Cayley Table

eg. $r \circ a \Rightarrow r$ following a

$\longleftarrow$ Order of action

a : reflect thru A
b : " " B
c : " " C
r : 120° c/w rotation
s : 120° cc/w rotation
e : Identity.

240° rotation returns to S.

Choose : Column first then row

$\circ$	e	r	s	a	b	c
e	e	r	s	a	b	c
r	r	s	e	b	c	a
s	s	e	r	c	a	b
a	a	c	b	e	s	r
b	b	a	c	r	e	s
c	c	b	a	s	r	e

$\longleftarrow$ Symmetry group of $\triangle ABC$.

A group comprises a set G (whose members are the elements of the group) and an operation $*$ on this set which together satisfy 4 properties :

1) Closure
2) Identity
3) Inverse
4) Associativity.

① Closure

given any 2 elements $g, h \in G$, then the operation gives us an element $g * h$ which is required to be an element of G

We say ~~grou~~ set G is closed under operation $*$.

② <u>Identity</u>

$\exists e \in G : g * e = e * g = g$

ie. e is an identity for $*$

③ <u>Inverse</u>

g^{-1} must be an element of G too.

$\forall g \in G \Rightarrow \exists g^{-1}_{(\in G)} : g * g^{-1} = g^{-1} * g = e$

④ <u>Associativity</u>

given $g, h, k \in G$ we have $g*(h*k) = (g*h)*k$

⑤ Abelian group

→ where commutativity is satisfied

ie. $g * h = h * g$

If set G and operation $*$ satisfy the 4 group axioms then we say $(G, *)$ is a group under operation $*$

<u>For Symmetry group of $\triangle ABC$ (figure F)</u>

① $G = \{e, r, s, a, b, c\}$

For any Symmetry g, h of F $g \circ h$ is also a symmetry of F

$\Rightarrow$ Axiom of closure is satisfied under operation $\circ$

② Inverse exists

ie. $s = r^{-1}$: $\cancel{s \circ r^{-1} = e}$

and $r = s^{-1}$: $\cancel{r \circ s^{-1} = e}$

③ Identity element exists

~~$s \circ p^{-1}$~~

$s \circ s^{-1} = s \circ r = e$

④ Associativity holds

$(a \circ b) \circ r = s \circ r = e$

$r \circ (s \circ a) = r \circ c = a$

1) Prove the integers $\mathbb{Z}$ form a group under addition.
ie. Show $(\mathbb{Z}, +)$ is a group.

Closure

Given $m, n \in \mathbb{Z} \Rightarrow (m+n) \in \mathbb{Z}$

Formally

Theorem

$\forall m,n \in \mathbb{Z}, (m+n) \in \mathbb{Z}$

$\Rightarrow$ The integers are closed under addition.

Identity

$\forall m \in \mathbb{Z}, m + 0 = m$ where 0 is the identity element for the operation $+$.

Inverse

$(\exists -n \in \mathbb{Z} :)$

$\forall n \in \mathbb{Z}, n + (-n) = 0$ where $-n \in \mathbb{Z}$

Associativity

$\forall n,m,p \in \mathbb{Z} \quad (n+m)+p = n+(m+p)$

Show $(\{0,1,2\}, +_3)$ where $+_3$ is addition modulo 3

ie. $2 +_3 2 = 1$

$\hookrightarrow 3 \overline{\big) 2+2} = 3 \overline{\big) 4} \Rightarrow$ Remainder 1

$+_3 \Rightarrow$ Addition
Divide by 3
Take remainder.

Modulo
$0 \bmod 3 = 0$
$1 \bmod 3 = 1$
$2 \bmod 3 = 2$
$3 \bmod 3 = 0$
$4 \bmod 3 = 1$

1) Closure

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Since only members of the set appear in the Cayley table
$\Rightarrow$ Axiom of closure is satisfied.

2 ~~Inverse~~ Identity
0 is the identity element $\longrightarrow$ leaves other element unchanged.
$m +_3 0 = 0 +_3 m = m$

3 Inverse $\longrightarrow$ Returns Identity when composed.
$0 +_3 0 = 0 \Rightarrow 0$ is the inverse of 0
$1 +_3 2 = 0 \Rightarrow 1$ is the inverse of 2

$$\boxed{l +_3 (m +_3 n) = (l + m + n) \bmod 3}$$

4) <u>Associative.</u>

~~$1 +_3 2$~~

Both $l +_3 (m +_3 n)$ and $(l +_3 m) +_3 n$ are the remainder of $(l+m+n) \bmod 3$ and are hence equal.

↳ Use this general argument instead of checking for each element.

<u>NON - EXAMPLES OF A GROUP</u>

↳ Need to show one of the axioms fail.

1) The set of integers under the operation of multiplication. $(\mathbb{Z}, \times)$

1) Closure - The integers are closed under multiplication
ie. $\forall m,n \in \mathbb{Z} \Rightarrow (m \times n) \in \mathbb{Z}$

Proof

- 1^{st} : Define -ve integers
- 2^{nd} : Use peano's axioms for $n+1$ then define multiplication.
- 3^{rd} : Strong Induction.

② Associativity
$\forall n,m \in \mathbb{Z} \quad n \times m = m \times n$

③ Identity
↳ 1
$\forall n \in \mathbb{Z} \quad n \times 1 = 1 \times n = n$

$0 = 1 * (2 * 3)$
$4 = (1 * 2) * 3$

0 2

④ Inverse
$\nexists n \in \mathbb{Z} : n \times n^{-1} = e = 1$

∴ Since Inverse property fails $\Rightarrow (\mathbb{Z}, \times)$ is not a group.

3/ Show that $(\mathbb{Z}, *)$ is not a group where $*$ is the operation defined by
$n * m = nm - n - m + 1$.

Closure (satisfied) ✓
Associativity? X
Identity?
Inverse?

