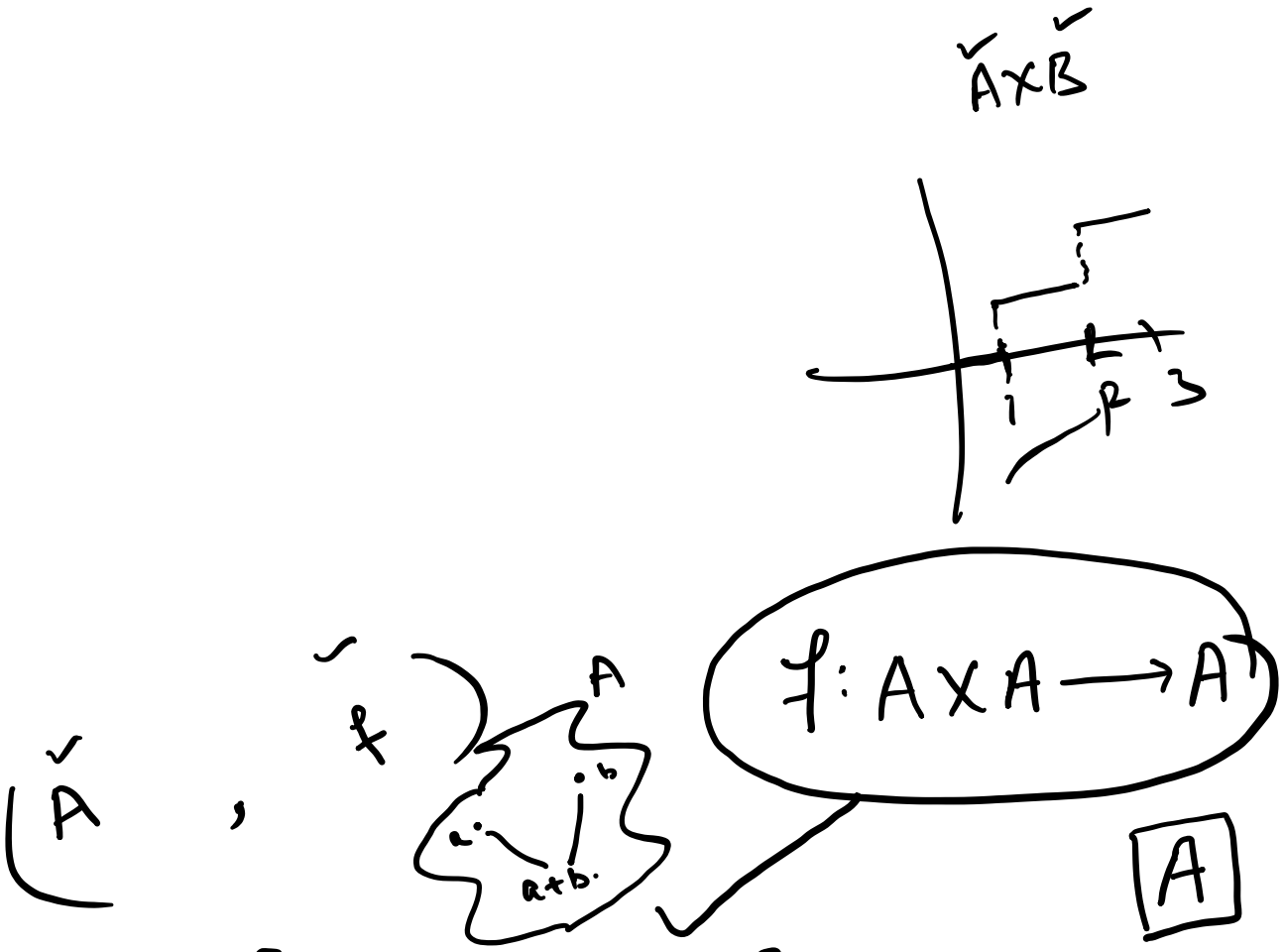


Def: [Binary operation]

A binary operation '$*$' in a set A is a function from $A \times A \to A$.

$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

Eg: Addition is a binary operation on $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.

but negation is not a binary operation

Also Subtraction is not a binary operation on $\mathbb{N}$.

