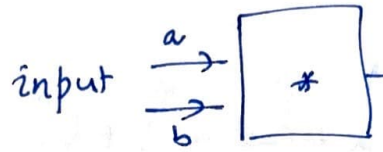
Dt: 01/01/2025:

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

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



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

$*(a,b) \mapsto \frac{a+b}{ab}$ / 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 $\mathbb{Z}$ $(- : (3,5) \mapsto 3-5 = -2 \in \mathbb{Z})$

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

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

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

- $*$ is commutative $(a*b = b*a)$
- $*$ is associative $(a*(b*c) = (a*b)*c)$
- $\mathbb{R}$ has identity w.r.t. $*$. $(a*e = e*a = a)$
  Every $x \in \mathbb{R}$ has an inverse w.r.t. $*$. $(a * a^{-1} = e)$

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 $x * e = xe$ for e.

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

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 $1 \updownarrow 3$ or $2 \updownarrow 4$

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

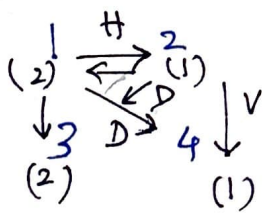
D: move diagonally $3 \swarrow\nearrow 2$ $1 \swarrow\searrow 4$.

I: Stay put.

$*$: {Set of moves} x {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				

Def. More formerly: A set $G(\neq \phi)$ together with an operation $*$ which satisfies the axioms

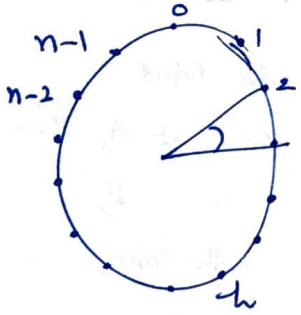
(i) $*$ is associative

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

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

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

Ex.



Integers modulo n

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

$h+k$ = start with h and go clockwise through arc of k times $\frac{2\pi}{n}$,

Inverse of $h = (n-h)$

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

$n = 6$

$(Z_6, +)$

	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

Ex. 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.

1 : 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 ($\in M_8$) : Do not change anything. }

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

	(A)	(B)
Initial	$C_1(H)$	$C_2(H)$
M_6'	$C_1(H)$	$C_2(T)$
M_6^2	$C_2(T)$	$C_1(H)$

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

$*$: 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 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 $a = a_1 a_2 \cdots a_n$ [Sent],

$\downarrow$

but $b = b_1 b_2 \cdots b_n$ [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 $e_i = \begin{cases} 0 & \text{if } a_i = b_i \\ 1 & \text{if } a_i \neq b_i \end{cases}$

Let $a = (a_1, \cdots, a_n)$

$b = (b_1, \cdots, b_n)$ } code words.

Then $a+b = (a_1+b_1, \cdots, a_n+b_n)$ / 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 $B^n = \{ (a_1, \cdots, a_n) \mid a_i = 0 \text{ or } 1 \ (1 \le i \le n) \}$. 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)

$\Rightarrow xb^2 = xx^4 (= e)$ (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. $(G = \{1, i, -1, -i\}, \cdot)$

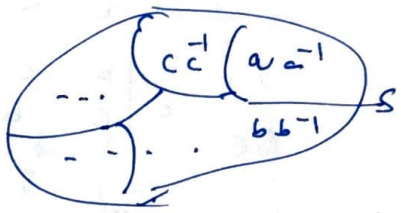
$\cdot$	1	i	-1	$-i$
1	**1**	i	-1	$-i$
i	i	-1	$-i$	**1**
-1	-1	$-i$	**1**	i
$-i$	$-i$	**1**	i	-1

Own inverses $1, -1$.

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))

·	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 $y = a$, $yy = a^2 = b \neq e$.

·	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 $ax = b$ and $ya = b$ have unique solution for $x, y \in G$.

Refer property (1): $ax = b$

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

a^{-1} (unique)

Sol is unique.

$ya = b$

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

Sol is unique.

Examples of Non-abelian groups.

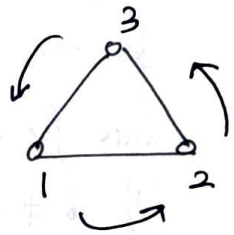
(1) Symmetrices of an equilateral Δ^{le}.

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

Rotation Symmetry:

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

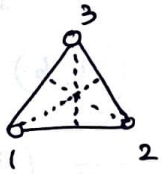
$= 0^\circ, 120^\circ, 240^\circ$.



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

Reflections Symmetry:

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



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

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:

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

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

Therefore $rs \neq sr$.

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:

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

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"

$$G = \left\{ T_{a,b} : \mathbb{R} \to \mathbb{R} \;\middle|\; a, b \in \mathbb{R}, a \neq 0 \right\}.$$

Consider the product as composition of functions.

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

$$\left(T_{a,b} \circ T_{c,d}\right)(x) = T_{a,b}\left(T_{c,d}(x)\right)$$

$$= a\, T_{c,d}(x) + b$$

$$= a(cx+d) + b$$

$$= (ac)x + (ad+b)$$

$$= T_{ac,\, ad+b}(x). \qquad \forall x \in \mathbb{R}$$

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

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

$$\left(T_{a,b} \circ T_{c,d}\right) \circ T_{e,f} = T_{ac,\, ad+b} \circ T_{e,f}$$

$$= T_{ace,\, acf+ad+b}$$

$$= T_{a,b} \circ T_{ce,\, cf+d}$$

$$= T_{a,b} \circ \left(T_{c,d} \circ T_{e,f}\right)$$

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

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

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

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

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

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

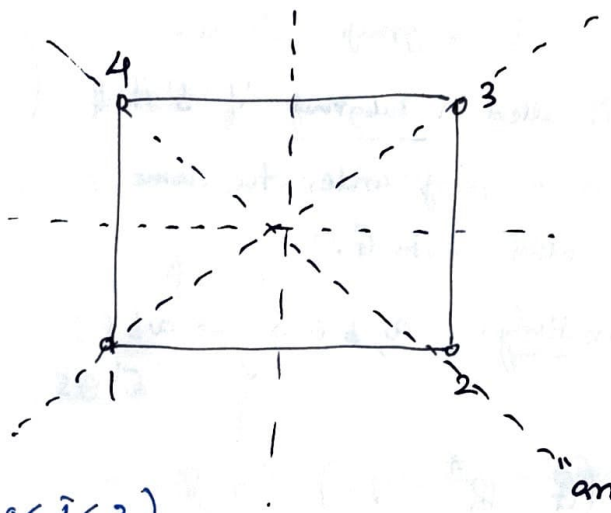
$$\Leftrightarrow \quad x = 1/a \ (\text{here } a \neq 0), \quad y = -b/a$$

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.

