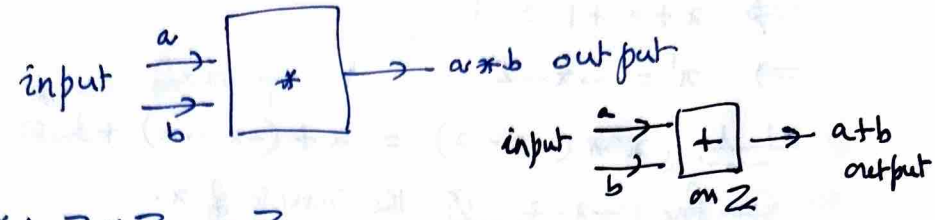
Dt: 01/01/2025:

Binary operation: $* \; A \times A \to A$, where $A \neq \phi$.

$$*(a,b) \mapsto a * b.$$



Ex: $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

$*(a,b) \longmapsto \frac{a+b}{ab}$ / Not an operation on $\mathbb{Z}$.

Take $(a,b) = (2,3)$

$$*(2,3) = \frac{2+3}{2\times 3} = \frac{5}{6} \notin \mathbb{Z}.$$

Check: 1. $a * b = \sqrt{|ab|}$ on the set $\mathbb{Q}$.

2. Subtraction on $\mathbb{Z}$ $\quad (-: (3,5) \mapsto 3-5 = -2 \in \mathbb{Z})$

3. Subtraction on $\{n \in \mathbb{Z} \mid n \geq 0\}$. $\quad -: (5,8) \mapsto 5-8 = -3 \notin \mathbb{Z}^+$

Properties: Let $\mathbb{R}$: real numbers.

$$*: \mathbb{R} \times \mathbb{R} \to \mathbb{R}.$$

$*$ is commutative $\quad (a*b = b*a)$

$*$ is associative $\quad (a*(b*c) = (a*b)*c)$

$\mathbb{R}$ has identity w.r.t. $*$. $\quad (a*e = e*a = a)$

Every $x \in \mathbb{R}$ has an inverse w.r.t. $*$. $\quad (a * a^{-1} = e)$

Ex: $x * y = x + y + 1$.

Asso.	Commu.	Identity	Inverse
☑	☑	☑	☑

(i) $x * y = x+y+1 = y+x+1 = y * x$.

(ii) $x * (y*z) = x*(y+z+1) = x+(y+z+1)+1 = x+y+z+2$

$(x*y)*z = (x+y+1)*z = (x+y+1)+z+1 = x+y+z+2$.

(iii) Solve for $x * e = x$ for e.

$$x*e = x+e+1 \; (\underset{\text{to be}}{=} x) \Rightarrow e = -1 \in \mathbb{R}$$

Check: $x * (-1) = x + (-1) + 1 = x$, and

$(-1) * x = (-1) + x + 1 = x$.

Therefore -1 is an identity.

(iv) Solve for $x * x' = e$ ie; $x * x' = -1$

$\Rightarrow x + x' + 1 = -1$

$\Rightarrow x' = -x - 2$

Check: $x * (-x-2) = x + (-x-2) + 1 = -1$.

Therefore $-x-2$ is the inverse of x.

Ex (practice!) $x * y = |x - y|$ (on $\mathbb{R}$)

$x * y = \dfrac{xy}{x+y+1}$ (on $\mathbb{R}^+$).

Ex: Checkerboard Game:

Checkerboard has only four squares numbered 1, 2, 3 and 4.

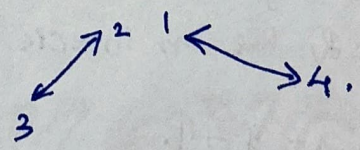
1	2
3	4

Moves:

V: move vertically $\begin{matrix} 1 \\ \updownarrow \\ 3 \end{matrix}$ or $\begin{matrix} 2 \\ \updownarrow \\ 4 \end{matrix}$

H: move horizontally $1 \longleftrightarrow 2$, $3 \longleftrightarrow 4$

D: move diagonally

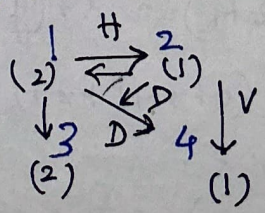


I: Stay put.