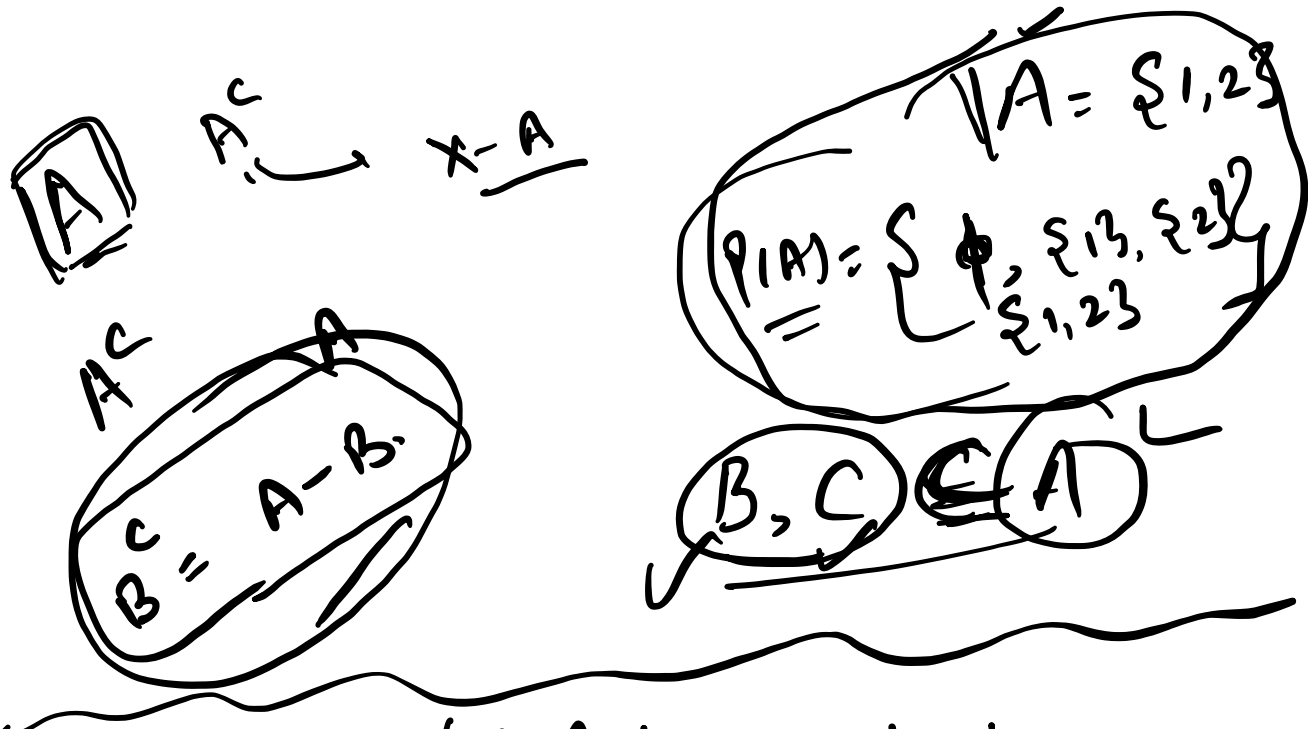
$-: \mathbb{N} \times \mathbb{N} \to ?$

$-(2,3) = 2-3 = -1 \notin \mathbb{N}$ (2,3.)

Eg 2: Union, intersection, difference are binary operations on $P(A)$ for any set A.

$P(A)$ (power set)

:= Collection of all subsets of A.



Let A be a set. Let $*$ be a function on $A \times A \to A$

i) Closure: if $\forall\ a, b \in A$

$\Rightarrow a * b \in A$

(A is closed under $*$)

All binary operations are closed.

as $* A \times A \to A$.

#

Associativity:

If $\forall\ a, b, c \in A$

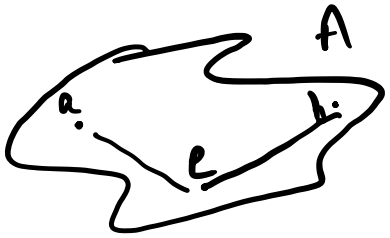
$\Rightarrow (a * b) * c = a * (b * c)$

Neutral element (Identity)

$(A, *)$

If $\exists\ e \in A$ s.t

$\forall a \in A: \quad a * e = e * a = a$



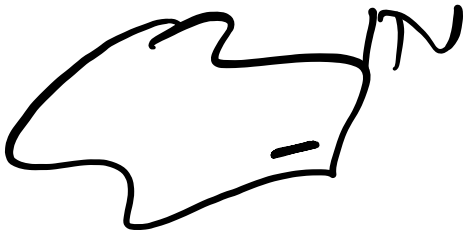
Inverse:

$$\forall \; a \in A; \quad \exists \; b \in A$$

s.t $\quad a * b = b * a = e$

where e is the identity of A.

Groupoid:



A non empty set A, together with a binary operation '*' ie (A, *) - pair is called groupoid.

Eg: Let E be a set of even numbers. Then (E, +) is a groupoid.

Semi-group:

Let A be a non-empty set. Then the algebraic structure $(A, *)$, where $*$ is a binary operation on A, is called Semi-group if the operation $*$ is associative.