Example: Consider the square with vertices (corner points)



ρ_i : Rotations $(0 \le i \le 3)$

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

δ_i : diagonal flips. $(i = 1, 2)$

Then $G = \{ \rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$, $\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ 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

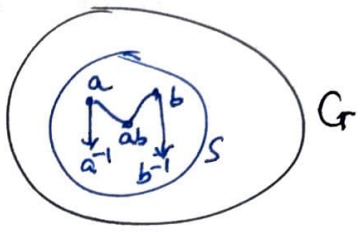
$\delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ diagonal, $\delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \}$ diagonal.

$\circ$	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 subgroup if S itself forms a group under the same operation as in G.



Alternatively: $a, b \in S \Rightarrow ab \in S$ and $a^{-1} \in S$. 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.

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

$2^n \in H \Rightarrow \frac{1}{2^n} = 2^{-n} \in H$ (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) $(\mathbb{Q} \setminus \{0\}, \cdot) \not\leq (\mathbb{R}, +)$ operation mismatch.

7) $(\mathbb{Z}^+, +) \not\leq (\mathbb{Z}, +)$

$3 \in \mathbb{Z}^+$ but $-3 \notin \mathbb{Z}^+$

8) $(\mathbb{Z} \setminus \{0\}, \cdot) \not\leq (\mathbb{Q} \setminus \{0\}, \cdot)$

$5 \in \mathbb{Z} \setminus \{0\}$, but $\frac{1}{5} \notin \mathbb{Z} \setminus \{0\}$.

Property:

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

H is a subgroup $\iff$ 1) $H \neq \phi$
2) $\forall x, y \in H$, $xy^{-1} \in H$.

Suppose H is a subgp of G. $\not\rightarrow$ 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 $xy^{-1} \in H$.

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

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

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

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

Order of an element:

Order: Let G be a gp and $x \in G$. The order of x is defined to be the smallest positive integer 'n' such that $x^n = 1$ (identity). Denoted by $|x|$ or $o(x)$. Infinite order if no such 'n' exists.

Ex: 1) An elt of a group has order 1 $\iff$ it is identity.
$G = \{1\}$ or $\{e\}$.

2) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ } order of non-zero element is infinite.

3) $\mathbb{R} \setminus \{0\}$, $\mathbb{Q} \setminus \{0\}$ as multiplicative groups.

order of $1 = 1$

order of $-1 = 2$ (since $(-1)(-1) = 1 =$ identity).

order of $x \notin \{1, -1\}$ = infinite.

4) $(\mathbb{Z}_9, +)$: $o(\bar{6}) = 3$ (since $\underbrace{6+6+6}_{} = 0$ in $\mathbb{Z}_9$)

$o(\bar{4}) = 9$ (since $\underbrace{\bar{4}+\bar{4}+\cdots+\bar{4}}_{9 \text{ times}} = 0$ in $\mathbb{Z}_9$)

5) Symmetries of a Δ^{le}:

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

$$\left. sr^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},\ id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \right\}.$$

$= r^0$.

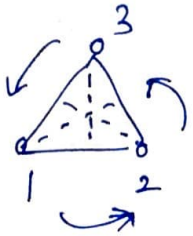
$o(r^0) = 1$

$o(r) = 3$ (since $r^3 = id$)

$o(r^2) = 3$

$o(sr) = 2$, $o(sr^2) = 2$.

$o(s) = 2$, $o(s^2) = 1$.



Remark: Let H be finite and closed under multiplication. Then H is a subgp.

Pf. Let $x \in H$.

$\Rightarrow x \cdot x \in H$ (closed)

$\Rightarrow$ ⋮

$x, x^2, \ldots \in H$

Since H is finite, $x^a = x^b$ ($b > a$ assume!).

Take $n = b-a$. Then

$x^n = x^{b-a} = x^b \cdot x^{-a}$

$= x^a \cdot x^{-a}$

$= x^0$

$= 1$. (identity)

$\Rightarrow o(x) = n$ (finite) $\forall x \in H$.

Now $x^n = 1 \Rightarrow x^{n-1} \cdot x = 1$

$\Rightarrow x^{-1} = x^{n-1}$

Also $x^{n-1} = x^{-1}$ (inverse). Therefore H is a subgp.

Def. (order of a group): The number of elements of a group. $|G|$. If $|G|$ is finite then G is said to be a finite gp. Otherwise, G is an infinite gp.

$(\mathbb{Z}, +)$: infinite order.

Notation: For each $n > 1$, $U(n)$: Set of all positive integers less than n and relatively prime to n.

$U(n)$ is a group under multiplication modulo n.

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

mod 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

$a \bmod n$ = unique integer r with the property

$a = nq + r$

$0 \le r < n$

If n is prime, $U(n) = \{1, 2, 3, \ldots, (n-1)\}$.

Ex: $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ is a group under multiplication modulo 15. $|U(15)| = 8$.

Compute order of each element in the group $U(15)$.

$|1| = 1$

$|2| = 4$ ($2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16 \equiv 1 \pmod{15}$). (id).

$|3| =$

$|4| = 2$

$|5| =$

$|8| = 4$

$|13| = 4$. ($13 \equiv -2 \pmod{15}$, $13^2 \equiv (-2)(-2)$

$|14| = 2$ $13^3 \equiv (-2)(-1)(-2) = 8$

$13^4 \equiv (-2)(-8) = 16 \equiv 1 \pmod{15}$).

Ex: (Try!) Compute the orders of following groups.

1) $U(12)$ 2) $U(35)$, 3) $U(20)$.

Cyclic Subgroup: Let G be a group, and $a, b, c \in G$.