$*$: {Set of moves} $\times$ {Set of moves} $\longrightarrow$ {Set of moves}.

: performing moves successively.

$* : (H * V) \longmapsto D$



$H * H = I$

$(G, *)$ is satisfied:

(i) $*$ is associative

(ii) has identity I.

(iii) has inverse for every move.

$*$	I	V	H	D
I		⋮	⋮	
V		⋮	⋮	
H	- - - -	D	- - -	I
D				

<u>Def.</u> More formally: A set $G(\neq \phi)$ together with an operation $*$ which satisfies the axioms

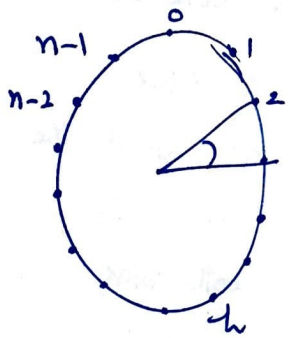
(i) $*$ is associative

(ii) $\exists\ e \in G \ni a * e = a = e * a$

(iii) To each $a \in G\ \exists\ a^{-1} \in G \ni a * a^{-1} = a^{-1} * a = e$.

is <u>called a group</u>. Further, G is <u>abelian</u> if $a * b = b * a\ \forall a, b \in G$.

<u>Ex.</u>



Integers modulo n

$\{0, 1, 2, \ldots, n-1\}$.

$h + k$ = start with h and go clock-wise through arc of k times $\frac{2\pi}{n}$.

Inverse of $h = (n-h)$

$h + (n-h) = n = 0$.

<u>$n = 6$</u>

$(\mathbb{Z}_6, +)$

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2						
3		1				1
4		⋮				⋮
5	5	0	1	2	3	4.

<u>Ex.</u> Let $G = \left\{ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, C = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, D = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, K = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} \right\}$.

$*$: matrix (usual) multiplication.

I : Identity.

$(G, *)$ is a gp.

$*$	I	A	B	C	D	K
I	I	A	B	C	D	K
A	A	I	C	B	K	D
B	B	K	D	A	I	C
C	C	D	K	I	A	B
D	D	C	I	K	A	B
K	K	B	A	D	C	I

A Coin Game:

Assume initially H H.

Imagine 2 coins on a table, at positions A and B (coins with H, T

Let $G = \{$ all possible moves $\}$

$= \{ M_1$: flip over the coin A

M_2 : " " B

M_3 : " " both coins

M_4 : Switch the coins

M_5 : flip coin at A, then switch

M_6 : " " B, " "

M_7 : " both coins, " "

$I \ (= M_8)$: Do not change anything. $\}$

	A	B
Initial	$C_1(H)$	$C_2(H)$
$M_4 \mapsto$	$C_2(H)$	$C_1(H)$
$M_1 \mapsto$	$\boxed{C_2(T)}$	$\boxed{C_1(H)}$

	A	B
Initial	$C_1(H)$	$C_2(H)$
M_6^1	$C_1(H)$	$C_2(T)$
M_6^2	$\boxed{C_2(T)}$	$\boxed{C_1(H)}$

$= \{ I, M_1, M_2, \ldots, M_7 \}$.

$*$: performing any two moves in succession.

$*$	I	M_1	M_2	M_3	M_4	M_5	M_6	M_7
I		⋮			⋮			
M_1		⋮			⋮			
M_2	- -	⋮	- -	- -	- -	M_6		
M_3		⋮						
M_4	- -	M_6						
M_5								
M_6								
M_7								

Groups in binary codes:

The basic way of transmitting information ~~into~~ is to code it into strings of 0's and 1's, such as 0010110, 10110, 01, etc. Such strings are called binary words. Number of 0's and 1's in binary word is called its length.

Illustration:

If $a = a_1 a_2 \cdots a_n$ $\boxed{\text{sent}}$,

but $b = b_1 b_2 \cdots b_n$ $\boxed{\text{received}}$

$a_i = 0$ or $1 = b_i$ $(1 \le i \le n)$

Then the error pattern:

word $e = e_1 e_2 \cdots e_n$ where $e_i = \begin{cases} 0 & \text{if } a_i = b_i \\ 1 & \text{if } a_i \ne b_i \end{cases}$

Let $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$ } code words.