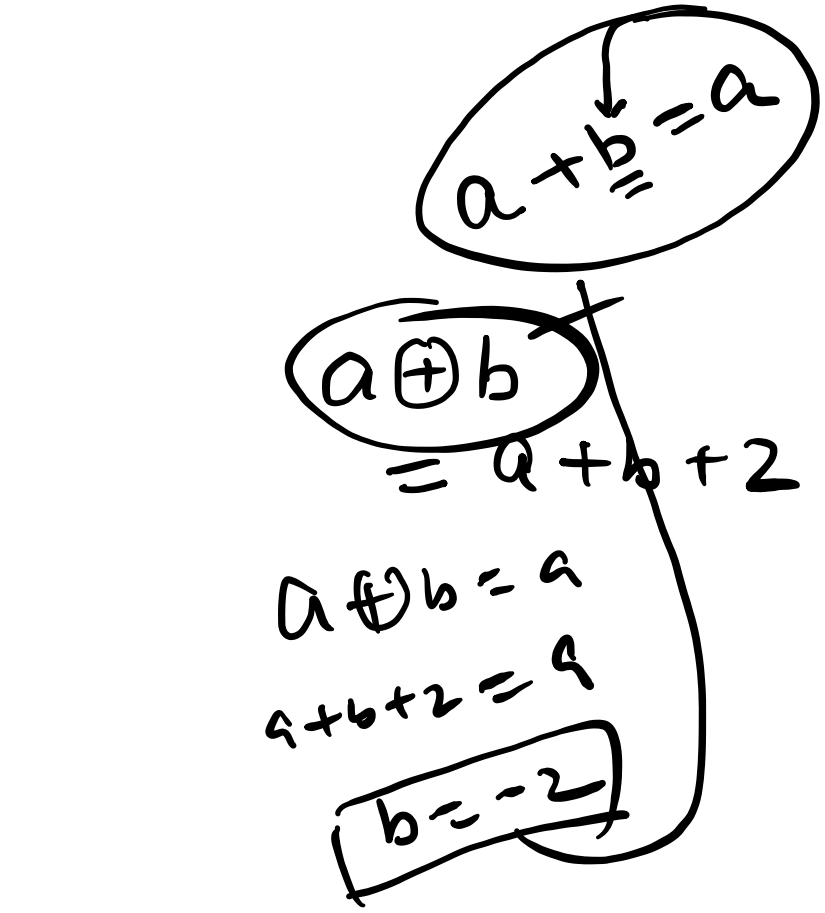
Eg: $(\mathbb{N}, +) \longrightarrow$ Semi-group.

$(\mathbb{N}, \times) \longrightarrow$ Semi group

Monoid: A semi-group $(M, *)$ is a monoid if it has the neutral (identity) element.

Eg: $(\mathbb{Z}', +) \longrightarrow$ $e \in \mathbb{Z}'$, $a + e = e + a = a$.

$(\mathbb{Z}', +)$ is monoid as $\exists\ 0 \in \mathbb{Z}'$, $a + 0 = 0 + a = a$ $\forall\ a \in \mathbb{Z}'$



Group:

Def! A group is an algebraic structure $(G, *)$; in which the (binary) operation $*$ on G satisfies:

[G-0: $\forall a, b \in G \Rightarrow a * b \in G$.

G-1: $\forall\ a, b, c \in G$

$\Rightarrow a * (b * c) = (a * b) * c$

G-2: $\exists\ e \in G:\quad a * e = e * a = a$

G-3: $\forall\ a \in G:\quad \exists\ b \in G$

s.t $a * b = b * a = e$

$b = a^{-1}$

$0 \times ? = 1$

Examples:

(i) $(\mathbb{Z}, +)$ ✓

(ii) $(\mathbb{R}, +)$ ✓

(iii) $(\mathbb{R}, \times)$ ✗

(iv) $(\mathbb{Z} - \{0\}, \times)$ ✗

(v) $(\mathbb{N}, +)$ ✗

(vi) $(\mathbb{R} - \{0\}, \times)$ ✓

(Commutative:) if $\forall\ a, b \in A$

$\Rightarrow a * b = b * a$

(Commutative group) or (Abelian group.)

Let $(G, *)$ be a group. Then $(G, *)$ is called an abelian group if

$*$ is commutative operation

eg: $(\mathbb{Z}, +)$ is an abelian group.

$(\mathbb{Z}, \cdot)$ NOT $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}_{2\times 2} : ad - bc \neq 0 \quad a, b, c, d \in \mathbb{R} \right\}$

$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$\begin{bmatrix} a & -b \\ -c & a \end{bmatrix}$ ✓

$|AB|$

$|A||B|$.

$A^{-1} = \frac{1}{(ad-bc)} \begin{bmatrix} & \\ & \end{bmatrix}$ $= \begin{bmatrix} & \\ & \end{bmatrix}$

$a_1 \neq 0$
$a_{12} \neq 0$

$(G, *)$

\# A group G is said to be finite group if the no. of elements in G is finite.
otherwise G is an infinite group.

For eg: $(\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{R} - \{0\}, \times)$ → infinite groups

$G = \{1, -1\}$ is a finite group under multiplication.

Order of a finite group:

The order of a (finite) group G means the number of elements in the set G; denoted as $O(G)$ or $|G|$.

$G = \{1, -1\}$; $O(G) = 2$

$\boxed{i^2 = -1}$

Eg: Show that the set $G = \{1, -1, i, -i\}$ where $i^2 = -1$; is an abelian group wrt multiplication.

Sol: : Composition table : Right

Left	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

$i \times (-i) = 1$

$a \cdot e = e \cdot a = a$

(Clearly $\forall\ a, b, c \in G$;