$S = \{$ all possible products of a, b, c and their inverses with repetition of factors permitted

$= a^r b a c^{-1}, c^{-1} a^{-1}, bbc, abc, b^{-1} a^{-1} a^9 c b, \cdots \} \leq G$

which is called the Subgroup generated by a, b, c.

In particular, $\langle a \rangle$ is called the Subgp generated by $a \in G$.

$\langle a \rangle = \{a, aa, aaa, \cdots, a^{-1}, a^{-1}a^{-1}, \cdots, aa^{-1} = e\}$.

We call this as the cyclic subgroup of G generated by a.

Ex: Let $G = \{e, a, b, b^2, ab, ab^2\}$ whose generators are a, b; satisfying equations: $a^2 = e$, $b^3 = e$, $ba = ab^2$. Draw a multiplication table of G.

$\cdot$	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b	b^2
b	b	ab^2	b^2	b^3	a	ab.
b^2	b^2					
ab	ab	. .	.			b.
ab^2	ab^2					

$(ab)(ab^2) = abab^2$

$= aaab^2b^2$

$= a^2b^4$.

$= a^2b^3b$

$= a^2eb$

$= e\cdot b = b$.

$a(ab) = a^2\cdot b$

$= e\cdot b$

$= b$.

$b(ab) = (ba)b$

$= ab^2\cdot b$

$= ab^3$

$= a\cdot e$.

$= a$

$b(ab^2) = (ba)b^2$

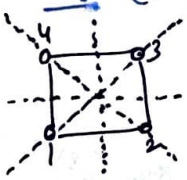
$= ab^2\cdot b^2$

$= a\cdot b^4$

$= a\cdot b^3\cdot b$

$= ab$.

Ex. (Try!) Let $G = \{e, a, b, b^2, b^3, ab, ab^2, ab^3\}$ whose generators satisfy: $a^2 = e$, $b^4 = e$, $ab^3 = ba$. Write the table for G. (G is called the dihedral group D_4).



Def. (Cyclic group): If G is a group and $a \in G$, it may happen that every element of G is a power of a. That is $G = \{a^n \mid n \in \mathbb{Z}\}$. In this case, G is called a cyclic group. We write $G = \langle a \rangle$.

Note: If $G = \langle a \rangle$ and $|a| = n$, then we say that G is of order n.

$= \{e, a, a^2, \cdots, a^{n-1}, (a^n = e)\}$.

Division algorithm: If $m, n \in \mathbb{Z}$ (and $n \in \mathbb{Z}^+$), then $\exists\ q, r \ni$

$m = nq + r$, $0 \le r < n$.

(q: quotient; r: remainder)

Property:

Th: (Powers of a, if a has finite order): Let G be a gp and $a \in G$. If $o(a) = n$, then there are exactly n different powers of a,

$a^0, a, a^2, \cdots, a^{n-1}$

Pf. We show every power of a is equal to one of the powers $a^0, a^1, a^2, \cdots, a^{n-1}$.

Let a^m be the power of a.

$m = nq + r, \quad 0 \le r < n.$

List: $e = a^0, a^1, a^2, \cdots, a^{n-1}$

$= a^n$. (n is least)

$a^m = a^{nq+r} = a^{nq} \cdot a^r = (a^n)^q a^r = e^q \cdot a^r = e^r$

$\Rightarrow a^m = a^r$ and $r \in \{0, 1, 2, \cdots, n-1\}$.

Next we prove that: $a^0, a^1, a^2, \cdots, a^{n-1}$ are all different.

Contrary: Suppose not. (contrary hypo.)

ie; $a^r = a^s$ (where r and s are distinct from $0, \cdots, (n-1)$.

Now either $r < s$ or $s < r$, say $s < r$.

Then $0 \le s < r < n$.

$\Rightarrow 0 < r - s < n$.

Now $a^r = a^s$ (hypo.)

$\Rightarrow a^r (a^s)^{-1} = a^s (a^s)^{-1}$ (post multiply with $(a^s)^{-1}$)

$\Rightarrow a^r (a^s)^{-1} = e$

$\Rightarrow a^{r-s} = e$., a contradiction $r - s < n$. and $o(a) = n$., n is least.

Thus, $a^0, a^1, \cdots, a^{n-1}$ are all different.

Property:

Th: (Powers of a, if a has infinite order): If $o(a) =$ infinite, then all the powers of a are different.

That is; $r \neq s$ (integers) $\Rightarrow a^r \neq a^s$. (contrapositive: $a^r = a^s \Rightarrow r = s$)

Pf. Let $r, s \in \mathbb{Z}$. Suppose $a^r = a^s$

$\Rightarrow a^r (a^s)^{-1} = (a^s)(a^s)^{-1}$ (post multiply with $(a^s)^{-1}$)

$\Rightarrow a^{r-s} = e$

But $o(a) =$ infinity, implies $a^m \neq e$ for any integer except 0. Thus $r - s = 0 \Rightarrow \boxed{r = s}$.

Comparision between $\langle a \rangle$ and $\mathbb{Z}_n$ $(n \in \mathbb{Z}^+)$: Let $a \in G$,

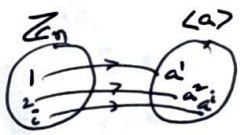
1) and $G = \langle a \rangle$, cyclic group of order n. Then.
(finite)

$$\langle a \rangle = \{ a^0, a^1, a^2, \ldots, a^{n-1} \}, \text{ multiplicative gp.}$$
(all distinct)

$$\mathbb{Z}_n = \{ 0, 1, 2, \ldots, n-1 \}, \text{ additive gp.}$$

(every element of $\mathbb{Z}_n$ is mapped to exactly one element of $\langle a \rangle$ and no element of $\langle a \rangle$ left out).

Define: $f: (\mathbb{Z}_n, +) \to (\langle a \rangle, \cdot)$ by



$$f(i) = a^i \quad (0 \le i \le n-1).$$

Then f is one-one and onto, and hence bijection map.

Further property: $f(i+j) = a^{i+j}$
$= a^i a^j$ / operation preserving.
$= f(i) \cdot f(j)$

Operation in $\mathbb{Z}_n$ ↗ ↖ operation in $\langle a \rangle$.

In this case we say that $\mathbb{Z}_n \cong \langle a \rangle$.