Associativity

$a*(b*c) \overset{?}{=} (a*b)*c$

$a*(b*c)$
$= a*(bc - b - c + 1)$
$= abc - a - (bc - b - c + 1) + 1$
$= abc - bc - a + b + c$

$(a*b)*c$
$= (ab - a - b + 1)*c$
$= abc - c - (ab - a - b + 1) + 1$
$= abc - ab - c + a + b$

Since $a*(b*c) \neq (a*b)*c$
$\Rightarrow$ Associativity fails.
(Hence $(\mathbb{Z}, *)$ is not a group)

Identity

Does an element e exist such that
$n * e = n$?

$n * e = n$

$ne - n - e + 1 = n$

$\cancel{n(2 - e) = 1 + e}$

$e(n-1) = (2n-1) \implies e = \dfrac{2n-1}{n-1}$

$\cancel{e} = \dfrac{2(\cancel{n-1})}{\cancel{n-1}}$

$= \dfrac{n + n - 1}{n-1}$

$\cancel{e = 2}$

$\dfrac{2\cancel{n} - n \cancel{- 2} + \cancel{1}}{n}$

$= \dfrac{n}{n-1} + 1$

$n = 2 \Rightarrow e = 3$

$\Rightarrow 2 * 3 \overset{!}{=} 2$

$2 \times 3 - 2 - 3 + 1 =$

$6 - 5 + 1 = 2$

e is the identity only ~~when~~ for $n = 2$

$\Rightarrow$ Identity does not exist

$\Rightarrow (\mathbb{Z}, *)$ is not a grop.

Soln 2

Suppose q is an identity

$\therefore\ q * n = n \quad \forall n \in \mathbb{Z}$

taking $n = 0$ (Not rigorous)
we have

$q \times 0 - q - 0 + 1 = 0$

$\Rightarrow q = 1$

But then $q * 1 = 1 - 1 - 1 + 1 = 0 \neq 1$

$\Rightarrow q$ is not an identity.

Invertibility

For $(\mathbb{Z}, *)$ | $n * m = nm - n - m + 1$

We need one s.t

$a * b = e$ and $b = a^{-1}$ and e denotes the identity element.

No identity $\Rightarrow$ No inverse.

Is $(\mathbb{Z}, \times)$ a group where $\times$ denotes integer multiplication.

Identity

We need $e \in \mathbb{Z}$ s.t
$a \times e = a$ where $a \in \mathbb{Z}$
$e = a/a = 1$
$\Rightarrow 1$ is the identity element for the integers under operation addition.

Invertibility

$(\exists b \in \mathbb{Z})$
~~$\forall a \in \mathbb{Z}$~~
$\forall a, b \in \mathbb{Z}$ we need $a \times b = e \mid b = a^{-1}$ and $e = 1$ in $(\mathbb{Z}, \times)$
$a \times a^{-1} = 1$
$a^{-1} = 1/a \notin \mathbb{Z}$

(More rigorously required)

$\Rightarrow$ Invertibility fails

$\boxed{a \times a^{-1} = e}$

$\cancel{a \times a^{-1} = e}$
$\cancel{a^{-1} \times a x = e x}$
$a \times a^{-1} = e$
$\cancel{a^{-1} \times a \times a^{-1} = e \times a^{-1}}$
e

* explain $\mathbb{N}$, $S: \mathbb{N} \mapsto \mathbb{N} : S(n) = n+1$ and $0 \in \mathbb{N}$

Associativity

$(\mathbb{Z}, \times)$ where $\times$ denotes Integer multiplication

implies set P is closed under s.

$\forall a, b, c \in \mathbb{Z} \mid a \times (b \times c) = (a \times b) \times c$

---

* Natural numbers ($\mathbb{N}$)
Peano's axioms

In this case S is a binary relation which associates one element of P to only one other element in P.

Let there be a given set P and a mapping $s : P \mapsto P$ and a distinguished element 0.
implies 0 is an element of P.

(P3) $\forall m, n \in P : S(m) = S(n) \Rightarrow m = n$
implies S is injective
that is the output uniquely determines its input.
Defn of injection
$\forall x_1, x_2 \in \mathrm{Dom}(f) : f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

* eg. $\forall x, a, b \in \mathbb{N}$
① Let $f : x \mapsto x + 2$
$\Rightarrow f(a) = f(b)$
$\Rightarrow a + 2 = b + 2$
$\Rightarrow a = b$

Defn of multiplication as repeated addition.
~~Peano~~

?? multiplication is repeated addition.

② Let $g : x \mapsto 2x$
$g(a) = g(b)$
$2a = 2b$
$\Rightarrow a = b$

$\subseteq$: Subset $\subset$. Proper subset.

Induction : Seperate observation $\rightarrow$ General conclusion

Deduction : General Principle $\rightarrow$ Specific conclusion

Defn of addition (in $\mathbb{N}$)

A Peano Structure $(P, 0, s)$ comprises a set P with a Sucessor mapping $s : P \mapsto P$ and a non Sucessor element 0.
The three are required to satisfy Peano's axioms
The mapping $s : P \mapsto P$ is called the sucessor mapping on P
The image element $s(x)$ of s is called the sucessor of x.

Sucessor mapping on Natural numbers
Let $\mathbb{N}$ be the set of naturals
Let $s : \mathbb{N} \mapsto \mathbb{N}$ be the mapping defined as
$s = \{ (x,y) \mid x \in \mathbb{N}, y = x+1 \}$

Addition in Peano Structure
Let ~~(P, S, 0)~~ $(P, 0, s)$ be a Peano structure
The binary operation $+$ is defined on P as follows

$$\forall m,n \in P : \begin{cases} m+0 = m \\ m+s(n) = s(m+n) \end{cases}$$

$\longrightarrow$ $m = 2 \quad n = 3$
$s(n) \overset{def}{=} n+1 = 4$
$m+s(n) = 2+4 = 6$
$s(m+n) = m+n+1$
$= 2+3+1$
$= 6$

This operation is called addition.