Then $a + b = (a_1 + b_1, \ldots, a_n + b_n)$ / sum. "word addition" "resulting word"

Error pattern is "e".

For ex:

$$\begin{array}{r} 0010110 \\ +\ 0011010 \\ \hline 0001100 \end{array} \qquad \begin{array}{r} 10100111 \\ +\ 11110111 \\ \hline 01010000 \end{array}$$

Now, let $B^n = \{(a_1, \ldots, a_n) \mid a_i = 0 \text{ or } 1,\ 1 \le i \le n\}$. Then "+" is

1) commutative
2) Associative
3) $\exists$ identity element for word addition
4) To each word, $\exists$ an inverse under word addition.

Note: $a + b = a - b$ (where $a - b = a + (-b)$)

$a + b = c \implies a = b + c$.

1. Properties: Let $a, b, c \in G$, where G is a group. Then.

(1) $ab = ac \Rightarrow b = c$

(2) $ba = ca \Rightarrow b = c$

(3) $(ab)^{-1} = b^{-1}a^{-1}$

(4) $(a^{-1})^{-1} = a$, (5) $ab = e \Rightarrow a = b^{-1}$, $b = a^{-1}$

Sol: (1) $ab = ac$ (Given)

$\Rightarrow a^{-1}(ab) = a^{-1}(ac)$ (inverse exists)

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$ (by asso.)

$\Rightarrow eb = ec$ (identity)

$\Rightarrow b = c$.

In general, we cannot cancel 'a'.

(2) Similar.

(3) $(ab)(b^{-1}a^{-1}) = a[(bb^{-1})a^{-1}]$ (by asso.)

$= a[ea^{-1}]$ (inverse)

$= aa^{-1}$ (identity)

$= e$. (inverse)

By (2), $(ab)^{-1} = b^{-1}a^{-1}$.

(4) $aa^{-1} = e \Rightarrow a$ is the inverse of a^{-1} ie, $a = (a^{-1})^{-1}$.

Problem: Solve simultaneously $x^2 = b$ and $x^5 = e$, $x, b, e \in G$ (find x?)

Sol: $b = x^2$

$\Rightarrow b^2 = x^4$ (Squaring)

$\Rightarrow xb^2 = x^5 (= e)$ (multiplying by x)

$\Rightarrow xb^2 = e$

$\Rightarrow (xb^2)(b^2)^{-1} = e(b^2)^{-1}$ (post multiply with $(b^2)^{-1}$)

$\Rightarrow x = (b^2)^{-1}$

Ex. $(G = \{1, i, -1, -i\}, \cdot)$

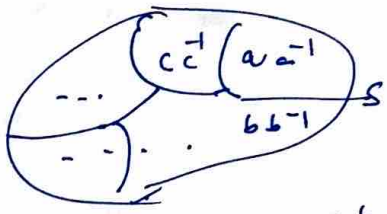
Own inverses $1, -1$.

$\cdot$	1	i	-1	$-i$
1	$\boxed{1}$	i	-1	$-i$
i	i	-1	$-i$	$\boxed{1}$
-1	-1	$-i$	$\boxed{1}$	i
$-i$	$-i$	$\boxed{1}$	i	-1

Counting elements and their inverses:

Let G be a finite gp.

$S = \{x \in G \mid x \neq x^{-1}\}$



Try: In any group G, the number of elements not equal to their own inverse is an even number.

Constructing small groups:

Let G: any group, e: identity.

1) If $a, b \in G$, prove

If $a^2 = a$, then $a = e$

If $ab = a$, then $b = e$

If $ab = b$, then $a = e$.

2)

	$\cdots y_1 \cdots y_2 \cdots$
$\vdots$	
a	$\cdots x \cdots x.$

$ay_1 = ay_2 = (x)$

$\Rightarrow y_1 = y_2$

3) Let $S = \{e, a, b\}$. Construct group table.

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

If $ab = a$, then $b = e$, a contra.

" $ab = b$, then $a = e$, a contra.

Only for $ab = e$

If $ba = a$, then $b = e$, ...

If $ba = b$, then $a = e$, ...

