in G. $\left(\because e, e' \in G\right)$

Claim : <u>We prove that $e = e'$</u>

$\because$ e is identity element in G $\Rightarrow a.e = e.a = a \quad \forall a \in G$

$\because e' \in G \quad \Rightarrow e'.e = e.e' = e' \rightarrow (1)$

$\because$ e' is identity element in G $\Rightarrow a.e' = e'.a = a \quad \forall a \in G$

$\because e \in G \quad \Rightarrow e.e' = e'.e = e \rightarrow (2)$

From (1) & (2), we get $e = e'$

Hence proved

In a group, Inverse of any element is unique

Proof : Let G be a group and b and c are two inverse elements of a in G. $(\because e \in G)$

Claim : $\underline{\text{We prove that } b = c}$

$\because$ b is inverse element of a $\Rightarrow$ $a.b = b.a = e \quad \forall a \in G \rightarrow (1)$

$\because$ c is inverse element of a $\Rightarrow$ $a.c = c.a = e \quad \forall a \in G \rightarrow (2)$

Now $\quad b = be = b(ac) = (ba)c = (e)c = c$

$$\therefore \; b = c$$

Hence proved

Let G be a group, if $a \in G$ then prove that $\left(a^{-1}\right)^{-1} = a$

Let G be a group and $a, b \in G$

Let $b = a^{-1} \Rightarrow$ b is the inverse element of a

$\Rightarrow ab = e$ and $ba = e$

$\therefore ba = ab = e$

$\Rightarrow a = b^{-1} \quad (\because$ a is the inverse element of b$)$

$\Rightarrow a = \left(a^{-1}\right)^{-1} \quad \left(\because a^{-1} = b\right)$

Hence proved

Let G be a group, if $a, b \in G$ then prove that $(ab)^{-1} = b^{-1}a^{-1}$

Proof : Let G be a group and $a, b \in G$

By inverse property $aa^{-1} = a^{-1}a = e$

By identity property $ae = ea = a$

Now

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

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

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

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

Hence proved

PROB : If G is a group such that $(ab)^m = a^m b^m \ \forall a,b \in G$ for three consecutive $+$ve integers then show that $(G, \bullet)$ is an abelian group.

Proof: Let G be a group and $a,b \in G$

Suppose m,m+1, m+2 be the three consecutive integers such that $\Rightarrow (ab)^m = a^m b^m$,

$(ab)^{m+1} = a^{m+1} b^{m+1}$, and $(ab)^{m+2} = a^{m+2} b^{m+2}$

Claim : <u>We prove that G is an abelian group</u>

$\because (ab)^{m+2} = a^{m+2} b^{m+2} \Rightarrow (ab)^{m+1}(ab) = a^{m+1} ab^{m+1} b$

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

$\Rightarrow a^{m+1}(b^{m+1}a)b = a^{m+1}(ab^{m+1})b \ (\because \text{Cancellation Laws})$

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

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

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

$\therefore G$ is an abelian group.

Theorem : Let G be a group and $a, b \in G$ then show that the equations $ax = b$ and $ya = b$ have unique solutions.

Proof: Let G be a group and $a, b \in G \Rightarrow a^{-1}b^{-1} \in G$

Given equation $ax = b \quad \Rightarrow a^{-1}(ax) = a^{-1}b$

$\Rightarrow (a^{-1}a)x = a^{-1}b \quad \Rightarrow (e)x = a^{-1}b \quad \Rightarrow x = a^{-1}b$

Now $\quad ax = a(a^{-1}b) = (aa^{-1})b = (e)b = b$

$\therefore a^{-1}b$ is a solution of the equation $ax = b$

<u>We prove that it is a unique solution</u>

Let x_1, x_2 be two solutions of $ax = b$

$\Rightarrow ax_1 = b$ and $ax_2 = b \quad \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$

$\therefore$ The equation $ax = b$ has unique solution

Similarly we prove that $ya = b$ has unique solution

Hence proved

Idempotent Element: Let G be a group and $a \in G$. 'a' is said to be an idempotent element if $a^2 = a$.

Theorem: Let G be a group and $e \in G$. Show that 'a' is an idempotent element in G iff a = e.

Proof: Let G be a group and $e, a \in G$

Suppose a is an idempotent $\Rightarrow a^2 = a$

$\Rightarrow a.a = a.e \Rightarrow a = e \quad (\because \text{LCL})$

Again suppose $a = e$

$\Rightarrow a.a = a.e \Rightarrow a^2 = a \Rightarrow$ a is idempotent

Hence proved

Congruent modulo n

Let n be a positive integer and a, b $\in$ Z.