Conclusion: Any finite cyclic group is isomorphic to $\mathbb{Z}_n$ for some $n \in \mathbb{Z}^+$.

2) $O(a) =$ infinity.

$$\langle a \rangle = \{ \ldots a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots \} \text{ (all are distinct)}$$
$$\mathbb{Z} = \{ \ldots -2, -1, 0, 1, 2, \ldots \}$$

Define $f: (\mathbb{Z}, +) \to (\langle a \rangle, \cdot)$ by $f(i) = a^i$

Then f is one-one and onto. also operations preserving
$f(i+j) = f(i) \cdot f(j)$ (as above).

Therefore, $\mathbb{Z} \cong \langle a \rangle$. Where $\langle a \rangle$ = infinite.

Conclusion: Any infinite cyclic group is isomorphic to $\mathbb{Z}$ (the additive gp of integers).

Cayley Diagram: (Representation of finite group)

→ There is one point for every element of the group

→ The arrows represent the result of multiplying by a generator.

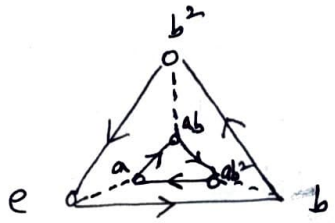
$e \longrightarrow a \longrightarrow a^2 \longrightarrow a^3 \longrightarrow \cdots$

Ex. $G = \{e, a, b, b^2, ab, ab^2\}$, $a^2 = e$, $b^3 = e$, $ba = ab^2$.

Generators = a, b.

⟶ "multiply by b"

- - - → "multiply by a".



ba

$ba = ab^2$

$ab \longrightarrow ab \cdot b = ab^2$

$ab^2 \longrightarrow ab^2 \cdot b = ab^3 = a$

$\boxed{a \longrightarrow ab}$

$b^2 a = b\,ba$

$= b\,ab^2$

$= ab^2 b^2$

$= ab^3 \cdot b$

$= ab \cdot$

$\Rightarrow \boxed{b^2 \text{ - - - } ab}$

$b \cancel{ab^2} = \cancel{ba}\,b^2$

$= ab^2 b^2$

$= ab^3 b$

$= ab^2 b = ab^3$

$= ae$

$= a$

$\Rightarrow \boxed{ab^2 \longrightarrow a}$

$ba = ab^2$

$\Rightarrow \boxed{b \text{ - - - } ab^2}$

Note: Cayley diagram of a group contains the same information as the group's table.

For instance: To check the product $(ab)(ab^2)$, see the fig. above.

$(ab)(ab^2)$: Stands for "start with 'ab' and follow the path corresponding to 'ab^2'.

(ab) - - - - $b^2 \longrightarrow e \longrightarrow b$

multiply right with a; multiply right with b; multiply right with b

Property: Suppose $a \in G$ and $o(a) = n$. (n is least $\ni a^n = e$.) Then

$$a^t = e \iff t \text{ is a multiple of } n.$$

(ie; $t = nq$ for some integer q).

Verification:

($\Rightarrow$): $a^t = e$ / Supposition.

Then, by using division algorithm,

$$t = nq + r, \quad 0 \le r < n.$$

Now $e = a^t = a^{nq+r} = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$.
($a^n = e$)

Therefore $a^r = e$, $0 \le r < n$.

If $r \neq 0$, then r is a positive integer $< n$, where n is smallest positive integer such that $a^n = e$, a contradiction to n is small.

Therefore $r = 0$, and so $\boxed{t = nq}$

($\Leftarrow$): Suppose $t = nq$.

Then $a^t = a^{nq} = (a^n)^q = e^q = e$.

Property: Every subgroup of a cyclic group is cyclic.

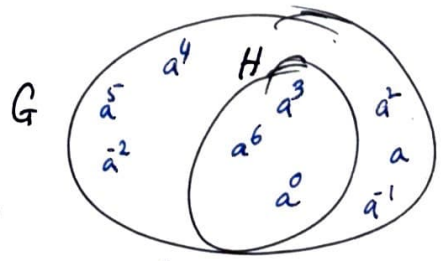
Verification: (proof!) Let $G = \langle a \rangle$ be cyclic with generator 'a';

and $H \le G$ (subgroup!).

Claim: H is also cyclic.

ie; we need to find a generator for H.

Since H is a subgp of G, each element of H is some power of a.



Therefore the generator (which we are searching!) is some power of a.

Let m be the smallest least +ve integer $\ni a^m \in H$.

Now we show that $H = \langle a^m \rangle$ ie; every element of H is a power of a^m.

Let $a^t \in H$ (arbitrary element of H).

Divide t by using division algorithm,

$$t = mq + r, \quad 0 \le r < m.$$

Then $a^t = a^{mq+r}$

$$= a^{mq} \cdot a^r$$

$$\Rightarrow a^r = (a^{mq})^{-1} a^t \quad (\text{since } a^{mq} \in G)$$

$$= \underbrace{(a^m)^{-q}}_{\in H} \underbrace{a^t}_{\in H} \cdot \in H.$$

This shows that $a^r \in H$, $r < m$ and m is smallest $\Rightarrow a^m \in H$.

Therefore $r = 0$. then $t = mq$.

Hence, every element $a^t \in H$ is of the form $a^t = (a^m)^q$, ie., power of a^m. Therefore H is cyclic with generator a^m.

Def.: For any set A, the group of all permutations of A is called the **Symmetric group** on A (S_A).

For $n \in \mathbb{Z}^+$, the symmetric group on the set $\{1, 2, \cdots, n\}$ is called the **Symmetric group on n elements** denoted by S_n.

$n=3$, $|S_3| = 3! = 6$

$|S_4| = 4! = 24$. $\cdots$, $|S_n| = n!$

Cycle: Let $a_1, a_2, \cdots, a_s \in \{1, 2, \cdots, n\}$. By a **cycle** $(a_1 a_2 \cdots a_s)$ we mean the permutation:

$a_1 \to a_2 \to a_3 \to \cdots \to a_{s-1} \to a_s$

For any $\sigma \in S_3$,

$\sigma = (1\,2\,3)$

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

– disjoint –

For ex: S_6: the cycle $(1\,4\,2\,6)$ is the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 2 & 5 & 1 \end{pmatrix}$

Ex: $(2\,4\,5)(1\,2\,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}$.

