Note: ~~But~~ $\mathbb{Z}_n$ is not a group, since inverse of every element does not exist in $\mathbb{Z}_n$ as can be seen from the example below:

Take $n=4$, then $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$.

In $\mathbb{Z}_4$, for the element $\bar{2} \in \mathbb{Z}_4$, there does not exist any element $\bar{y} \in \mathbb{Z}_4$ such that

$$\bar{2} \cdot \bar{y} = \bar{1} = \bar{y} \cdot \bar{2}.$$

Hence $\mathbb{Z}_4$ is not a group.

let us Consider the set consisting of those elements in $\mathbb{Z}_n$, whose inverse exist in $\mathbb{Z}_n$ and forms a multiplicative group. Let this set be denoted by $\mathbb{Z}_n^*$.

Now, for any element $\bar{x} \in \mathbb{Z}_n$, if inverse of $\bar{x}$ exists then

$$\bar{x} \cdot \bar{y} = \bar{1} = \bar{y} \cdot \bar{x}$$, where $\bar{y}$ is the inverse of $\bar{x}$.

i.e. $\bar{x} \cdot \bar{y} = \bar{1}$

$\Rightarrow \overline{xy} = \bar{1}$

$\Rightarrow xy \equiv 1 \pmod{n}$

Since, from the knowledge in Number Theory related to Congruences, we know that the equation

$ax \equiv 1 \pmod{n}$ has a solution iff

g.c.d $(a, n) = 1$. i.e. Greatest Common divisor of (a, n) is 1.

Therefore, $xy \equiv 1 \pmod{n}$ has an inverse if

$(x, n) = 1$.

Hence, for any $\bar{x} \in \mathbb{Z}_n$, inverse of $\bar{x}$ exists iff

$(x, n) = 1$.

~~By Euler function~~ defined The no. of such elements are denoted by $\phi(n)$, where ϕ is the Euler function.

i.e. $\phi(n)$ = no. of +ve integers less than n and co-prime to n.

Hence order of multiplicative group $\mathbb{Z}_n^*$ is $\phi(n)$.

14.) Consider the set $G = \{e, a, b, c\}$ such that

$$a^2 = b^2 = c^2 = e \quad \text{and} \quad ab = ba = c,$$
$$bc = cb = a \quad \text{and} \quad ac = ca = b.$$

Then it can be easily checked that G forms a group with identity element 'e' and inverse of every element is itself that element. Also from the definition of group G, it can be checked that it is abelian.

Hence G is abelian group.

This group is known as Klein's four Group.

15.) Consider the following matrices of order 2×2

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

Then G forms a nonabelian group of order 8 under multiplication of matrices. This group is known as the group of quaternions.

Further, let $\pm e = \pm\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\pm i = \pm\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, $\pm j = \pm\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and

$$\pm k = \pm \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

Then it can be easily checked that $i^4 = e$, $ij = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = k$.,

Similarly, $ji = -k$, $jk = i$, $kj = -i$, $ki = j$ and $ik = -j$.

Hence G forms a nonabelian group with identity $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

16) Let X be a nonempty set and let G be the set of all bijective mappings from X to X.

i.e. $G = \{ f : X \to X \mid f \text{ is bijective function} \}$

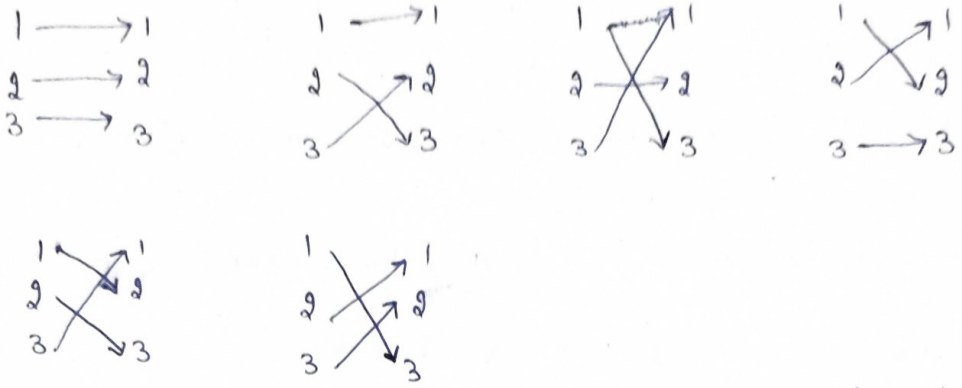
Then G is a group under the usual composition of functions. This group is known as Permutation group or Symmetric group. and is denoted by S_X.

If X is a set having n elements i.e. $|X| = n$ then no. of bijective functions from $f: X \to X$ are $n!$.

Therefore, order of Permutative group is $n!$ i.e. $o(S_X) = n!$ and in this case group is denoted by S_n.

Consider the case for $n = 3$.

Let $X = \{1, 2, 3\}$ then no. bijective functions are given by



Let e. These permutations are denoted in the following nice manner respectively!

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

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

and in cyclic form also written as respectively:

$e = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$, $(2\ 3)$, $(1\ 3)$, $(1\ 2)$, $(1\ 2\ 3)$, $(1\ 3\ 2)$.

Here the image of each element in the row is the next element and the image of last element is the first element.

Also the fixed element is not mentioned in the cycle as

$\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$ means 1 remains find but $2 \to 3$ and $3 \to 2$,

so in cyclic form it is written as $(2\ 3)$.

Composition of two permutations is defined as the usual Composition of functions from right to left shown in following example:

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

where from right $1 \to 3$ and then left $3 \to 2$

$\therefore$ $1 \to 2$ and so on.

identity element is obviously $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$.

For the inverse of any element say

$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, find by the following nice manner:

Write bottom row on the top place and top row on the bottom place i.e. interchange the position of rows i.e.

$\begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix}$ will be the inverse of a, which

can be rewritten also in standard form as:

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

such that

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

Hence for $X = \{1, 2, 3\}$, the set of bijections from a group denoted by S_3 and is of order $3! = 6$.

also if $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

then $a^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $a^3 = e$, $b^2 = e$, $ab = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

and $a^2b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

Hence $S_3 = \{e, a, b, a^2, ab, a^2b\}$.