Then a is said to be congruent to b modulo n

if n divides a - b. It is denoted by $a \equiv b \pmod{n}$

$\therefore a \equiv b \pmod{n} \Leftrightarrow n / a - b$ **OR** $a - b = nq$ **for** $q \in Z$

Note : a divides b $\Rightarrow a / b$ **OR** $\frac{b}{a}$ **OR** $b = aq$ **for** $q \in Z$

<u>Examples</u>

1. $32 \equiv 2 \pmod{5} \quad \because \frac{32-2}{5} = \frac{30}{5} = 0$

2. $-47 \equiv 7 \pmod{9} \because \frac{-47-7}{9} = \frac{-54}{9} = 0$

3. **is** $26 \equiv 5 \pmod{4}$ **?**

No. $\because \frac{26-5}{4} = \frac{21}{4} \neq 0$ $(\because$ **4 does not divides 21**$)$

Prove that the relation congruent modulo n is an equivalence relation on Z.

$\mathbf{Problem:}$ Let $a \in Z$, Z is the set of Integers.

1. <u>Reflexive Relation</u>

$$\because \quad n / 0 \Rightarrow n / a-a$$

$$\Rightarrow a \equiv a \pmod{n} \qquad \because a \equiv b \pmod{n} \Leftrightarrow n / a-b$$

2. <u>Symmetric Relation</u>

Let $a \equiv b \pmod{n} \Rightarrow n / a-b$

$$\Rightarrow a-b=nq,\ q \in Z \qquad \Rightarrow b-a=n(-q),\ -q \in Z$$

$$\Rightarrow b-a=n(p),\ p \in Z\,[\because -q=p] \Rightarrow b \equiv a \pmod{n}$$

$$\therefore a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$$

3. <u>**Transitive Relation**</u>

Suppose that $a \equiv b \pmod{n}$ **and** $b \equiv c \pmod{n}$

$\because a \equiv b \pmod{n} \Rightarrow n / a - b,$

$\because b \equiv c \pmod{n} \Rightarrow n / b - c,$

$\Rightarrow n / (a - b) + (b - c) \Rightarrow n / a - c \quad \Rightarrow a \equiv c \pmod{n}$

$\therefore a \equiv b \pmod{n} \;\&\; b \equiv c \pmod{n} \quad \Rightarrow a \equiv c \pmod{n}$

$\therefore$ **The congruent modulo n is an equivalence relation.**

Hence Completed.

RESIDUE CLASSES

The equivalence classes under the relation congruent modulo n on Z are called residue classes modulo n.

NOTE

1. **The residues class containing an inter a is denoted by $[a]$ OR $\bar{a}$.**
2. **The set of all residue classes modulo n is denoted by Z_n.**
3. **If n is a positive integer then we write $Z_n = \{\bar{0}, \bar{1}, \bar{2} \cdots\cdots\cdots\cdots \overline{n-1}\}$ and $o(Z_n) = n$**
4. **If $a \in Z$ then $\bar{a} = \bar{r} \in Z_n$, where r is the remainder of a when divided by n $\left(\because \frac{\bar{a}}{n} = \bar{r}\right)$**
5. **The set $\{\bar{0}, \bar{1}, \bar{2} \cdots\cdots\cdots\cdots \overline{n-1}\}$ is called the complete set of residue classes modulo n.**
6. **The set $\{0, 1, 2 \cdots\cdots\cdots\cdots n-1\}$ is called the complete set of <u>least positive</u> residue classes modulo n.**

Example

We know that $\mathbf{Z_n} = \left\{ \overline{0}, \overline{1}, \overline{2}, \overline{3} \cdots\cdots\cdots \overline{\mathbf{n}-1} \right\}$

The elements of $\mathbf{Z_6}$ are $\left\{ \overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5} \right\}$

Here $\left(\because \mathbf{n} = 6 \Rightarrow \textbf{modulo } 6 \right)$

$$\overline{0} = \left\{ \cdots\cdots -12, -6, 0, 6, 12, \cdots\cdots \right\}$$

$$\overline{1} = \left\{ \cdots\cdots -13, -7, 1, 7, 13, \cdots\cdots \right\}$$

$$\overline{2} = \left\{ \cdots\cdots -14, -8, 2, 8, 14, \cdots\cdots \right\}$$

$$\overline{3} = \left\{ \cdots\cdots -15, -9, 3, 9, 15, \cdots\cdots \right\}$$

$$\overline{4} = \left\{ \cdots\cdots -16, -10, 4, 10, 16, \cdots\cdots \right\}$$

$$\overline{5} = \left\{ \cdots\cdots -17, -11, 5, 11, 17, \cdots\cdots \right\}$$

$\because \overline{6} = \overline{0}, \quad \overline{7} = \overline{1}, \quad \overline{8} = \overline{2}$ **..... etc repeated.**

Let S be a semigroup. If for $x,y \in S$, $x^2y = y = yx^2$ prove that S is an abelian group.