Transposition: A transposition is a cycle of length 2.

$(a_1 a_2 \cdots a_r) = (a_r a_{r-1})(a_r a_{r-2}) \cdots (a_r a_3)(a_r a_2)(a_r a_1)$

For ex: $(1\,2\,3\,4\,5) = \cancel{(1\,5)(1\,4)(1\,3)(1\,2)}$

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

(many ways possible!) or $(1\,2\,3\,4\,5) = (1\,5)(1\,4)(1\,3)(1\,2)$.

Try: Compute: for S_9

1) $(1\,4\,5)(3\,7)(6\,8\,2)$ $\quad$ 2) $(1\,7)(6\,2\,8)(9\,3\,5\,4)$.

Ex: Try: Express each of the following as product of transpositions in S_8.

1) $(13742\,8)$ 2) $(416)(8235)$.

3). $(147)(1678)(74132)$.

Sol: (3): $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 2 & 6 & 5 & 1 & 7 & 4 \end{pmatrix}$.

Ex: Write each of the following permutations in S_9 as a product of disjoint cycles.

1). $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 2 & 5 & 1 & 7 & 6 & 8 & 3 \end{pmatrix}$ Sol: $(145)(293)(67)(8)$.

2) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 9 & 5 & 3 & 1 & 2 & 4 & 8 & 6 \end{pmatrix}$ Sol:

3) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 4 & 3 & 6 & 5 & 1 & 2 \end{pmatrix}$

Ex: Express each of the following as a product of transpositions in S_8.

1) $(13742\,8)$

2) $(416)(8235)$

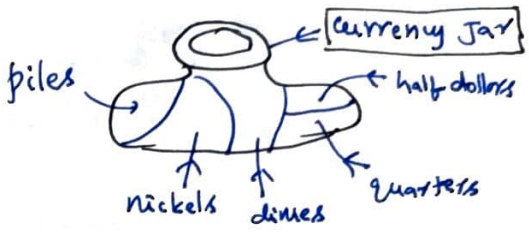
3) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 2 & 8 & 7 & 6 & 5 \end{pmatrix}$.

Partitions and Equivalence Relations:

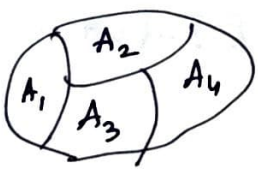
Motivation:

The delegates to the Democratic national Convention may be classified according to their home state, falling into 28 separate classes, one for each state.

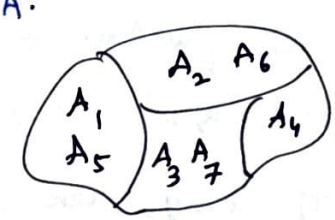
Motivation: Ex:



Partition: A partition of a set A is a family $\{A_i \mid i \in I\}$ of non-empty subsets of A which are mutually disjoint and whose union is all of A.



All disjoint



A_1, A_5: represent same class.

Note:

If two classes are not disjoint, they must be equal.

Partition: By a partition of a set A we mean a family $\{A_i \mid i \in I\}$ of non-empty subsets of A such that

1) If any two classes, A_i and A_j have a common element x, then $A_i = A_j$,
2) Every element x of A lies in one of the classes.

Def.: (Equivalence relation): By an equivalence relation ($\sim$) on a set A, we mean "$\sim$" is

1) Reflexive: $x \sim x \quad \forall x \in A$
2) Symmetric: $x \sim y \Rightarrow y \sim x$
3) Transitive: $x \sim y, y \sim z \Rightarrow x \sim z$.

$\forall x, y, z \in A.$

Ex. 1) "x is parallel to y"

2) "x weighs the same as y".

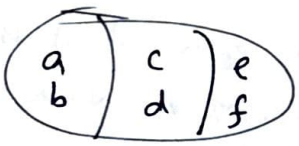
3) "x is same color as y"

Equivalence relation determined by the partition:

Consider the partition $\{A_i \mid i \in I\}$ of A.

(I ← index set)

Define $\sim$ on A by $x \sim y \iff x$ and y are in the same class of the partition.



$a \sim b$
$c \sim d$
$e \sim f$.

Denote the equivalence class of x in A as $[x]$. Then.

$[a] = \{a, b\}$, $[c] = \{c, d\}$, $[e] = \{e, f\}$.

Note: If $x \sim y$, then $[x] = [y]$.

In above $[a] = [b]$, as $a \sim b$.

Similarly, $[c] = [d]$, and $[e] = [f]$.

Note: (property): If $\sim$ is an equivalence relation on A, (then) the family of all the equivalence classes, that is,

$\{[x] : x \in A\}$ is a partition of A.

Verification: $x \sim x$ and so $x \in [x]$, (ie., each equivalence class is nonempty subset of A)

Next to show two classes are disjoint (or if two classes have a common element, they are equal)

Suppose $u \in [x]$ and $u \in [y]$.

Then $u \sim x$ and $u \sim y$.

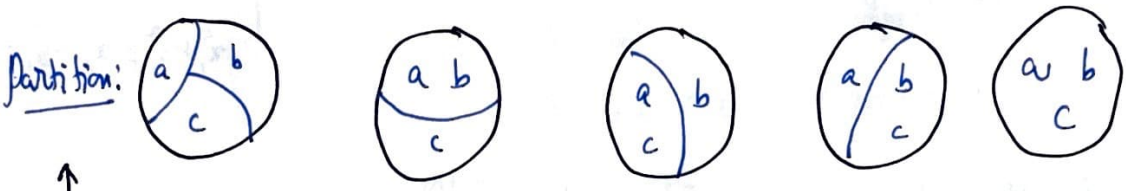
By transitive and symmetry, $x \sim y$. Thus $[x] = [y]$ (by above note)

Thus the family of all classes forms a partition.

Conversely: (very important!)

There are many ways of partitioning a given set A.
Each partition determines (and is determined by)
exactly one specific equivalence relation on A.

If $A = \{a, b, c\}$, then there are 5 ways of partitioning A.