Defn of multiplication (in $\mathbb{N}$)

Let $+$ denote addition.

also multiplication can be defined as follows:
$\forall m,n \in \mathbb{N} : m \times n := +^n m$
where $+^n m$ denotes the n^{th} power of m under addition.

The binary operation $\times$ is recursively defined on $\mathbb{N}$ as follows.

$$\forall m,n \in \mathbb{N} \begin{cases} m \times 0 = 0 \\ m \times (n+1) = m \times n + m \end{cases}$$

This operation is called multiplication.

(P4) $\forall n \in P : s(n) \neq 0$ $\quad$ 0 is not the image of s
ie. 0 is not the sucessor to any element in P.

PBI

(P5) Principle of mathematical induction.

$$\forall A \subseteq P : (0 \in A \land (\forall z \in A : s(z) \in A)) \Rightarrow A = P$$

$\uparrow$ Subset

$\hookrightarrow$ Any subset A of P containing 0 and closed under S is equal to P.

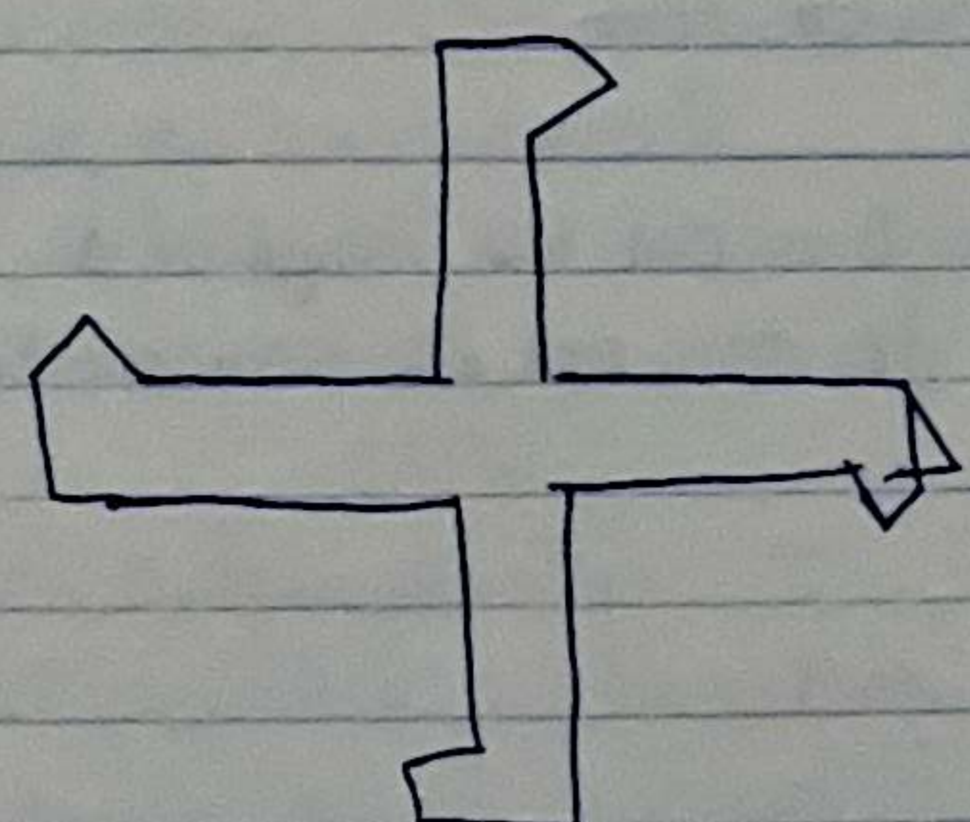
↗ late.

Inverse Completion of Natural numbers.

14 b

1(a) Symmetry → figure "look the same"
ie. occupy the same region of space.

Symmetry group of 4 blade windmill.



No reflection

e : identity
$r_{\pi/2}$: 90° rotation c/w
r_{π}^{2} : 180° rotation c/w
$r_{-\pi/2}$: 90° rotation cc/w
$r_{-\pi}$: ~~180°~~ rotation ~~c/w~~
$r_{3\pi/2}$: 270° c/w rotation. cc/w

Cayley table to find the inverse of the symmetry group.

o

14b

1(a) Symmetry group of 4 - blade windmill.

e = identity
$r_1 = 90°$ rotation c/w
$r_2 = 180°$ rotation c/w
$r_3 = 270°$ rotation c/w

Why not include 360° rotation and anti-clockwise rotations?

~~$r_1^{-1} =$~~
~~$e^{-1} = e$~~

~~$r_1^{-1} = r^3$~~

Inverse is defined such that
$a \circ b = e$

Let initial posn be defined for identity e.

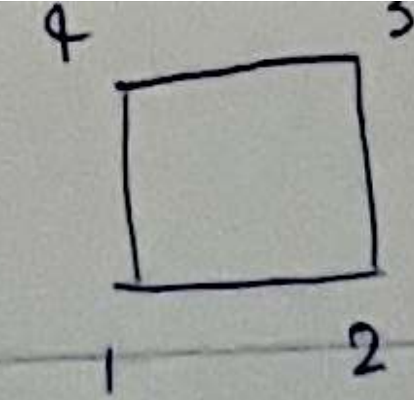
$e^{-1} = e$

$r_1 \circ r_3 = e$
$\Rightarrow r_1^{-1} = r_3$

$r_2 \circ r_2 = e$
$\Rightarrow r_2^{-1} = r_2$

$r_3 \circ r_1 = e$
$\Rightarrow r_3^{-1} = r_1$

In the group of Symmetry, we do NOT encode the action of (for eg.) rotating the object by 90° but the (posn) state of the object after it has undergone rotation
ie. $r_{\pi/2}$ represents the state of the object after it has undergone $r_{\pi/2}$ (state must also be a symmetry).
we do not include 360° rotation as:
$r_{360} = e$ (no need to include twice in a group) (An element appears only once in a group)?? Yes. Due to set.
$r_{\pi/2} = r_{-\frac{2\pi}{3}}$
Same as 270° cc/w rotation.



