GROUP THEORY
DAY 1

• **Group:** A non-empty set coupled with a binary operation that satisfy the following axioms:

Let S be the non-empty set and '$\circ$' be the binary operation. Then,

1) **Associativity:** $a \circ (b \circ c) = b \circ (c \circ a) = c \circ (a \circ b)$. where $a, b, c \in S$.

2) **Inverses:** $a \circ \bar{a}^{-1} = e$ where $a, \bar{a}^{-1}, e \in S$.

3) **Identity:** $a \circ e = e \circ a = a$ $a, e \in S$.

} Existence Axioms.

• **Sets:** Set is a collection. e.g. Set of numbers, animals, etc.

$\mathbb{R} \Rightarrow$ Set of Real numbers.

$\mathbb{Z} \Rightarrow$ Set of Integers.

• **Matrices:** A $n \times m$ array of numbers [though they can (be) [shame] anything you want].

If M is a $n \times m$ matrix, $M = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & & a_{2m} \\ a_{31} & a_{32} & & & a_{3m} \\ \vdots & \vdots & & & \vdots \\ a_{n1} & \cdots & & & a_{nm} \end{bmatrix}$ where the a_{ij}^{th} entry belongs to the i^{th} row and the j^{th} column.

$n \equiv$ No. of rows
$m \equiv$ No. of Columns.

Addition: It is done Componet-wise.

e.g. For a 2×2 Matrix that has $\mathbb{R}$ entries,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} a+a' & b+b' \\ c+c' & d+d' \end{bmatrix}.$$

Multiplication: It is done by multiplying the row of one matrix with the Column of another Matrix.

e.g. For a 2×2 matrix, with $\mathbb{R}$ entries,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{bmatrix}.$$

Note: $AB \neq BA$.
It is non-Commutative.

* Modular Arithmetic: Performing addition, multiplication, division, and subtraction with a different base number.

General addition, etc. are in base 10.

However, choose whatever base you like but mention it while performing arithmetic.

∴ $a \equiv b \pmod{n}$ means "a is congruent to b modulo n", which means that "b is the remainder one gets if one divides a by b."

∴ $a \equiv b \pmod{n} \Rightarrow a = kn + b$. $\quad a, k, b \in \mathbb{R}$.

⇓ Division Algorithm

e.g. $2 \equiv 0 \pmod{2}$, $\quad 5 \equiv 5 \pmod{7}$, $\quad 9 \equiv 1 \pmod{8}$

Exercises.

1). Solve the following:

- $5 \pmod{4}$
- $3 \pmod{3}$
- $11 \pmod{4}$
- $15 \pmod{7}$
- $8 \pmod{9}$
- $11 \pmod{15}$
- $3^2 \pmod{3}$
- $4^{71} \pmod{5}$.
- $100^{100^{100}} \pmod{101}$

2) Solve the following:

- $\begin{bmatrix} 2 & 8 \\ 7 & 6 \end{bmatrix} + \begin{bmatrix} 11 & 1 \\ 14 & 7 \end{bmatrix}$.
- $\begin{bmatrix} 6 & 3 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 11 & 3 \\ 7 & 2 \end{bmatrix}$.
- $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
- $\begin{bmatrix} 8 & 1 \\ 9 & 0 \end{bmatrix} + \begin{bmatrix} 7 & 0 \\ 1 & 9 \end{bmatrix}$
- $\begin{bmatrix} 6 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 6 & 3 \\ 3 & 6 \end{bmatrix}$
- $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$