Equivalence relation:

$a \sim a$	$a \sim a$	$a \sim a$	$a \sim a$	$a \sim a$
$b \sim b$	$b \sim b$	$b \sim b$	$b \sim b$	$b \sim b$
$c \sim c$	$c \sim c$	$c \sim c$	$c \sim c$	$c \sim c$
	$a \sim b$	$a \sim c$	$b \sim c$	$a \sim b$
				$a \sim c$
				$b \sim c$

Examples:

1) In $\mathbb{Z}$, define $m \sim n \iff |m| = |n|$.

2) In $\mathbb{Q}$, define $r \sim s \iff r - s \in \mathbb{Z}$.

3) In $\mathbb{Z}$, define $m \sim n \iff m - n$ is a multiple of 10.

Transitive: $m \sim n \Rightarrow m - n = 10k_1$
$n \sim p \Rightarrow n - p = 10k_2$
$m - n + n - p = 10(k_1 + k_2)$ Adding.
Therefore $m \sim p$.
k_1, k_2: integers.

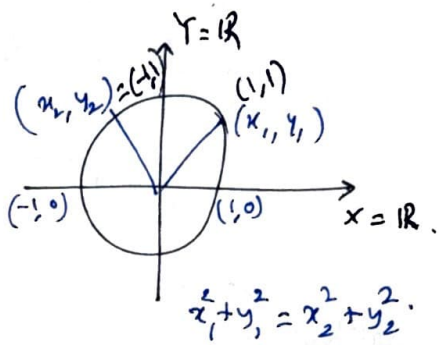
4) In $\mathbb{R}$, define $a \sim b \iff a - b \in \mathbb{Q}$.

Example: Define $\sim$ on $\mathbb{R}^2$ as:

$$(x_1, y_1) \sim (x_2, y_2) \iff x_1^2 + y_1^2 = x_2^2 + y_2^2$$

Two pairs of real numbers are in the same partition when they lie on the same circle about the origin.

$\sim$ is an equivalence relation on $\mathbb{R}^2$.



Example: let $r, s \in \mathbb{Z}$ and $n \in \mathbb{N}$.

$$r \equiv s \pmod n \iff r - s \text{ is divisible by } n.$$

ie: $r - s = nk$ for some $k \in \mathbb{Z}$.

Reflexive: $r - r = 0$ divisible by n, so $r \equiv r \pmod n$.

Symmetric: $r \equiv s \pmod n \Rightarrow r - s = -(s - r)$ is divisible by n

$= s - r$ " "

$\Rightarrow s \equiv r \pmod n$.

Transitive: $r \equiv s \pmod n$, $s \equiv t \pmod n$

$$\Rightarrow r - t = \underbrace{r - s}_{kn} + \underbrace{s - t}_{ln} = kn + ln = \underbrace{(k+s)}_{\in \mathbb{Z}} n$$

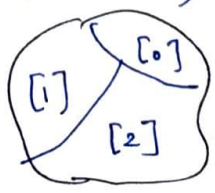
kn for some $k \in \mathbb{Z}$; ln for some $l \in \mathbb{Z}$

Therefore $r \equiv t \pmod n$.

Example: Equivalence relation established by "integers modulo 3".

for $r, s \in \mathbb{Z}$, $r \equiv s \pmod 3$.

$$[0] = \{\ldots -3, 0, 3, 6, \ldots\}$$
$$[1] = \{\ldots -2, 1, 4, 7, \ldots\}$$
$$[2] = \{\ldots -1, 2, 5, 8, \ldots\}$$



$[0] \cup [1] \cup [2] = \mathbb{Z}$.

partition of integers.

Example: Let G be a group and H a subgroup of G.

Define $a \sim b \iff ab^{-1} \in H$, where $a, b \in G$.

Verify! $\sim$ is an equivalence relation on G.

$\sim$ is reflexive: $a \sim a$ (since $e = aa^{-1} \in H$)

$\sim$ is Symmetric: $a \sim b \Rightarrow ab^{-1} \in H$

$\Rightarrow (ab^{-1})^{-1} \in H$ (since H is a subgp)

$\Rightarrow (b^{-1})^{-1} a^{-1} \in H$ (property)

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

$\Rightarrow b \sim a$.

$\sim$ is transitive: $a \sim b$ and $b \sim c$

$\Rightarrow ab^{-1} \in H$ and $bc^{-1} \in H$ (def.)

$\Rightarrow a\underbrace{b^{-1}b}_{e}c^{-1} \in H$ (closed)

$\Rightarrow ac^{-1} \in H$. Therefore $a \sim c$.

Therefore $\sim$ is an equivalence relation G.

Compute equivalence class containing 'e' identity:

$$[e] = \{a \in G \mid a \sim e\}$$

$$= \{a \in G \mid ae^{-1} \in H\}$$

$$= \{a \in G \mid a \in H\} = H$$

Counting: (cosets):

Let G be a group, and H a subgroup of G.

For any $a \in G$, we denote

$aH = \{$ set of all products 'ah' $\}$; called as left

- aH: operation in G
- 'ah': 'a' remains fixed; 'h' ranges over H.
- operation in G.

Coset of H in G.

In a similar way, $Ha = \{ ha \mid h \in H \}$

- ha: 'h' ranging over H; 'a' fixed.

Note: Every coset is a subset of G.

Ex: Let $G = (\mathbb{Z}_4, +)$, $H = \{0, 2\}$. Compute $a+H$ $\forall a \in G$.

"$a+H$"

operation '$+$'

$0+H = \{0, 0+2\} = \{0, 2\} = H$

$1+H = \{1+0, 1+2\} = \{1, 3\}$

$2+H = \{2+0, 2+2\} = \{2, 0\}$

$3+H = \{3+0, 3+2\} = \{3, 1\}$.

Property: If $a \in Hb$, then $Ha = Hb$ (Two cosets are equal).

Given $a \in Hb \Rightarrow a = h_1 b$ for some $h_1 \in H$.

To prove $Ha = Hb$:

Let $x \in Ha \Rightarrow x = h_2 a$ for some $h_2 \in H$

$= h_2 (h_1 b)$ (as $a = h_1 b$)

$= (h_2 h_1) b$ (associative)

$\in Hb$ ($h_2 h_1 \in H$ as H is closed)

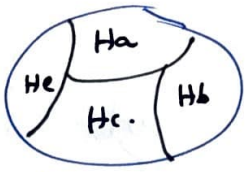
Thus $Ha \subseteq Hb$. In a similar way, $Hb \subseteq Ha$.