Only for $ba = e$

4) There is exactly one group G of four elements, say $G = \{e, a, b, c\}$, satisfying the additional property $xx = e$ for every $x \in G$. Complete the following table. (using part (1))

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

* 5) There is exactly one group G of four elements, say $G = \{e, a, b, c\}$ such that $xx = e$ for some $x (\neq e) \in G$, and $yy \neq e$ for some $y \in G$ (Say $aa = e$ and $bb \neq e$). Complete the group table.

Label: $e = id$, a, $b = a^2$, $c = a^3$

Take $x = b$, $xx = (a^2)^2 = e$ and $y = a$, $yy = a^2 = b \neq e$.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

2. Property: Let G be a group and let $a, b \in G$. The equations

$$ax = b \quad \text{and} \quad ya = b$$

have unique solution for $x, y \in G$.

Refer property (1): $ax = b$

$x = a^{-1}b$ (left multi a^{-1})

Sol is unique. (unique)

$ya = b$

$y = ba^{-1}$ (right multi a^{-1})

Sol is unique.

Examples of Non-abelian groups.

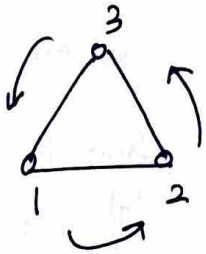
(1) Symmetrices of an equilateral Δ^{le}.

Symbols $n = 3$: $\{1, 2, 3\}$.

Rotation Symmetry:

$$\frac{2\pi i}{n}, \quad i = 0, 1, 2.$$

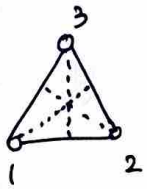
$$= 0^\circ, 120^\circ, 240^\circ.$$



$$r^0 = id. = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad r^1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad r^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Reflections symmetry:

From a fixed vertex $\perp^{rl}$ bisectors onto the opposite side.



$$s = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad sr = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad sr^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Therefore groups $G = \{ \underbrace{r^0 = id, r, r^2}_{\text{rotations anti clockwise}}, \underbrace{s, sr, sr^2}_{\text{reflections.}} \}$,

"with respect to function Composition"

G is non-abelian:

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

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

Infer $rs \neq sr$.

2) Let $G = \{(a,b) \mid a, b \in \mathbb{R},\ a > 0\}$. Define the following operation on G as follows.

$$(a,b) * (c,d) = (ac,\ bc+d)$$

for all $(a,b), (c,d) \in G$.

Since for any $(a,b), (c,d) \in G$, $ac \neq 0$. (as $a \neq 0 \neq c$)

If $b \neq 0$ and $c \neq 0$, then $bc+d \neq 0$. So $*$ is a binary operation on G.

Associative operation:

$$\begin{aligned}
&((a,b) * (c,d)) * (e,f) \\
&= (ac,\ bc+d) * (e,f) && (\text{def.}) \\
&= (ace,\ bce+de+f) && (\text{def.}) \\
&= (a,b) * (ce,\ de+f) && (\ \text{"}\ ) \\
&= (a,b) * ((c,d) * (e,f))
\end{aligned}$$

Also, $(a,b) * (1,0) = (1,0) * (a,b) = (a,b)$

So $(1,0)$ is an identity.

$$(a,b) * \left(\frac{1}{a}, \frac{-b}{a}\right) = \left(a \cdot \frac{1}{a},\ b \cdot \frac{1}{a} + \left(\frac{-b}{a}\right)\right) = (1,0)$$

also, $\left(\frac{1}{a}, -\frac{b}{a}\right) * (a,b) = (1,0)$.

Therefore $\left(\frac{1}{a}, -\frac{b}{a}\right)$ is the inverse of (a,b).

Hence G is a group.

G is not abelian:

$$\begin{aligned}
(2,3) * (1,4) &= (2,7) \\
(1,4) * (2,3) &= (2,11)
\end{aligned} \quad \neq$$

3) Let $a, b \in \mathbb{R}$, $a \neq 0$.

Define $T_{a,b} : \mathbb{R} \to \mathbb{R}$ as, $T_{a,b}(x) = ax+b$ for each $x \in \mathbb{R}$

" linear maps "

$$G = \{ T_{a,b} : \mathbb{R} \to \mathbb{R} \mid a, b \in \mathbb{R}, a \neq 0 \}.$$

Consider the product as composition of functions.