Symmetry group of a Square

Find inverses : $\boxed{a \circ b = e \quad \text{where } b = a^{-1}}$

Square will have $2n = 2(4) = 8$ symmetries

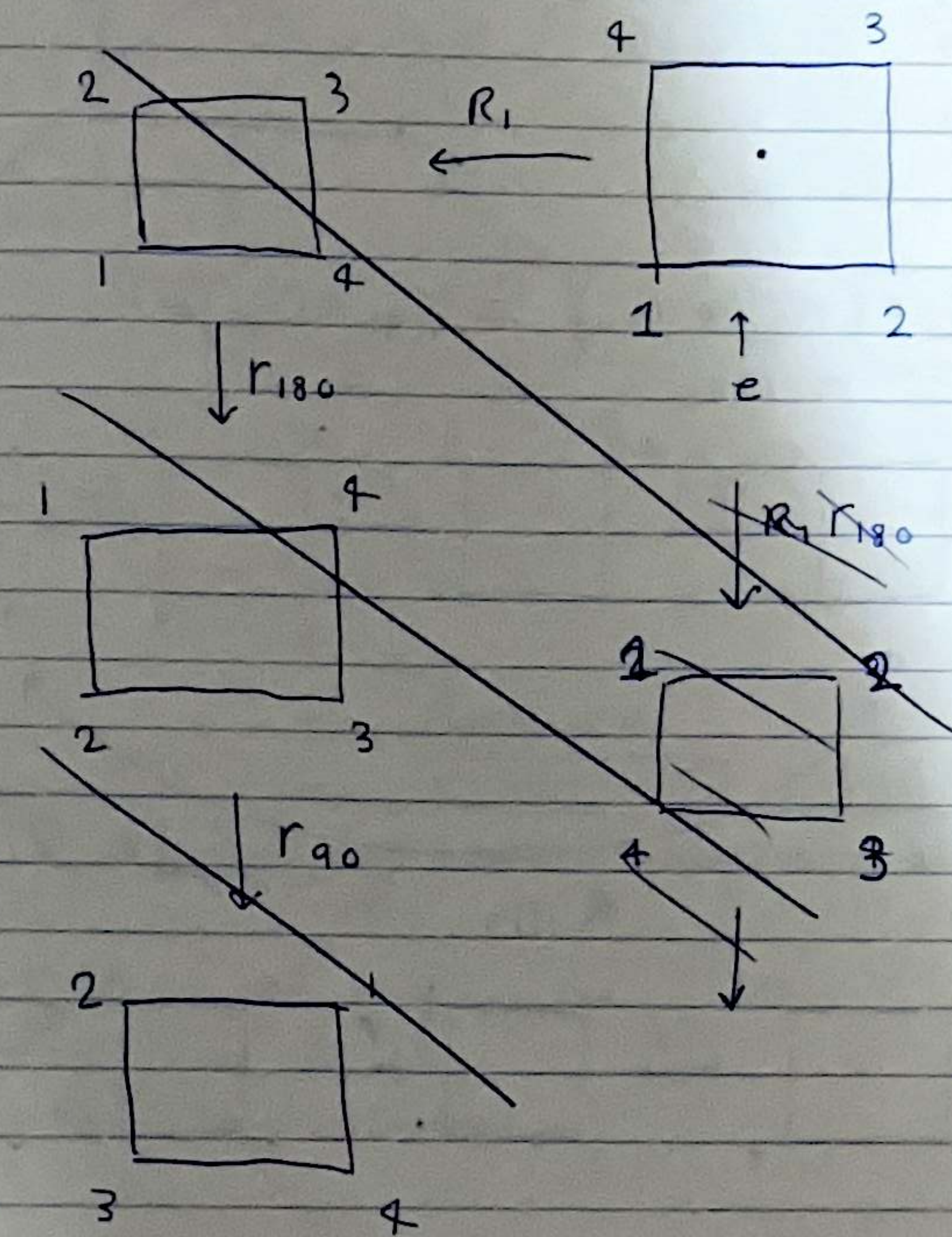
e	$e^{-1} = e$	Inverse of All Symmetries of Square.
c/w 90°	$r_{90}^{-1} = r_{270}$	
c/w 180°	$r_{180}^{-1} = r_{180}$	
c/w 270°	$r_{270}^{-1} = r_{90}$	
reflect thru vertex 1	$R_1^{-1} = R_1$	
,, vertex 2	$R_2^{-1} = R_2$	
median Hor ~~vertex 3~~	$R_{m_1}^{-1} = R_{m_1}$	
median Ver ~~vertex 4~~	$R_{m_2}^{-1} = R_{m_2}$	