Hence $Ha = Hb$.

Note: Any property holds for right coset will hold (or true) for left cosets.

Property: The family of all the cosets Ha, as 'a' ranges over G, is a partition of G.

Verification: (proof).



First we show that any two cosets, say, Ha and Hb are either disjoint or identical.

If they are disjoint, we are done.

If not, let $x \in Ha \cap Hb$.

$x \in Ha \Rightarrow x = h_1 a$ for some $h_1 \in H$

$x \in Hb \Rightarrow x = h_2 b$ for some $h_2 \in H$.

Therefore $h_1 a = h_2 b$

$\Rightarrow a = (h_1^{-1} h_2) b$ / solving for a.

$\underbrace{\quad}_{\in H}$

$\in Hb$.

By above property, $Ha = Hb$.

Next we show every element $c \in G$ is in one of the cosets of H.

Now $c = ec$ (where $e \in H$ is the id.)

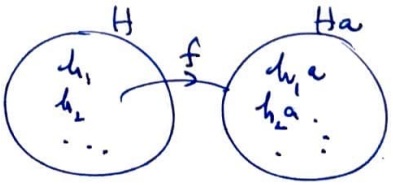
$\Rightarrow c = ec \in Hc$. That is c is an element in coset Hc.

Thus family of all cosets of H is a partition of G.

Theorem: (property:) If Ha is any coset of H, then there is a one-to-one correspondence from H to Ha.

Proof. Define $\boxed{f: H \to Ha}$

$f(h) = ha$



f is 1-1: $f(h_1) = f(h_2)$

$\Rightarrow h_1 a = h_2 a$

$\Rightarrow h_1 = h_2$ (by cancellation)

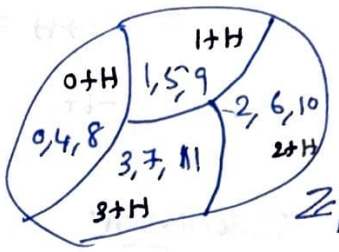
f is onto: Every element of Ha is of the form ha for some $h \in H$ and $ha = f(h)$.

Therefore f is a bijection.

Ex: Consider the additive group $(\mathbb{Z}_{12}, +) = \{0,1,2,3,4,5,6,7,8,9,10,11\}$.

$H = \{0,4,8\} \leq \mathbb{Z}_{12}$.

Choose $6 \in \mathbb{Z}_{12}$.



Then $6+H = \{$adding 6 to each element of $H\}$

$= \{6+0, 6+4, 6+8\} = \{6,10,2\}$.

Now compute $a+H$ to each $a \in \mathbb{Z}_{12}$.

$0+H = 4+H = 8+H = \{0,4,8\} = H$ (original) ← these are subgroups

$1+H = 5+H = 9+H = \{1,5,9\}$

$2+H = 6+H = 10+H = \{2,6,10\}$

$3+H = 7+H = 11+H = \{3,7,11\}$.

} None of these are subgroups as $0 \notin$ (all these).

Observations:

1) $a+H$ contains the element a

2) $0+H = 4+H = 8+H$ = original subgroup

3) All the cosets have the same size, namely size of H.

4) The distinct cosets form a partition of $\mathbb{Z}_{12}$.

Ex: (Example of cosets where the group and subgroup have infinitely many elements).

Consider $(\mathbb{Z}, +)$ gp.

$H = 5\mathbb{Z} = \{\ldots -20, -15, -10, -5, 0, 5, 10, 15, 20, \ldots\}$

Now $7+H = \{7+h \mid h \in H\}$.

$= \{\ldots 7+(-20), 7+(-15), 7+(-10), 7+(-5), 7+0, 7+5, 7+10, 7+15, 7+20, \ldots\}$

$= \{\ldots, -13, -8, -3, 2, 7, 12, 17, 22, 27, \ldots\}$.

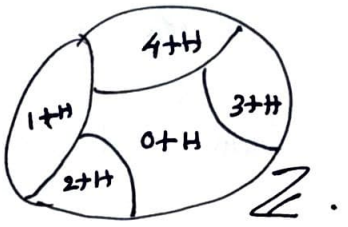
$\cdots = -5+H = 0+H = 5+H = 10+H = \cdots$ (original)

$\cdots = -4+H = 1+H = 6+H = 11+H = \cdots$

$\cdots = -3+H = 2+H = 7+H = 12+H = \cdots$

$\cdots = -2+H = 3+H = 8+H = 13+H = \cdots$

$\cdots = -1+H = 4+H = 9+H = 14+H = \cdots$



Observation:

1) 12 and 7 are different, but
$7+H = 12+H$

2) All five distinct cosets form a partition for $\mathbb{Z}$.

Property: Let $H \leq G$, and let $a, b \in G$. Then
$aH = bH$ if and only if $a^{-1}b \in H$.

Verification: Suppose $\boxed{aH = bH.}$

To show $a^{-1}b \in H$.

Let $ah_1 \in aH = bH$.

$\Rightarrow ah_1 = bh_2$ for some $h_2 \in H$.

$\Rightarrow \underbrace{a^{-1}a}_{e} h_1 = a^{-1}b h_2$ (pre multiply with a^{-1})

$\Rightarrow e h_1 h_2^{-1} = a^{-1}b \underbrace{h_2 h_2^{-1}}_{e}$ (post multiply with h_2^{-1})

$\underbrace{h_1 h_2^{-1}}_{\in H}$

$\Rightarrow \boxed{a^{-1}b \in H}$.

In case of additive group: $a+H = b+H \iff a-b \in H$.

Converse: Suppose $\boxed{a^{-1}b \in H.}$

To show $aH = bH$.

Let $a^{-1}b = h$ (for some $h \in H$)

$\Rightarrow \underbrace{a a^{-1}}_{e} b = ah \in aH$.

$\Rightarrow b \in aH$.

$\Rightarrow \boxed{bH = aH}$ (by property).

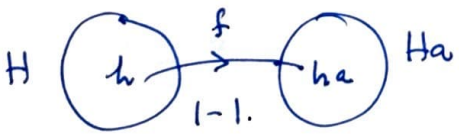
Properties: (cosets).