$a * (b * c) = (a * b) * c.$

Image of $1 \longrightarrow 1$

$i \longrightarrow -i$

$-i \longrightarrow i$

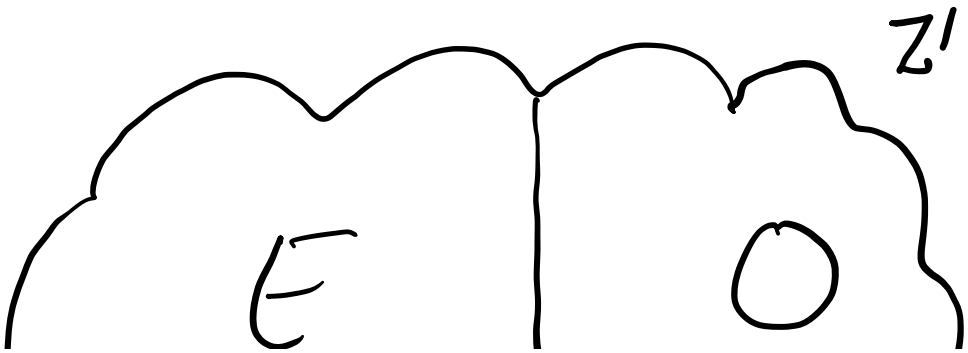
$-1 \longrightarrow -1$

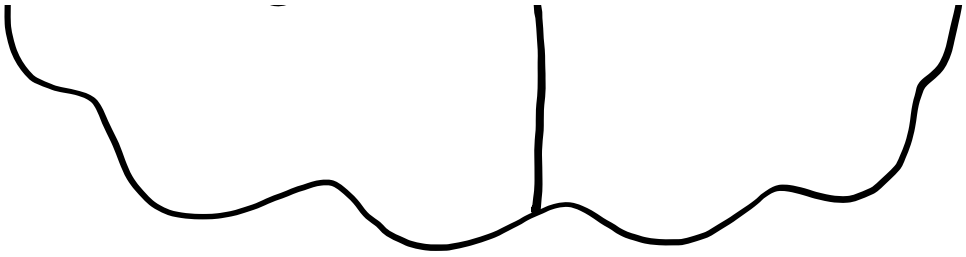
$x^n = 1$

Let $G = \{1, \omega, \omega^2, \omega^3, \cdots \omega^{n-1}, \}$ $\omega^n = 1$;

Then G is a group under multiplication.

Moreover G is an abelian group.

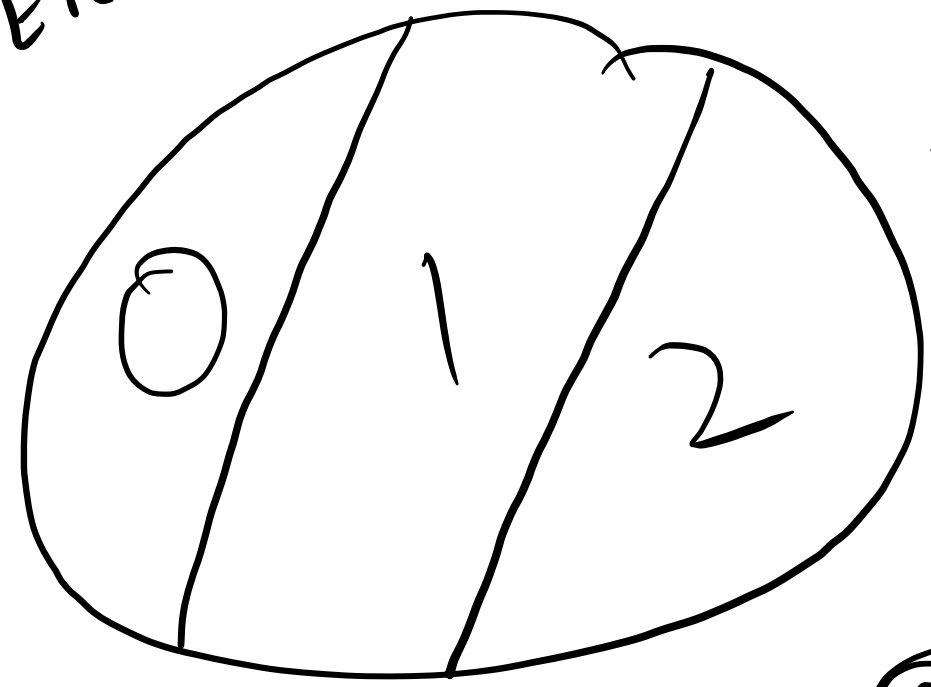




$E \cup O = Z'$.

$E \cap O = \phi$.

partition



$a \in Z'$

Let Z' be a set of integers. Let us divide Z' into n equivalence (partition) classes: or:

$$\bar{0} = \{ m \in \mathbb{Z}' : m = n\ell_1 \text{ for some } \ell_1 \}$$

$$\bar{1} = \{ m \in \mathbb{Z}' : m = n\ell_2 + 1 \text{ for some } \ell_2 \}$$

— — — — —

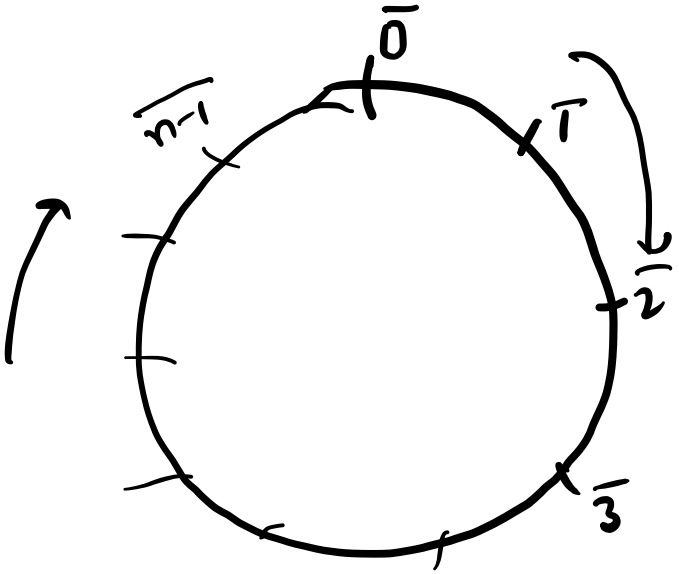
$$\overline{n-1} = \{ m \in \mathbb{Z}' : m = n\ell_n + (n-1) \text{ for some } \ell_n \text{ integer} \}$$

Note $\bar{n} = \bar{0}$

Construct a set $= \{\bar{0}, \bar{1}, \bar{2}, \cdots \overline{n-1}\}$

denoted by $\mathbb{Z}_n$.