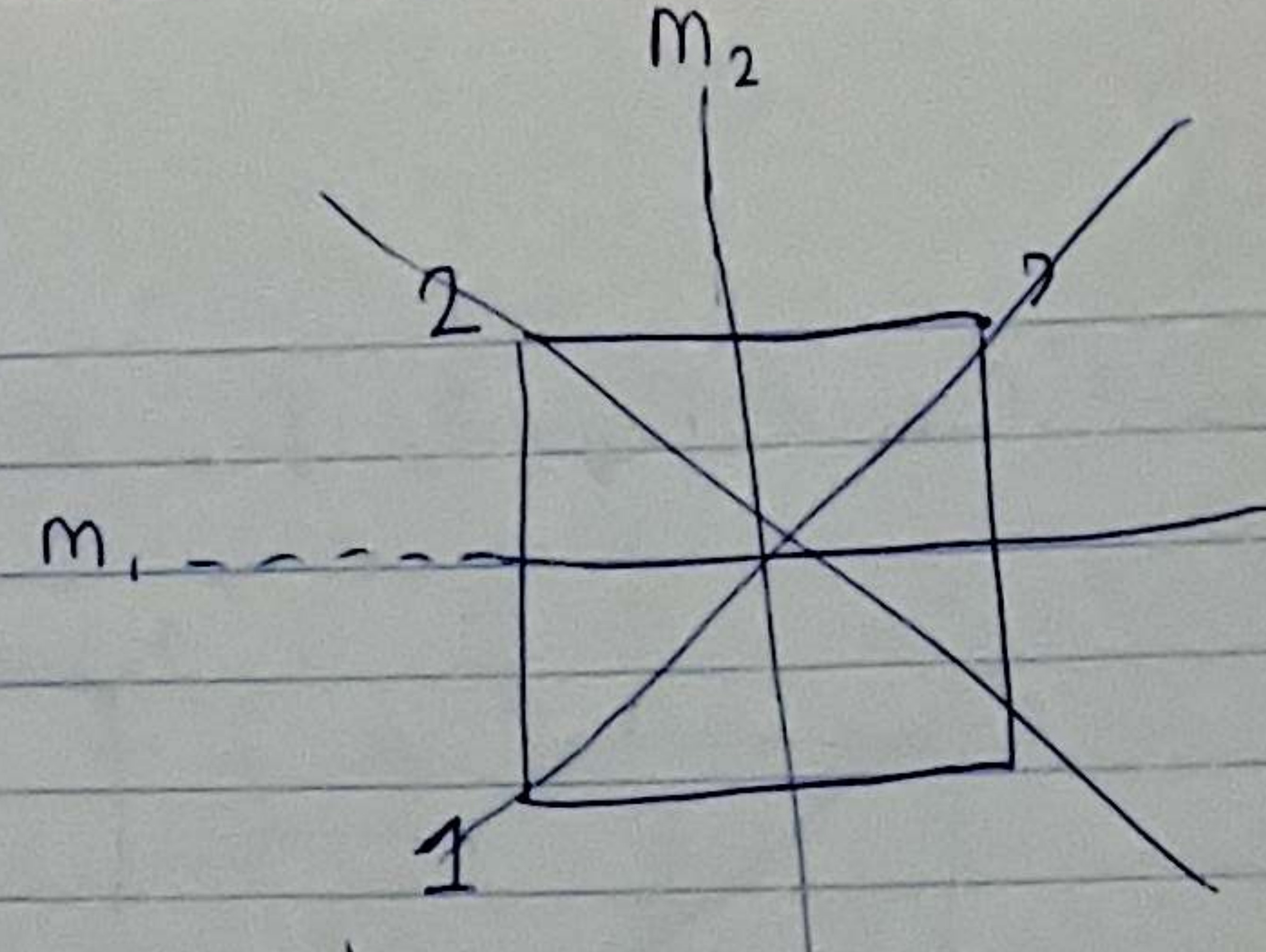
Check 3 cases for associativity of the symmetry group of square

$$(r_{90} \circ r_{180}) \circ r_{270} \overset{!}{=} r_{90} \circ (r_{180} \circ r_{270})$$
$$= r_{180} \qquad\qquad = r_{180}$$

$\Rightarrow$ Associative

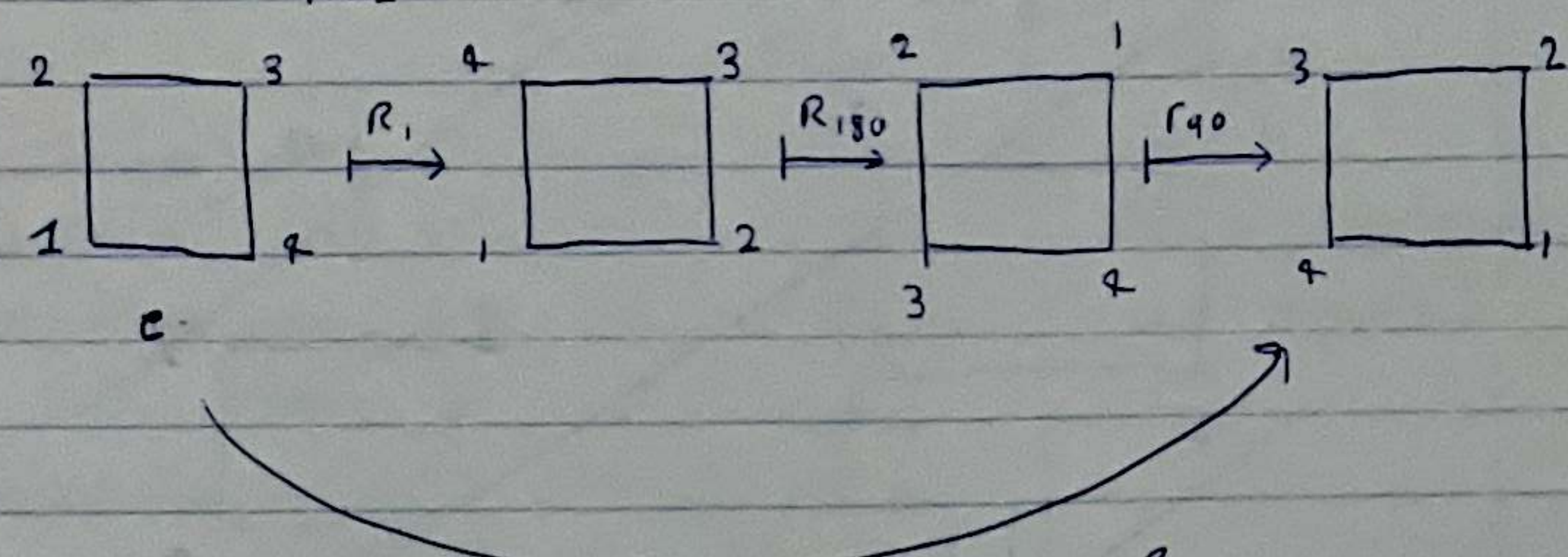
$$r_{90} \circ (r_{180} \circ R_1) \overset{!}{=} (r_{90} \circ r_{180}) \circ R_1$$



