Recall :-

Def$^{\underline{n}}$ of Groups :- $(G, \cdot)$ such that

a) $\cdot : G \times G \to G$ $\quad (a \in G, b \in G$
$\quad a \cdot b \in G)$

b) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

c) $\exists\ 1_G \in G$ s.t $a \cdot 1_G = 1_G \cdot a = a$

The Identity

d) for every $a \in G$, $\exists\ b \in G$ s.t

$$ab = ba = 1_G$$

The Inverse of b

$b = a^{-1}$

$\mathbb{Z}/n\mathbb{Z}$:- Given $n \in \mathbb{N}$

$\sim$ is a relation on $\mathbb{Z}$ s.t

$a \sim b$ iff $n \mid a - b$

$\sim$ is an equivalence relation

$a \in \mathbb{Z}$

$$a + n\mathbb{Z} = \{ d \in \mathbb{Z} : n \mid d - a \}$$

For $0 \leq k \neq l \leq n-1$

$$k + n\mathbb{Z} \neq l + n\mathbb{Z}$$

$k + n\mathbb{Z} = l + n\mathbb{Z} \iff n \mid k - l$

$n > |k - l| \geq n$ $(\longrightarrow \longleftarrow)$

$0 + n\mathbb{Z}, \quad 1 + n\mathbb{Z}, \quad \ldots, \quad (n-1) + n\mathbb{Z}$

$a \in \mathbb{Z}$ $\quad a + n\mathbb{Z}$ $\quad a = nq + r$

$0 \leq r \leq n-1$

$$a + n\mathbb{Z} = r + n\mathbb{Z}$$

$\mathbb{Z}/n\mathbb{Z} := \{0+n\mathbb{Z}, 1+n\mathbb{Z}, \dots, (n-1)+n\mathbb{Z}\}$

$$(a+n\mathbb{Z}) + (b+n\mathbb{Z}) = (a+b)+n\mathbb{Z}$$

Well defined and satisfies all the group criterions

$(\mathbb{Z}/n\mathbb{Z}, +) \to 0+n\mathbb{Z}$

$(\mathbb{Z}/n\mathbb{Z}, +) \to a+n\mathbb{Z} \to (-a)+n\mathbb{Z} = (n-a)+n\mathbb{Z}$

$(G, \cdot)$ group. $g \in G$, $|g| = n$ is the smallest natural number s.t $g^n = 1$. $|g| = \infty$ possible

Ex :- G is a group. $g \in G$ s.t $|g| = n \in \mathbb{N}$, $|g^{-1}| = n$

Further Examples :-

1) Symmetric Group / Permutation Group :-

S is a set, $S_\Omega := \{ f : S \to S \text{ s.t } f \text{ is a bijection} \}$

$$\circ : S_\Omega \times S_\Omega \longrightarrow S_\Omega$$
$$f \circ g$$

$(S_\Omega, \circ)$ is a group.

$1_S / id_S : s \longmapsto s, \ \forall s \in S$

$f \in S_\Omega \quad f^{-1} \qquad f \circ f^{-1} = f^{-1} \circ f = 1_S$

$s \longrightarrow f(s) \qquad f(s) \to s$

Notation :- $\quad S := \{1, 2, \dots, n\}$

$$(S_\Omega = S_n, \circ)$$

$$S = \{1, 2, 3\}$$

$$S_3 := \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

$$\underset{f}{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}} \circ \underset{g}{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$ab = ba$

$$\begin{aligned} (f \circ g)(1) &= f(g(1)) \\ &= f(2) \\ &= 1 \end{aligned}$$

$$(f \circ g)(2) = f(g(2)) = f(3) = 3$$

$$(f \circ g)(3) = f(g(3)) = f(1) = 2$$

$$|S_n| = n!$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

$\searrow$ not abelian $n \geq 3$

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 3 & 4 & n-1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & & n \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

$S_3 := \{$

$$f : \{1,2,3\} \longrightarrow \{1,2,3\}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \equiv (1\ 2\ 3)$$

$f(1) = 2$

$f(2) = f(f(1)) = 3$

$f(3) = f^3(1) = 1$

$(1\ 2)(3)(4)(5)$

$= (1\ 2)$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \equiv (1\ 2)\ (3) = (1\ 2) \in S_3$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 6 & 5 & 7 \end{pmatrix} = (1\ 2\ 3\ 4)(5\ 6)(7)$$

$\in S_7$

↳ 2 cycles / transposition

$f \quad (1\ 12\ 8\ 10\ 4)(2\ 13)(3)(5\ 11\ 7)(6\ 9)$

$$\equiv \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 3 & 1 & 11 & 9 & 5 & 10 & 6 & 4 & 7 & 8 & 2 \end{pmatrix} \in S_{13}$$

$$\underbrace{(1\,2)(3)(4)}_{f} \circ \underbrace{(1\ 2\ 3\ 4)}_{g} = (1)(2\ 3\ 4) = (2\ 3\ 4)$$

$f(g(1)) = f(2) = 1$

$$(1\ 2) \circ (1\ 2) = (1)$$

$$(1\ 2)\quad(1\ 2\ 3) = (2\ 3)$$

$$(1\ 2)^{(3\,4)}$$