G is closed under <u>composition</u>: Take $T_{a,b}$, $T_{c,d} \in G$., $x \in \mathbb{R}$

$$\begin{aligned}
(T_{a,b} \circ T_{c,d})(x) &= T_{a,b}(T_{c,d}(x)) \\
&= a\, \underbrace{T_{c,d}(x)} + b \\
&= a(cx+d)+b \\
&= (ac)x + (ad+b) \\
&= T_{ac,\, ad+b}(x). \qquad \forall x \in \mathbb{R}
\end{aligned}$$

Therefore $T_{a,b} \circ T_{c,d} = T_{ac,\, ad+b} \in G$

<u>Associative</u>: Take $T_{a,b}$, $T_{c,d}$ and $T_{e,f} \in G$.

$$\begin{aligned}
(T_{a,b} \circ T_{c,d}) \circ T_{e,f} &= T_{ac,\, ad+b} \circ T_{e,f} \\
&= T_{ace,\, acf+ad+b} \\
&= T_{a,b} \circ T_{ce,\, cf+d} \\
&= T_{a,b} \circ (T_{c,d} \circ T_{e,f})
\end{aligned}$$

<u>Identity element</u>: $T_{1,0} \circ T_{a,b} = T_{a,b} \circ T_{1,0} = T_{1,0}$.

To find inverse: $T_{a,b}^{-1}$

for any $x \neq 0$ in $\mathbb{R}$ and $y \in \mathbb{R}$,

$$T_{a,b} \circ T_{x,y} = T_{x,y} \circ T_{a,b} = T_{1,0}$$

$$\Leftrightarrow \quad T_{ax,\, ay+b} = T_{ax,\, bx+y} = T_{1,0}.$$

$$\Leftrightarrow \quad ax = 1 \quad \text{and} \quad ay + b = bx + y = 0.$$

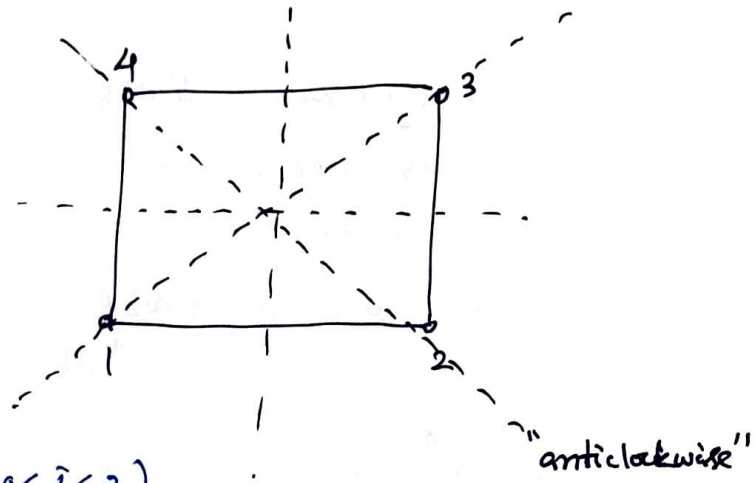
$$\Leftrightarrow \quad x = 1/a \ (\text{here } a \neq 0), \quad y = -b/a$$

Therefore $T_{a^{-1},\, -a^{-1}b}$ is the inverse of $T_{a,b}$.

Therefore $(G, \circ)$ is a group.

Since $T_{1,2} \circ T_{3,4} \neq T_{3,4} \circ T_{1,2}$, it follows that G is not abelian.

<u>Example:</u> Consider the square with vertices (corner points)



ρ_i : Rotations $(0 \le i \le 3)$

μ_i : Mirror images in $\perp^r$ bisectors of sides $(i = 1, 2)$

δ_i : diagonal flips. $(i = 1, 2)$

Then $G = \Big\{ \rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ 90°-anti, $\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ 180°-anti

$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ 270°-anti, $\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ mirror vertical, $\mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ mirror hori

$\delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \Big\}$

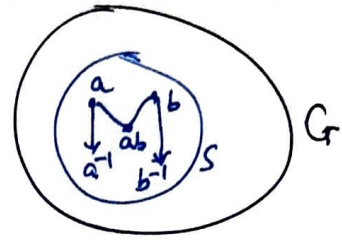
diagonal, diagonal.