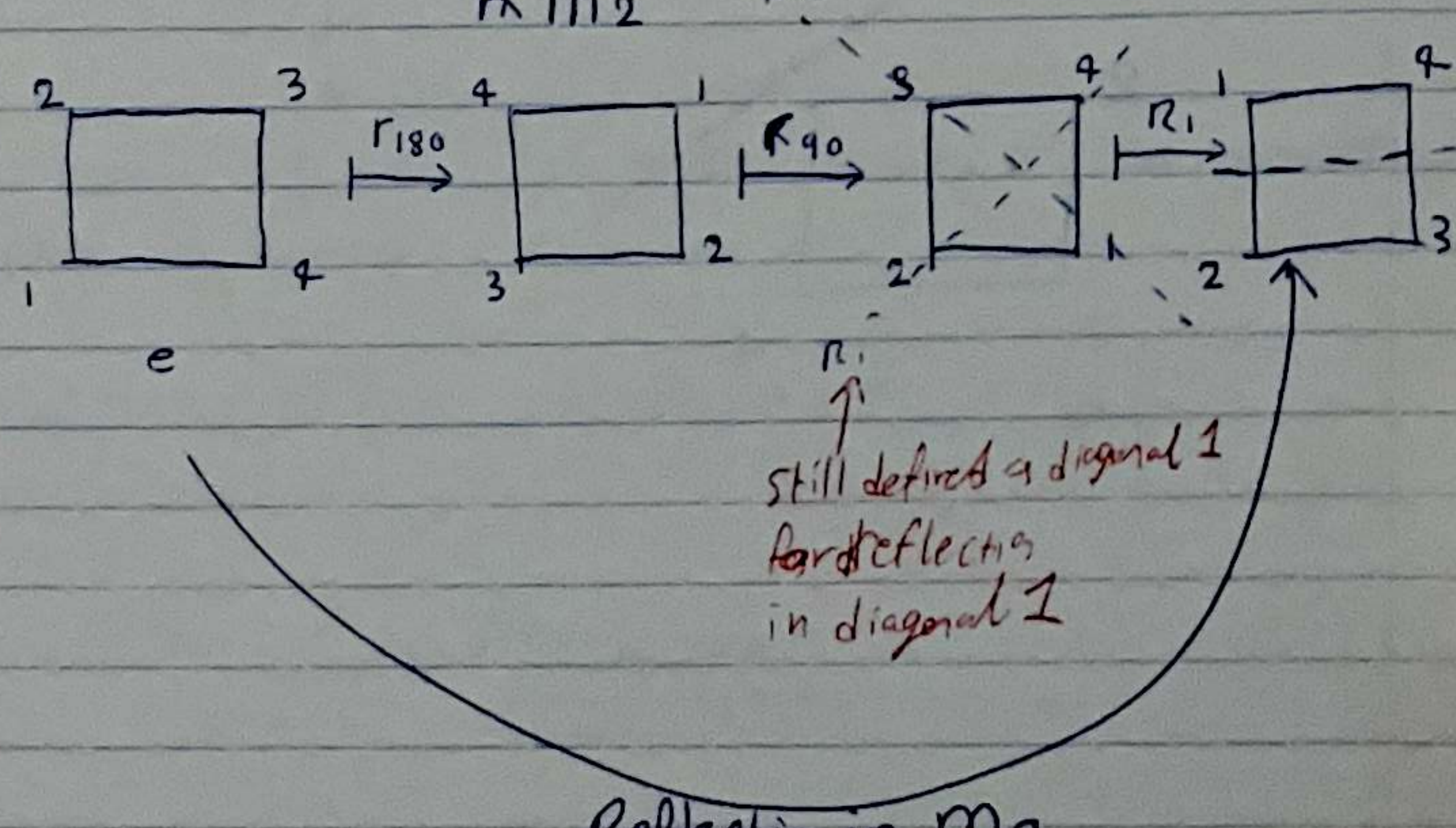


$$r_{90} \circ (r_{180} \circ R_1) \stackrel{!}{=} (r_{90} \circ r_{180}) \circ R_1$$