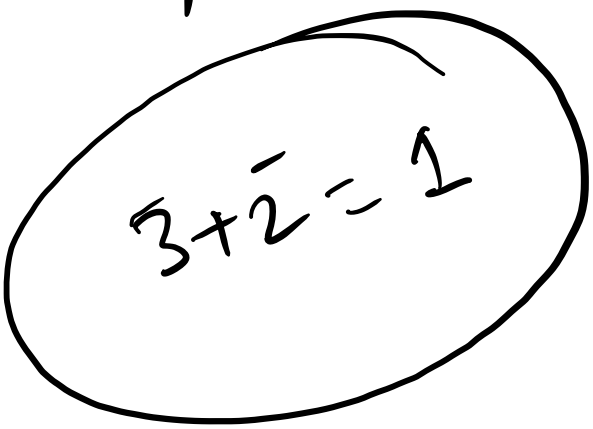
Also $\overline{n+1} = \bar{1}$ and so on

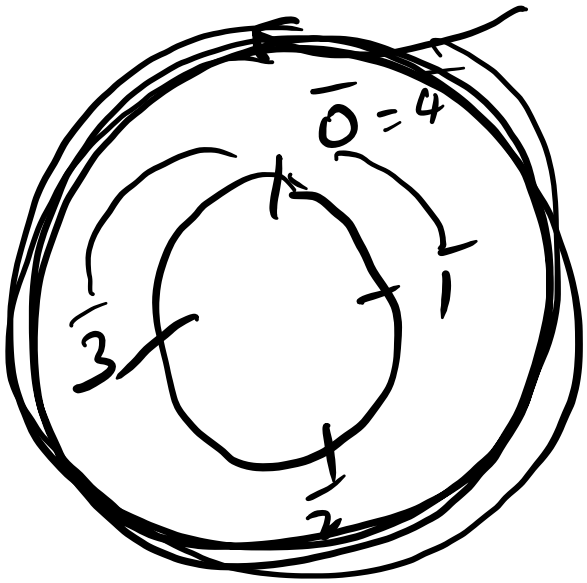


$\bar{3}$, 3

for eg:

Z_4





Defini. $+_n$: Addition under modulo 'n'.

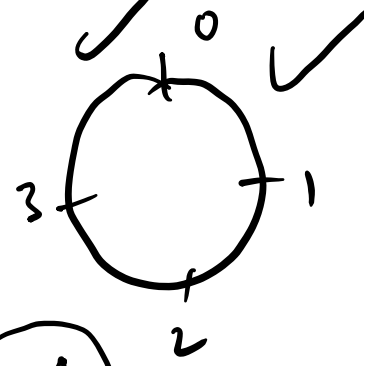
$$a +_n b = a + b \pmod n$$

Two integers a and b are Congruent ~~iff $a =$~~ modulo 'n' if $n \mid a-b$. and we write

$$a \equiv b \pmod n$$

$$a - b = nk$$

$$a = b + nk$$



(a)

$n = 4$

$a = 4 \times 2 + 1$

$5 \equiv 1 \pmod 4$

$a \equiv 1$

$4 \mid 5-1$

$a \equiv 1$

$a = 1$

4

$Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$(+_4)$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

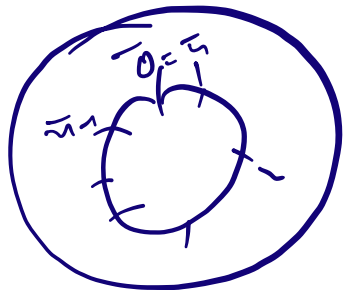
$\bar{0}$ is

$\bar{2} + \bar{2} = \bar{0}$

$(Z_4, +_4)$ is a group

#

$(Z_n, +_n)$ is an abelian group.



$$a +_n b \equiv \overline{a+b} \pmod{n} = \overline{(b+a)} \pmod{n} = b +_n a$$

if $\bar{x} \in Z_n$.