Let H be a subgroup of G, and let $a, b \in G$. Then

1) $a \in aH$
2) $aH = H \iff a \in H$
3) $aH = bH$ or $aH \cap bH = \phi$
4) $aH = bH \iff a^{-1}b \in H$
5) $|aH| = |bH|$
6) $aH = Ha \iff H = aHa^{-1}$
7) aH is a subgroup of $G \iff a \in H$.
8) $a \in Hb \Rightarrow Ha = Hb$

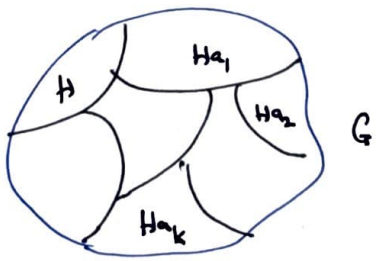
Lagrange's: If G is a finite group and H a subgp of G. Then the order of H divides order of G.

Proof: Let $|H| = n$, and the number of left cosets of H in G is k.



By property ..., $|H| = |Ha|$ for any $a \in G$.

Therefore $|Ha| = n$.



k : cosets wrt H.

→ All the cosets of H have the same number of elements, say $|H|$.

→ The distinct cosets of H form a partition. (they cover all of G without overlapping).

Therefore $G = H \cup Ha_1 \cup \cdots \cup Ha_k$ (all are distinct)

$$|G| = |H| + |Ha_1| + \cdots + |Ha_k| \quad \leftarrow k \text{ in number, each has } n \text{ elements.}$$
$$= k \cdot n$$

Objective Questions

1) Let $(G = \{1, -1, i, -i\}, \cdot)$ be a gp. Then the inverse of $\begin{cases} i = \underline{-i} \\ -i = \underline{i} \end{cases}$

2) Let $(G = Z_n = \{0, 1, 2, \cdots, (n-1)\}, +_n)$ be a gp. Then the inverse of $j > 0$ is $= \underline{n-j}$

$(Z_{12}, +_{12})$, inverse of $7 = \_\_$

" $9 = \_\_$

3). Let $U(n) = \{x \in Z^+ \mid x < n, (x, n) = 1\}$. Then

Inverse $\begin{cases} 7 \text{ in } U(10) \text{ is } \underline{3} \\ 9 \text{ in } U(10) \text{ is } \underline{9} \\ 3 \text{ in } U(10) \text{ is } \underline{7} \end{cases}$

$U(10) = \{1, 3, 7, 9\}$ is a gp with "mod 10"

4) $(Z_4, \cdot_4)$ is a group ☐ YES ☑ NO (2 has no inverse)

5) Let $(G = U(n), \cdot \bmod n)$, then the inverse of each 'k' is .

Solution to $kx \equiv 1 \bmod n$.

6) order of $11 \in U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ under "mod 15"

is $\underline{2}$ (since $11^1 = 11$, $11^2 = 121 \pmod{15} = 1$) ② order.

7). Centre: $Z(G) = \{a \in G \mid ax = xa \ \forall x \in G\}$.

Is centre of G is a subgroup ? ☐ Yes ☐ No.

If G is abelian, then its centre $\underline{G}$

8) $Z_{10} = \langle 3 \rangle$ (additively!)

$= \langle 7 \rangle$

$= \langle 9 \rangle$

Is $Z_{10} = \langle 2 \rangle$ ___

9) $(\mathbb{Z}, +)$ is cyclic. Generators.

1 $\qquad$ -1.

$1+1+1+\cdots$ $\qquad$ $(-1)+(-1)+\cdots$

$|n|$ times.

10) $U(10) = \{1,3,7,9\}$. cyclic (multiplicative gp mod 10.) Yes.

3 generators 7

$\{3^0, 3^1, 3^2, 3^3\}$. $\qquad$ $\{7^0, 7^1, 7^2, 7^3\}$.

$3^3 = 7$

11) $U(8) = \{1,3,5,7\}$ NOT cyclic

$\langle 1\rangle = \{1\}$, $\langle 3\rangle = \{3,1\}$, $\langle 5\rangle = \{5,1\}$ $\langle 7\rangle = \{7,1\}$.

12) List of all subgps of $\mathbb{Z}_{30}$. (additively)

$\langle 1\rangle = \{0,1,2,\cdots,29\}$ order 30.

$\langle 2\rangle = \{0,2,4,\cdots,28\}$ order 15

$\langle 3\rangle = \{0,3,6,\cdots 27\}$, order 10

$\langle 5\rangle = \{0,5,10,15,20,25\}$ order 6

$\langle 6\rangle = \{0,6,12,18,24\}$ order 5

$\langle 10\rangle = \{0,10,20\}$ order 3

$\langle 15\rangle = \{0,15\}$ order 2. $\qquad$ $\langle 30\rangle = \{0\}$ order 1.

13). Generators of $\mathbb{Z}_n$:

k is a generator of $\mathbb{Z}_n \iff \gcd(k,n) = 1$

Questions: Generators of $\mathbb{Z}_6$

" " $\mathbb{Z}_{36}$

" " $\mathbb{Z}_{24}$.

14) $\phi(n)$: Number of positive integers $< n$ and relatively prime to n.

$$\boxed{|U(n)| = \phi(n)}$$

15) If d is a positive divisor of n, then the number of elements of order d in a cyclic group of order n is $\underline{\phi(d)}$.

Ex. List all the elements of $\mathbb{Z}_{40}$ that have order 10.

16) Write all subgroups of S_3 = {symmetries of a Δ^{le}}.

17). List elements of the subgps $\langle 3 \rangle$ and $\langle 15 \rangle$ in $\mathbb{Z}_{18}$.

18) Give an example of a non cyclic group, all of whose proper subgps are cyclic.

$S_3 = D_6 = \{1, r, r^2, sr, sr^2, s\}$.

Note: In a group G, each element has unique inverse.

ie: Suppose x is invertible
x' rt. inverse
x'' left inverse.
$\Rightarrow x' = x''$.

Pf. By hypo. $x * x' = e$
$x'' * x = e$

Now $x' = e * x'$
$= (x'' * x) * x'$
$= x'' * (x * x')$
$= x'' * e.$
$= x''.$

Thus inverse to each element is unique.

Note: In a group, identity element is unique.