Basic Def$\frac{n}{=}$ etc. :-

1) Def$\frac{n}{=}$ of Groups :-

A group G is a set with a binary operation

• $\cdot : G \times G \to G$ s.t

$f(a) = b$

$f(a) = c$

$b = c$

Assosicativity ← a) $(g \cdot h) \cdot e = g \cdot (h \cdot e)$

Existence of identity ← b) $\exists\ 1 \in G$ s.t $g \cdot 1 = 1 \cdot g = g$

Existence of Inverse ← c) For every $g \in G$ $\exists\ h \in G$ s.t
$$gh = hg = 1$$

Additionally if for all g and h in G,
$$gh = hg$$
Then we define the group to be an Abelian Group

Remark :-

• Since the operation is associative

$a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_n$ is well defined

• The identity 1 is unique, i.e. if $\exists\ e \in G$ s.t
$$ge = g \quad , \forall g \in G$$
then $e = 1$

• Given $g \in G$, its inverse is unique, and hence we can define a notation for the inverse, i.e. g^{-1}

• In a group we have cancellation law :-
$$gh_1 = gh_2 \Rightarrow h_1 = h_2$$
$$g_1 h = g_2 h \Rightarrow g_1 = g_2$$
(This proves that (left) right inverse is unique $\Rightarrow$ (left) inverse = right inverse)

2) Def^n of Order :-

Let G be a group. Then for any $g \in G$ "Order" of g is the smallest natural number n

$$g^n = 1$$

Remark :- An element has order 1 iff it is the identity.

Remark :- Order of an element might be ∞

Example :-

1) $\{1\}$ s.t $1 \cdot 1 = 1$

2) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q} \setminus \{0\}, \times)$

3) $\mathbb{Z}/n\mathbb{Z} := \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

$\{ \sim : \mathbb{Z} \to \mathbb{Z}$, $a \sim b$ iff $n \mid a-b$

$a \sim a$

$a \sim b \Rightarrow b \sim a$

$\sim b,\ b \sim c \Rightarrow a \sim c$

$0 \le k \le n-1$

$$\bar{k} := \{ a \in \mathbb{Z} \text{ s.t } a \sim k \equiv n \mid a-k \}$$

$0 \le a \le n-1$, $0 \le b \le n-1$, $\bar{a} + \bar{b} := \overline{(a+b) \pmod n}$

This means the remainder upon dividing $a+b$ by n

$$\left.\begin{aligned} \bar{a} &= \bar{c} \\ \bar{b} &= \bar{d} \end{aligned}\right\} = \frac{\bar{a} + \bar{b}}{\overline{(a+b) \pmod n}} = \frac{\bar{c} + \bar{d}}{\overline{(c+d) \pmod n}}$$

$k \in \overline{(a+b) \pmod n}$

$\Leftrightarrow n \mid a+b-k$ $\qquad$ $n \mid a-c$, $n \mid b-d$

$\Leftrightarrow n \mid c+d-k$

$\Leftrightarrow k \in \overline{(c+d) \pmod n}$

$0 \le a \le n-1$

$$\bar{a} + \overline{(n-a)} = \bar{0}$$

Ex :- Consider $\mathbb{Z}/6\mathbb{Z}$ and find order of $\bar{2}$.

Thus we get the group $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$

We can define another operation

$$\bar{a} \cdot \bar{b} = \overline{ab \pmod n} \quad (\text{the id. is } \bar{1})$$

Under this operation $\mathbb{Z}/n\mathbb{Z}$ is never a group

$\mathbb{Z}/6\mathbb{Z}$, $\bar{2}$

When / for which n is $\left(\mathbb{Z}/n\mathbb{Z}, \cdot\right)$ a group.

Note that $\bar{0} \cdot \bar{a} = \bar{0} \quad \forall\, 0 \le a \le n-1$

So $\bar{0}$ has no multiplicative inverse for any n.

Thm :- $\mathbb{Z}/n\mathbb{Z} \setminus \{\bar{0}\}$ is a group iff n is a prime

Proof → $\mathbb{Z}/n\mathbb{Z} \setminus \{\bar{0}\}$ be a group under multiplicⁿ.

Let on contrary n be composite $\Rightarrow n = ab$, $a \ne 1$, $b \ne 1$

Let $\bar{a}$ has a inverse $\bar{x}$

$\Rightarrow \bar{a} \cdot \bar{x} = \bar{1} \Rightarrow ax \equiv 1 \pmod n$

$\Rightarrow ax - 1 = nk \Rightarrow ax - nk = 1$

Let $(a, n) = d \Rightarrow d \mid a,\ d \mid n \Rightarrow d \mid ax - nk \Rightarrow d \mid 1 \Rightarrow d = 1$ $(\rightarrow\leftarrow)$

$\Rightarrow a = 1$

Conversely, let n be a prime; then take any $\bar{a}$, $0 < a \leq n-1$

$$\Rightarrow \underbrace{(a,n) = 1 \Rightarrow ax+ny = 1}_{\text{Bezout}} \Rightarrow ax \equiv 1 \pmod{n}$$

$$\bar{a} \cdot \bar{x} = \overline{ax \pmod{n}} = \bar{1}$$

$$\bar{x} \cdot \bar{a} = \overline{xa \pmod{n}} = \bar{1}$$

Remark :- Consider $\mathbb{Z}/n\mathbb{Z}$. You can define $\bar{k}$ for any $k \in \mathbb{Z}$

$$\bar{k} := \{ a \in \mathbb{Z} \text{ s.t } a \sim k \Leftrightarrow n \mid a-k \}$$

$$\bar{a} + \bar{b} = \overline{a+b} \qquad \bar{a} = \bar{0} / \bar{1} / \cdots / \overline{n-1}$$

$$\bar{a} \cdot \bar{b} = \overline{ab}$$