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

$$-x = \overline{n-x} \pmod{n}$$

$Z_4 \longrightarrow$ 2

$-3 \longrightarrow 4-3 = 1$

$4-2 = 2$

X_n : Multiplication 'modulo n'.
in Z_n

$$a \times_n b = ab \pmod n$$

$(Z_4, \times_4)$

$$Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$$

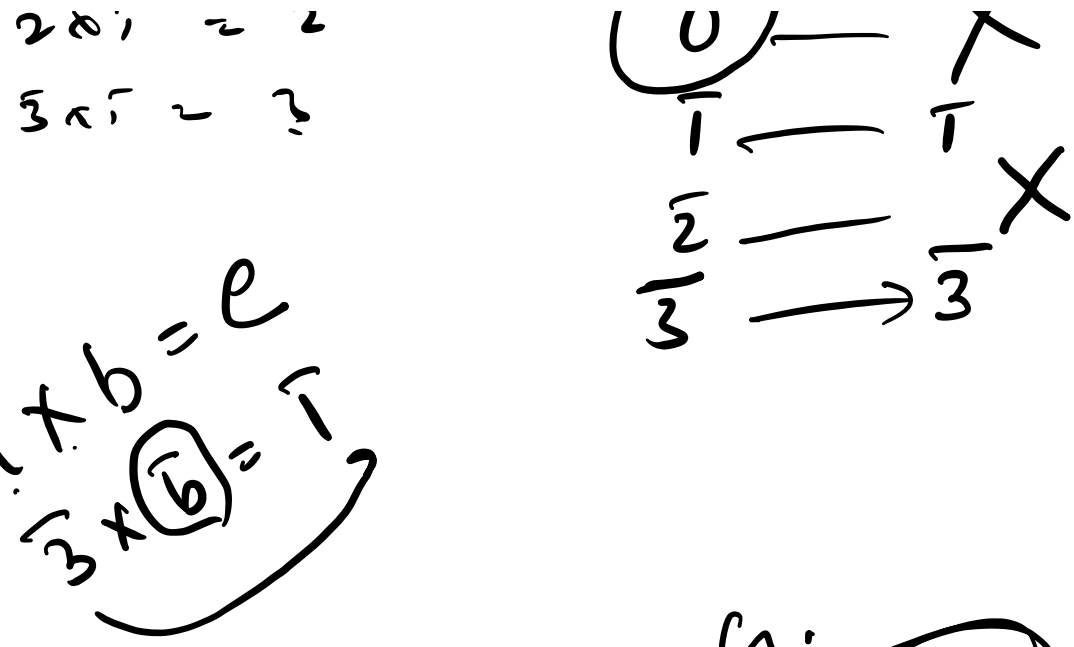
$$\bar{2} \times_4 \bar{3} = 6 \pmod 4 = \bar{2}$$

→ Identity →

$\bar{0} \times e = \bar{0}$ ✓
$\bar{1} \times e = \bar{1}$
$\bar{2} \times e = \bar{2}$
$\bar{3} \times e = \bar{3}$

✓
$\bar{0} \times \bar{1} = \bar{0}$
$\bar{1} \times \bar{1} = \bar{1}$

element — Inverse ✓

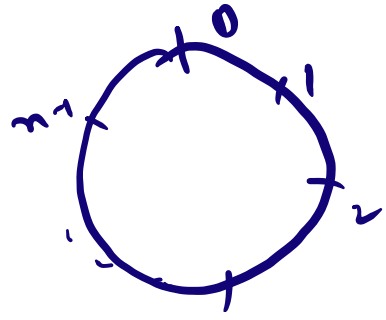


$$a +_n b = a + b \pmod n$$

$$a \times_n b = a \cdot b \pmod n$$

$$\bar{0} = \{ x \in \mathbb{Z} : x = nk_1 \}$$

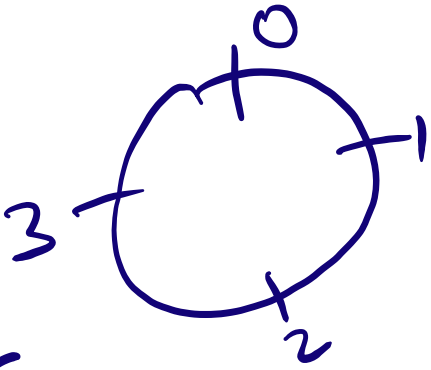
$$\bar{1} = \{ x \in \mathbb{Z} : x = nk_2 + 1 \}$$



$n = 4$

$6 \pmod 4 \equiv 2$

$6 = 4 + 2 \equiv 2$



n

$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$\mathbb{Z}_4^* = \{\bar{1}, \bar{3}\}$

