CLASS NOTES   GROUP THEORY

B.SC. (HONS.) MATHEMATICS
UNIVERSITY OF DELHI

CONTENTS

INTRODUCTION

Group theory of a branch of Mathematics that deals with the study of "Groups." In Mathematics, a group is defined as follows:

Definition   **Groups**

Let $G \neq \phi$ be a set and $+$ be any binary operation on G that assigns to each ordered pair (a, b) of G an element $a + b$ in G, then G forms a group under the operation $+$ if the following properties hold:

1. Closure: For all elements a, b in G, the operation $a + b$ belongs to G,
2. Associativity: For all elements a, b, c in G, the operations $a + (b + c)$ and $(a + b) + c$ are equal,
3. Existence of Identity: There exists an element in G, say e, such that $a + e = a = e + a$ for each element a in G,
4. Existence of Inverses: For each a in G, there exists a unique element b in G such that $a + b = e = b + a$.

A group is generally denoted by the notation $(G, +)$.

Definition   **Abelian Groups**

Let $(G, +)$ be a group. Then, if the operations $a + b$ and $b + a$ are equal for all a, b in G, *i.e.*, if Associativity holds in the group, then it is called an **Abelian Group**. Otherwise it is called a **Non-abelian Group.**

Below, a list of set-and-operations is given, along with whether they form a group or not:

e.g.   **Example**

The set $F = \{a_0 x^n + a_1 x^{-1} + \cdots + a_n : a_i \in \mathbb{R} \ \forall \ i = 1, 2, \ldots, n\}$ forms a group under function addition.

Table 1: A list of common set-operation combinations.

Set	Operation	Closure	Associativity	Identity	Inverses	Group	Abelian
$\mathbb{N}$	Addition	✔	✔	✗	○	✗	○
$\mathbb{N}$	Subtraction	✗	○	○	○	✗	○
$\mathbb{N}$	Multiplication	✔	✔	✔	✗	✗	○
$\mathbb{N}$	Division	✗	○	○	○	✗	○
$\mathbb{Z}$	Addition	✔	✔	✔	✔	✔	✔
$\mathbb{Z}$	Multiplication	✔	✔	✔	✗	✗	○
$\mathbb{Q}$	Addition	✔	✔	✔	✔	✔	✔
$\mathbb{Q}$	Multiplication	✔	✔	✔	✗	✗	○
$\mathbb{R}$	Addition	✔	✔	✔	✔	✔	✔
$\mathbb{R}$	Multiplication	✔	✔	✔	✗	✗	○

Solution. To prove that a certain set forms a group under the given operation, we need to prove the four properties mentioned above for all elements of the set. In this example, clearly, if we let $f_1 = \sum_{i=0}^{n} a_i x^{n-i}$, $f_2 = \sum_{i=0}^{n} b_i x^{n-i}$, and $f_3 = \sum_{i=0}^{n} c_i x^{n-i}$ belong to F, then the sum $f_1 + f_2 = \sum_{i=0}^{n} (a_i + b_i) x^{n-i}$ will also belong to F as the coefficients still belong to $\mathbb{R}$ (since $\mathbb{R}$ is closed under addition). Hence, closure holds for this set.

Similarly, we have, for each f_1, f_2, and f_3,

$$(f_1 + f_2) + f_3 = \sum_{i=0}^{n}[(a_i + b_i) + c_i]x^{n-i} = \sum_{i=0}^{n}[a_i + (b_i + c_i)]x^{n-i} = f_1 + (f_2 + f_3),$$

as addition is associative in $\mathbb{R}$, and hence Associativity also holds for the set F. Finally, we have $f_0 = 0x^n + 0x^{n-1} + \cdots + 0$ such that $f_i + f_0 = f_i = f_i + f_0$ for every $f_i \in F$, therefore identity exists. Also, for each $f_i = \sum_{i=0}^{n} a_i x^{n-i}$, we have $-f_i = -\sum_{i=0}^{n} a_i x^{n-i}$ such that $f_i + (-f_i) = f_0 = -f_1 + f_1$, hence inverses exist. And therefore, F forms a group under function addition,

CAYLEY'S TABLE

Cayley's table is a way to represent the group operation of a finite group using a square table. Each row and column in the table corresponds to an element of the group, and the entry at the intersection of a row and column represents the result of applying the group operation to the corresponding elements. Judging by the table, we can also tell if the given set forms a group or not. For example, if we consider the set $G = \{1, -1, \iota, -\iota\}$ with the operation of multiplication, then the following Cayley's Table can be formed.