$= m_2$ $\qquad$ $=$



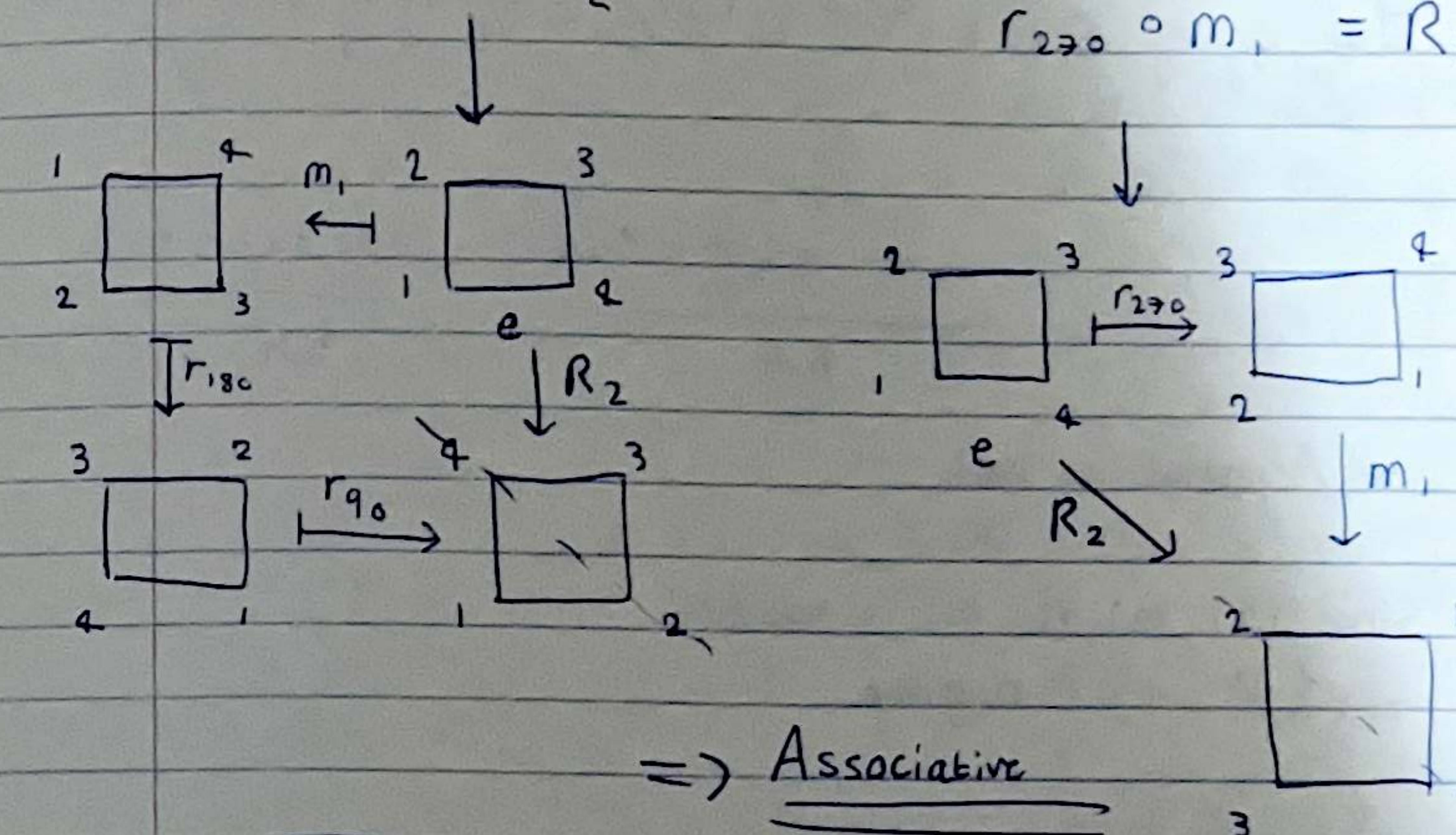
m_2 this is diagonal R_2



$\Rightarrow$ Associative.

$$r_{90} \circ (r_{180} \circ m_1) \stackrel{!}{=} (r_{90} \circ r_{180}) \circ m_1$$

$= R_2$ $\qquad$ $r_{270} \circ m_1 = R_2$



$\Rightarrow$ Associative

Prove $(\mathbb{Q}, +)$ is a group where + denotes rational addition.

1) Closure

$\forall a/b, c/d \in \mathbb{Q} \mid \frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd} = \frac{e}{f} \in \mathbb{Q}$

$\Rightarrow$ Set $\mathbb{Q}$ is closed under operation +

2) Identity

$\exists x \in \mathbb{Q} \mid \forall a/b \in \mathbb{Q} \mid a/b + x = a/b$

$\Rightarrow x = 0$ is the identity element

0 is rational as it can be expressed as a fraction eg. $0 = \frac{0}{n}$ where $n \in \mathbb{R}$

3) Invertibility

$\exists x \in \mathbb{Q} \mid \forall a/b \in \mathbb{Q} \mid a/b + x = e = 0$

$\Rightarrow x = -a/b$ is the additive inverse of a/b

K is rational for $k \in \mathbb{N}$ as $k = k/1 \Rightarrow k \in \mathbb{Q}$

4) **Associativity**

$$\forall a/b, c/d, e/f \in \mathbb{Q} \mid (a/b + c/d) + e/f = a/b + (c/d + e/f)$$

$$\downarrow$$

$$\frac{adf + cbf + edb}{bdf} = \frac{adf + cbf + edb}{bdf}$$

$\Rightarrow$ Associativity holds

Since (1), (2), (3), (4) is satisfied
$\Rightarrow (\mathbb{Q}, +)$ is a group.

2 Show that $(\mathbb{Q}^*, \times)$ forms a group where $\mathbb{Q}^*$ denotes the set of rationals excluding zero and operation $\times$ denotes rational ~~integer~~ multiplication.

1) **Closure**

$$\forall a/b, c/d \in \mathbb{Q}^* \mid a/b \times c/d = \frac{ac}{bd} = e/f \in \mathbb{Q}^*$$

$\Rightarrow$ Set $\mathbb{Q}^*$ is closed under operation $\times$.

2) Associativity

$$\forall a/b, c/d, e/f \in \mathbb{Q}^* \mid (a/b \times c/d) \times e/f = a/b \times (c/d \times e/f)$$

$$= \frac{ace}{bdf} \qquad = \frac{ace}{bdf} \qquad \Rightarrow \text{Associativity } \underline{\text{holds}}$$

3) **Identity**

$$\exists x \in \mathbb{Q}^* \mid \forall a/b \in \mathbb{Q}^* \mid a/b * x = a/b$$

$$\Rightarrow x = (a/b)^{-1}(a/b) = 1$$ (Assuming Associativity holds) & Invertibility.

$\updownarrow$ interdependent.

4) **Invertibility**

$$\exists x \in \mathbb{Q}^* \mid \forall a/b \in \mathbb{Q}^* \mid a/b \times x = 1$$

$$\Rightarrow x = b/a$$

Since Group axioms 1 - 4 are satisfied $(\mathbb{Q}^*, \times)$ forms a group.

7) Prove that $(\{0,1,2,3\}, +_4)$ is a group where $+_4$ is defined by adding and taking the remainder on division by 4.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

~~$a+b \pmod 4$~~

$a+b = \quad (\text{mod } 4)$

$8 \bmod 4 = 0$

$3 \bmod 4 = 3$

$1 \bmod 4 = 1$

$n \bmod 4$

↳ General formula.