Let S be a semigroup and $x,y \in S$

Given condition $x^2y = y = yx^2 \left(\because ab = ba = a \Rightarrow b = e\right)$

$$\Rightarrow x^2 = e \quad \Rightarrow x.x = e \quad \Rightarrow x = x^{-1}$$

$\therefore x \in S \Rightarrow x = x^{-1}$**, similarly** $y \in S \Rightarrow y = y^{-1}$

Claim : <u>We prove that S is abelian.</u>

Now $x, y \in S \Rightarrow xy \in S$

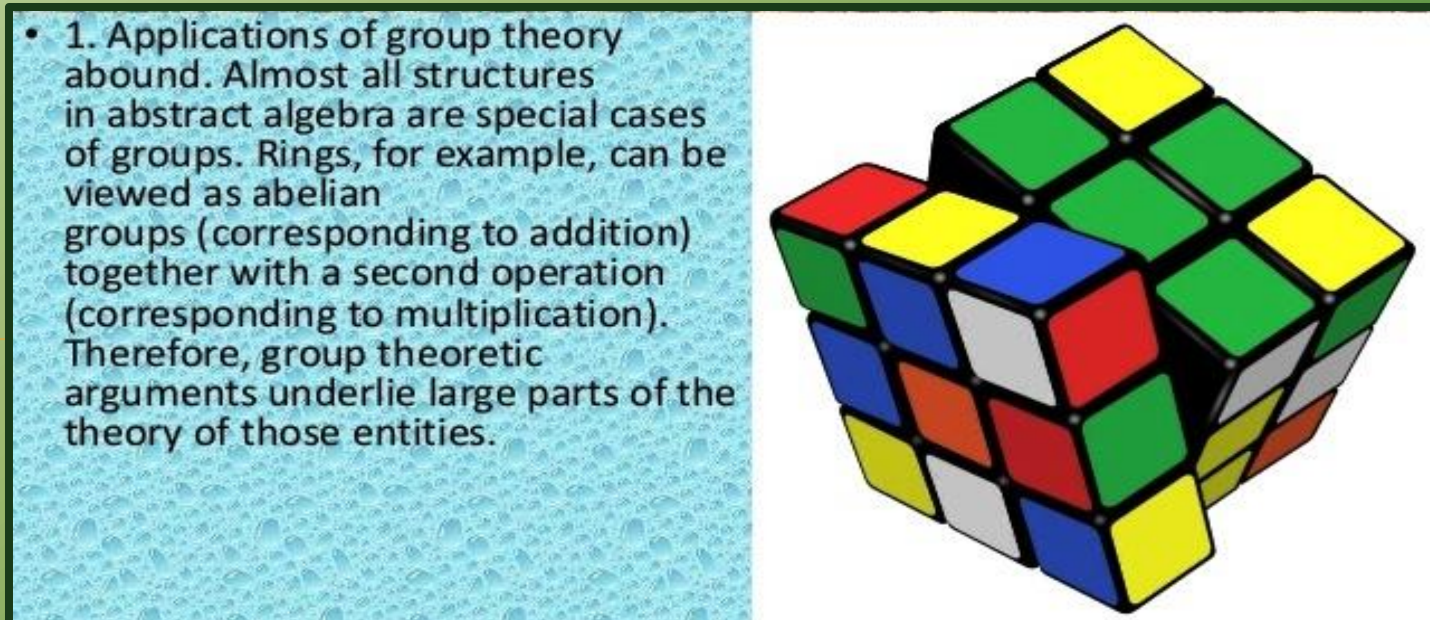
$$\Rightarrow \left(xy\right) = \left(xy\right)^{-1} = y^{-1}x^{-1} = yx$$

$\therefore$ **S is an abelian group.**

Hence Completed.

APPLICATIONS OF GROUP THEORY

Groups are vital to modern algebra; their basic structure can be found in many mathematical phenomena. Group theory has applications in physics, chemistry, and computer science, and even puzzles like Rubik's Cube can be represented using group theory.



CONCLUSION

I have concluded that PPT presentation is very useful in establishing objectives, illustrating concrete examples and statistical analysis.

I hope that utilizing all of these concepts through PPT slides helps to engage students with different types of learning styles.

I have added definitions, examples, problems and theorems of the chapter of Groups in brief and short methods.

Students may be demonstrated the ability to effectively utilize a variety of teaching techniques and classroom strategies to positively influence student learning.

S.K.B.R.COLLEGE AMALAPURAM