$\times$	①	-1	ι	$-\iota$
①	①	-1	ι	$-\iota$
-1	-1	1	$-\iota$	ι
ι	ι	$-\iota$	-1	1
$-\iota$	$-\iota$	ι	1	-1

We see that closure holds in this table, as all elements belong to G itself. Associativity already holds as multiplication is associative in $\mathbb{C}$. The identity can be found by the Cayley's Table as well. We refer to the column that is in exact order as the header column. Then, the first element in that column is the identity. Likewise for rows as well. In the above case, we see that the identity is 1. And finally, since there is the identity element in each row and column, we conclude that inverses exist as well. Hence $(G_1, \times)$ forms a group.

Inverses. As for the inverses, another table can be formed as follows:

$$
\begin{array}{c|c}
x & x^{-1} \\
\hline
1 & 1 \\
-1 & -1 \\
\iota & -\iota \\
-\iota & \iota
\end{array}
\quad \left.\vphantom{\begin{array}{c} 1 \\ 1 \\ 1 \\ 1\end{array}}\right\} \text{Self Inverse Elements}
$$

ORDERS

Order of a group. The order of a group is the number of elements present in it, and is denoted by $|G|$. For example, in the above example, the order of $G = \{1, -1, \iota, -\iota\}$ is 4.

Order of an element. Order of an element a of a group G is the smallest positive integer n such that $\underbrace{a + a + \cdots + a}_{n \text{ times}} = e$ where e is the identity of G, and $+$ is the operation. Mathematically, we write $|a| = n$.

> **Observations**
>
> 1. Order of identity e is 1.
> 2. Identity element is always self inverse.
> 3. If the order of an element is 2, then the element is self-inverse, and vice-versa.
> 4. $|a| = |a^{-1}|$.
> 5. If $\exists\, a \in G$ such that $|a| = |G|$, then G is called a **Cyclic Group** generated by a, denoted by $G = \langle a \rangle$.

THE SET OF SQUARE MATRICES

Let S be the collection of all 2×2 matrices with entries coming from $\mathbb{R}$, *i.e.*,

$$
S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}
$$

which is often represented as $M_2(\mathbb{R})$. Now, let $M_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ and $M_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$ such that $M_1, M_2 \in S$. Then $M_1 + M_2 = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix}$ which must also belong to S. Since matrix addition is associative, we conclude that S is also associative under matrix addition. And clearly, we have $M_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ such that $M_i + M_0 = M_i = M_0 + M_i$ for any $M_i \in S$. And finally, we have $-M_i$ for each $M_i \in S$ such that $M_i + (-M_i) = M_0 = -M_i + M_i$, thus inverses exist as well. And hence we get that S is a group under the operation of matrix addition. In fact, it is an Abelian Group!

SOME MORE MATRIX GROUPS

Following are some special types of sets based on matrices:

1. $\mathrm{GL}(2, \ \mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, ad \neq bc \right\}.$

2. $\mathrm{SL}(2, \ \mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}.$

and the following groups are formed for these sets:

1. $M_{\mathrm{m} \times \mathrm{n}}(\mathbb{R})$: Group w.r.t. matrix addition.
2. $\mathrm{GL}(2, \ \mathbb{R})$: Group w.r.t. matrix multiplication.
3. $\mathrm{SL}(2, \ \mathbb{R})$: Group w.r.t. matrix multiplication.