$\bar{2}$ has no inverse

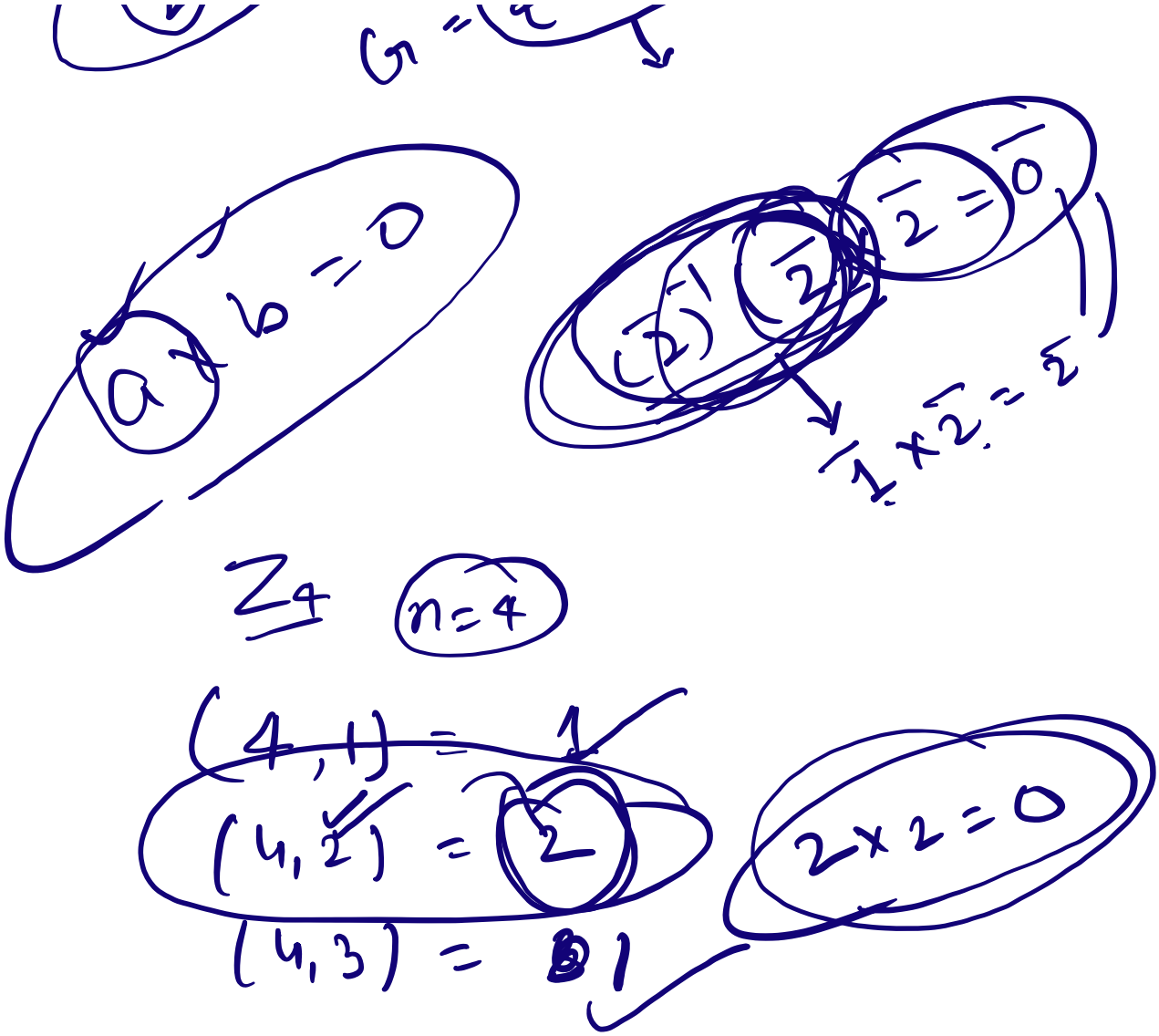
$\bar{2} \times \bar{0} = \bar{0}$

$\bar{2} \times \bar{a} = \bar{1}$

ϵ^{2k}

yes

$\{\bar{1}, \bar{3}\}$



Define: $U(n)$ = set of all positive integers less than 'n' and relatively prime to n.

For instance: $n = 10$

$U(10) = \{1, 3, 7, 9\}$

$Z_{10} = \{ \cancel{0}, 1, \cancel{2}, 3, \cancel{4}, \cancel{5}, \cancel{6}, 7, \cancel{8}, 9 \}$

$+_{10}$

$\times_{10}$

$5 \times 2 = 0$

Cayley table / Composition table

$U(10)$

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$\# Z_n^* = Z_n - \{\bar{0}\}$

is a group iff n is prime.

under $(\times_7)$.

$$Z_{(7)}^{*} = \{1, 2, 3, 4, 5, 6\}$$

Def: Order of an element:

Let $g \in G$. Then the order of g, denoted by $O(g)$ or $|g|$, is the smallest positive integer 'n' s.t

