$\langle \mathbb{N}, + \rangle \qquad 2 = 2 + 2 + 2 = 6$

- <u>Composition Table / Cayley Table</u> :-

$*$; $S = \{a_1, a_2, \dots, a_n\}$

$*$	a_1	a_2	a_3	$\dots$	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	$a_1 * a_3$		$a_1 * a_n$
a_2	$a_2 * a_1$	$a_2 * a_2$	$\dots$		—
a_3	- -	- - -	- - -		—
$\vdots$					
a_n	$a_n * a_1$	$a_n * a_2$	$\dots$		$a_n * a_n$

$$\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 7 & 4 \\ 3 & 4 & 9 \end{array} \longrightarrow \frac{n^2-n}{2}$$

$$n^{\left(\frac{n^2-n}{2} + n\right)} = n^{\left(\frac{n^2+n}{2}\right)}$$

Total places to be filled $= \dfrac{n^2-n}{2} + n$ → diagonal

<u>05/02/18</u>

- <u>Identity element</u> :-

Let $*$ be a <u>binary operation</u> defined on a set S. Then an element $e \in S$ is said to be the identity element of S under $*$ if

$$a * e = a = e * a, \quad \forall\, a \in S.$$

Eg:- $e = 0$, in $\langle R, + \rangle$

$e = 1$, in $\langle R, \cdot \rangle$

$e = I_n$, in $\langle M_{n \times n}, \times \rangle$

$S = \mathbb{N} = \{1, 2, \ldots\}$

$\Rightarrow$ $a * b = \max(a, b)$ $\Rightarrow$ Identity element, $e = 1$ here

Let $a \in S$, then $a * e = \max(a, 1) = a$

$e * a = \max(1, a) = a$

$\Rightarrow$ $a \diamond b = a$

Let e be the identity, then

$e \diamond a = e \longrightarrow$ a contradiction if $a \neq e$.

Because according to the defn of identity $e \diamond a$ should be a.

$\Rightarrow$ $a \otimes b = a^b$

Let e be the identity, Let $a = 2$,

Then $a \otimes e = a$

i.e. $2 \otimes e = 2$

$\Rightarrow 2^e = 2$

$\Rightarrow e = 1$.

as per the definition of identity

$e \otimes a = a$

i.e. $1 \otimes 2 = 2$

$\Rightarrow 1^2 = 2 \longrightarrow$ a contradiction.

- Proposition :-

The identity element in a set under a specific binary operation is unique.

Proof :- Let e_1 & e_2 be two distinct identity element.
Considering e_1 as the identity in S, we get

$e_1 * e_2 = e_2 = e_2 * e_1$ —— ①

Again considering e_2 as the identity element we get,

$e_1 * e_2 = e_1 = e_2 * e_1$ —— ②

From ① & ② since $*$ is a binary operation

$e_1 = e_2$ which is a contradiction to our hypothesis.

Hence, proved.

- Inverse :-

Let $*$ be a binary operation defined on a set S and a is an arbitrary element in S. An element b ∈ S is said to be the inverse of a if

$a * b = e = b * a$

Eg:- ① in $\langle \mathbb{R}, + \rangle$ the inverse of a is '$-a$'.
② in $\langle \mathbb{R}, \cdot \rangle$ the inverse of any $a \neq 0$ is '$\frac{1}{a}$'.

The inverse of a is denoted by a^{-1}. (a superscript -1, not power) → symbol

2^{-1} in $\langle \mathbb{R}, + \rangle = -2$

2^{-1} in $\langle \mathbb{R}, \cdot \rangle = \frac{1}{2}$

Axiomes :-

1) $a^n = \underbrace{a * a * a * \cdots * a}_{n\text{-times}}$; $n \in \mathbb{N}$

Here $*$ is an associative binary operation in S.

2) $a^0 = e$, $\forall\, a \in S$.

$\left[\begin{array}{ll} 2^0 = 0 , & \text{in } \langle \mathbb{R}, + \rangle \\ 2^0 = 1 , & \text{in } \langle \mathbb{R}, \cdot \rangle \end{array} \right]$

$$a^{-n} = (a^{-1})^n = \underbrace{a^{-1} * a^{-1} * a^{-1} \cdots * a^{-1}}_{n\text{- times}}$$

$$2^{-3} = (2^{-1})^3 = (-2)^3 = (-2) + (-2) + (-2)$$
$$= -6 \quad \text{in } \langle \mathbb{R}, + \rangle .$$

- <u>Proposition - 2</u> :-

Let a be an arbitrary element in $\langle S, * \rangle$. Then the inverse of a is unique.

<u>Proof</u> :- Let a_1 & a_2 be two distinct inverse.

$$a * a_1 = e = a_1 * a$$
$$a * a_2 = e = a_2 * a$$
$$a * a_1 = a * a_2$$

$$a_1 * (a * a_1) = a_1 * (a * a_2)$$
$$\Rightarrow (a_1 * a) * a_1 = (a_1 * a) * a_2$$
$$\Rightarrow e * a_1 = e * a_2$$
$$\Rightarrow a_1 = a_2$$

$$\Rightarrow \quad 2x = 6$$
$$\Rightarrow \frac{1}{2} \cdot (2x) = \frac{1}{2} \cdot (6)$$
$$\Rightarrow \left(\frac{1}{2} \cdot 2\right) x = 3$$
$$\Rightarrow 1 \cdot x = 3$$
$$\Rightarrow x = 3$$

- <u>Group</u> :-

Let S is a non-empty set and $*$ is a binary operation. Then $\langle S, * \rangle$ is said to be a group if —

1) $*$ is associative
2) there exist the identity element e in S
3) for every $a \in S$, the inverse of a, ie a^{-1} exists in S.

12/02/18

» $a \times b \pmod n = c$ Remainder when ab is divided by n.

$\Rightarrow n \mid ab - c$

» $a + b \pmod n = d$

$\Rightarrow n \mid (a+b) - d$

» $a \pmod n = r$

$\Rightarrow n \mid a - r$

$n = 5$

$[0] / \bar{0} = \{ \ldots -15, -10, -5, 0, 5, 10, \ldots \}$

$\bar{1} = \{ \ldots -14, -9, -4, 1, 6, 11, \ldots \}$

$\bar{2} = \{ \ldots -13, -8, -3, 2, 7, 12, \ldots \}$

$\bar{3} = \{ \ldots -12, -7, -2, 3, 8, 13, \ldots \}$

$\bar{4} = \{ \ldots -11, -6, -1, 4, 9, 14, \ldots \}$

$\mathbb{Z}_5 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4} \}$

$\mathbb{Z}_5 = \{ 0, 1, 2, 3, 4 \}$

Groups

$\langle \mathbb{Z}, + \rangle$

$\langle \mathbb{R} - \{0\}, \times \rangle$

$\langle M_{m \times n}, + \rangle$

$\langle \mathbb{C}, + \rangle$

$\langle \mathbb{Q} - \{0\}, \times \rangle$

rational

Non-groups

$\langle \mathbb{N}, - \rangle$, $\langle M_{n \times n}, \times \rangle$