$\circ$	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_1	δ_2	μ_2	μ_1
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	δ_2	μ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	δ_1	μ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	μ_1	δ_2	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	μ_2	δ_1	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

Def: (Subgroup)

Let G be a group. $S \subseteq G$.

S is called a <u>subgroup</u> if S itself forms a group under the same operation as in G.



Alternatively: $a, b \in S \begin{cases} \Rightarrow ab \in S \\ a^{-1} \in S. \end{cases}$ or $ab^{-1} \in S$.

Ex: $(G = \mathbb{R}^*, \cdot)$ ← multiplication operation.

1) $H = \{2^n \mid n \in \mathbb{Z}\}$

H is ☑ is not ☐ a subgroup of G.

$\left(2^n, 2^m \in H \Rightarrow 2^{n+m} = 2^n \cdot 2^m \in H \text{ as } n+m \in \mathbb{Z}. \right.$

$2^n \in H \Rightarrow \frac{1}{2^n} = 2^{-n} \in H$ (as $-n \in \mathbb{Z}$).

2) $G = (\mathbb{R}, +)$, $H = \{\log a \mid a \in \mathbb{Q}, a > 0\}$

H is ☐ is not ☐ a subgroup of G

3) $G = (\mathbb{R}, +)$, $H = \{x \in \mathbb{R} \mid \tan x \in \mathbb{Q}\}$

H is ☐ is not ☐ a subgroup of G.

4) $G = (\mathbb{R} \times \mathbb{R}, +)$, $H = \{(x, y) \mid x^2 + y^2 > 0\}$

H is ☐ is not ☐ a subgroup of G.

Subgps: Ex: Use Symbol "$\leq$" for subgp.

1) $G \leq G$
2) $\{1\} = \{e\} \leq G$.
3) $(\mathbb{Z}, +) \leq (\mathbb{Q}, +)$ and $(\mathbb{Q}, +) \leq (\mathbb{R}, +)$
4) Let $G = \{$Symmetries of a $\Delta^{le}\}$, $H = \{1, r, r^2\} \leq G$.
5) $(2\mathbb{Z}, +) \leq (\mathbb{Z}, +)$
6) $(\mathbb{Q} \setminus \{0\}, \cdot) \nleq (\mathbb{R}, +)$ operation mismatch.
7) $(\mathbb{Z}^+, +) \nleq (\mathbb{Z}, +)$
   $3 \in \mathbb{Z}^+$ but $-3 \notin \mathbb{Z}^+$
8) $(\mathbb{Z} \setminus \{0\}, \cdot) \nleq (\mathbb{Q} \setminus \{0\}, \cdot)$
   $5 \in \mathbb{Z} \setminus \{0\}$, but $\frac{1}{5} \notin \mathbb{Z} \setminus \{0\}$.

Property:

Subgp Criterion: Let G be a gp and H is a subset of G.

$$\boxed{H \text{ is a subgroup}} \iff \boxed{\begin{array}{l} 1)\ H \neq \phi \\ 2)\ \forall x, y \in H,\ xy^{-1} \in H. \end{array}}$$

Suppose H is a subgp of G. $\longrightarrow$ Then by def. H itself is a gp.

$\Rightarrow H \neq \phi$

Take $x, y \in H \subseteq G$

$\Rightarrow xy \in H$ & $x^{-1} \in H$, $y^{-1} \in H$

So $xy^{-1} \in H$.

$\longleftarrow$ Suppose H satisfies 1) and 2)

Since $H \neq \phi$, $x \in H$

Take $y = x$, Use 2) we get

$1 = xx^{-1} \in H$ (id.)

$1, x \in H \Rightarrow 1 \cdot x^{-1} \in H$ (by (2))

$\Rightarrow x^{-1} \in H$ (inverse)

For any $x, y \in H$.

$y \in H \Rightarrow y^{-1} \in H$

$\Rightarrow (y^{-1})^{-1} \in H$

$\Rightarrow x \cdot (y^{-1})^{-1} \in H$

$\Rightarrow xy \in H$. (closed)