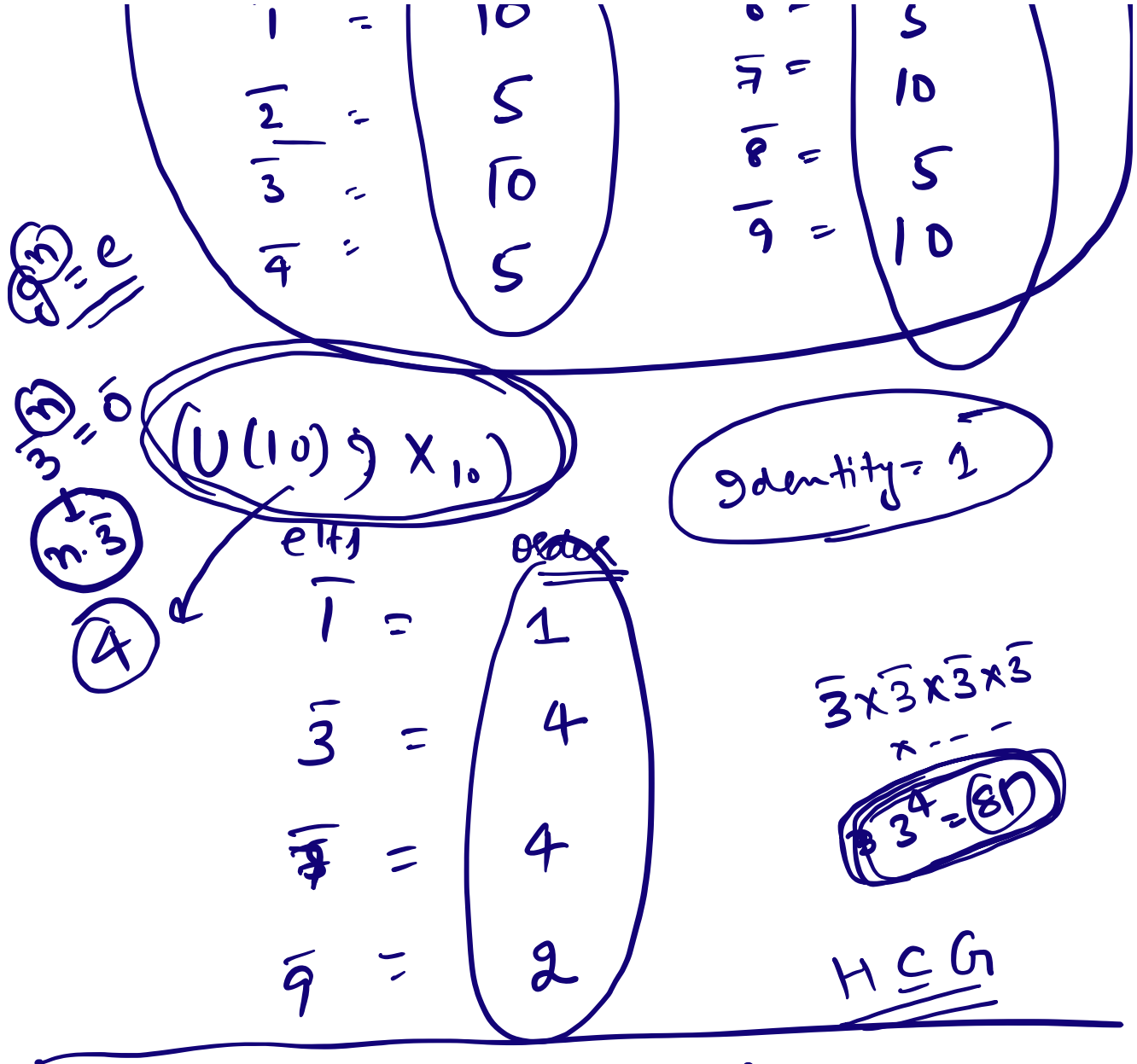
$$g^n = e \quad \text{i.e.} \quad \underbrace{g * g * \cdots * g}_{n \text{ times}} = e$$

identity.

If such 'n' does not exist; 'g' has infinite order.

Z_{10} $(Z_{10}, +_{10})$

elt	order
$\bar{0}$	1
$\bar{5}$	2



Subgroup: If a subset H of a group G is itself a group under the operation of G. (nonempty)

then H is called a subgroup of G.

we denote it as: $H \leq G$

eg: $G = Z_{10}$: $H = \{2, 4, 6, 8, 0\}$

$H_2 = \{1, 3, 7, 9\}$

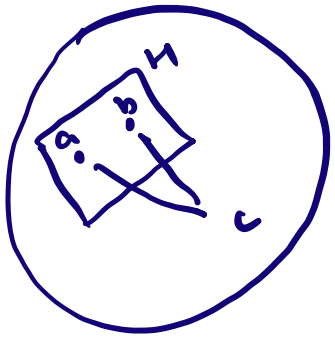
$H \subseteq G$. G

(i) ✓

(ii) ✗

(iii) ✗

(iv) $\forall\, a \in H \Rightarrow a^{-1} \in H$



$[a \in H,\ a^{-1} \in H]$

$aa^{-1} \in H$

Two Step Test:

Let G be a group and H a nonempty subset of G. Then H is a subgroup of G if

(i) $ab \in H \quad \forall \quad a, b \in H$

(ii) $a^{-1} \in H \quad \forall \quad a \in H.$

One step test

if $\forall \quad a, b \in H$

$\Rightarrow \quad ab^{-1} \in H$

$a \in G.$

$H = \{ a^n : n \in \mathbb{Z} \}$

$G = Z_{10}$

$H = \{ 2^n : n \in Z \}$

$H = \{ 2^1, 2^2, 2^3, 2^4, 2^5, \ldots \}$

$\{ 2, 4, 6, 8, 0 \}$

$a * a * \cdots * a = a^n$

na

$Z_{10} = \{1, 2, 3, \ldots, 0\}$

a^2

$2 * 2$ $\quad$ $3 * 3$ $\quad$ $3 + 3$

a^n

$G \ni a$

$H = \{ a^n : n \in Z \}$

Subgroup ?

$a^n * a^{-n}$, a^m, a^n, a^{m+n}

$U(10) = \{1, 3, 7, 9\}$ → Cyclic

$H_1 = \{1\}$

$H_2 = \{3^1, 3^2, 3^3, 3^4, \ldots\}$

$= \{3, 9, 7, 1\} = G_1.$

$H_3 = \{7^1, 7^2, 7^3, 7^4, \ldots\}$

$= \{7, 9, 3, 1\} = G_1$

$H_4 = \{9^1, 9^2, 9^3, 9^4\}$

$= \{9, 1\}$