Or

$1 \bmod 4 = 4 \lfloor 1$ $\quad R = 1$

$2 \bmod 4 = 4 \lfloor 2$ $\quad R = 2$

$5 \bmod 4 = 4 \lfloor 5$ $\quad R = 1$

1) Closure

Only the elements $\{0,1,2,3\}$ are present in the Cayley table. These elements are the only ones constituting the set.

$\Rightarrow$ Closure is satisfied.

2) Identity

0 is the identity element.

3) Invertibility

All the elements returns identity when composed with their respective inverses.

4) Associativity

$(0 +_4 1) +_4 2 \overset{?}{=} 0 +_4 (1 +_4 2)$

$= 3 \pmod 4 \qquad = 3 \pmod 4$

$\equiv 0+1+2 = 3 \bmod 4$

$= 3$

Since these 2 are equal

$\Rightarrow$ Associativity holds

Since the group axioms are satisfied $\Rightarrow (\{0,1,2,3\}, +_4)$ is a group.

Is $(\{0,1,2\}, \times_3)$ a group.

$\times_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\Rightarrow$ Closure ✓

Associativity holds ✓

0 has inverse 0

~~Identity~~ Invertibility

$\forall x \in \{0,1,2\} \mid \exists y \mid x \times_3 y = 1$ where $y = x^{-1}$

Identity

$\exists x, y \in \{0,1,2\} : x \times_3 y = x \longrightarrow$ 1 is the identity element.

~~There is no identity element~~

$\Rightarrow (\{0,1,2\}, \times_3)$ is not a group.

↘ 0 has no inverse

9) $(\{1,2\}, \times_3)$ is a group.

Is $(\{1,2,3\}, \times_4)$ a group?

Associativity ✓ ⟹ $2 \times 2 = 4 \bmod 4 = 0 \notin$ Set
Closure ✗

Identity $= 1$ ✓

NO closure
NO invertibility

Invertibility

$x \times_4 y = 1$ ✓

x	y
1	1
2	2
3	3

2 & 3 have no inverse. ✓

11) Is $(\{e,a,b\}, \square)$ a group?

Also abelian

$(a \square b) \square b \overset{!}{=} a \square (b \square b)$
$b \square b \quad\quad = e$
$= e \quad\quad = a$
⟹ Not associative

Closure ✓
Identity ✓
Inverse ✓
Associative ?

Associative !?

$(a \square b) \square e \overset{!}{=} a \square (b \square e)$
$b \quad\quad = b$

⟹ Associative.

Note: DO NOT use e when checking for associativity.

12) Is $(\{x,y,z\}, *)$ a group?

Closure ✓
y is identity ✓
Inverse ✓

Associative ✓

⟹ Group.

13 Show $(\mathbb{Q}^*, \div)$ is not a group.

set of rationals excluding 0

$\boxed{a \circ e = e \circ a = a}$

a/b
Identity $= 1$
closure ✓
Inverse ✓
~~Associativity~~ ✗
~~There~~

$x \div e = x$
$\Rightarrow x = \frac{x}{e}$
$\Rightarrow e = 1$

Identity but then
$e \circ a = 1/a \neq a$
⟹ Identity fails

$\frac{a}{b} \div \left(\frac{c}{d} \div \frac{e}{f}\right) = \frac{a}{b} \div \frac{cf}{de} = \frac{ade}{bcf}$

$\left(\frac{a}{b} \div \frac{c}{d}\right) \div \frac{e}{f} = \frac{ad}{bc} \times \frac{f}{e} = \frac{adf}{bce}$

⟹ Associativity fails

Is $(\mathbb{Z}, *)$ a group?

$n * m = n + m - 1$

Closure ✓

$n * e = n$

~~$n * e = m + n - 1 = n$~~

For an imput n
Identity occurs for $m = n - 1$ ✓✓

$n * b = n - 1$
where $b = n^{-1}$

$\Rightarrow$ ~~inverse of n is $(n-1)$~~

~~this the inverse~~

$n * 1 = n$
$\Rightarrow$ 1 is the identity element ✓✓

$n * b = \underline{1}$

$n + b - 1 = 1$
$b = 2 - n$
$(2-n)$ is the inverse of n ✓✓

~~$5 * -3 \overset{!}{=} 5$~~
$5 * -3 \overset{!}{=} 1$
$= 1$

$2 * 3 * 4$
$(2*3)*4 \overset{!}{=} 2*(3*4)$
$7 \quad = 7$
$\Rightarrow$ Associative
$\Rightarrow$ Group.

--

Group of $\mathbb{Z}_n$ (Integers modulo n) under $+_n$

$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

Closure : The remainder ~~of~~ is a non-negative integers less than n ~~lies~~ lying in $\mathbb{Z}_n$

Identity : 0 is an identity for $+_n$
i.e. $p +_n 0 = 0 +_n p = p \equiv p + 0 = 0 + p = p \pmod{n}$

Invertibility : 0 is the inverse of 0
$\forall p > 0 \in \mathbb{Z}_n$
$p +_n p \overset{!}{=} 0$
$p +_n (n-p) = 0$
$\cancel{p} +_n n - \cancel{p} = 0$

$0 +_n n = 0$
$\Rightarrow (n-p)$ is the inverse of p. in $(\mathbb{Z}_n, +_n)$

Associativity
~~But~~ $p +_n (q +_n r) = (p +_n q) +_n r \equiv (p + q + r) \bmod n$

must satisfy axioms of group AND commutativity.

Abelian Groups

- These are groups where the binary operation is commutative for all the elements constituting the group.

ie. $G(S, \circ)$

$$\forall g,h \in G \mid g \circ h = h \circ g$$

eg. for $(\mathbb{Z}, +)$ is an abelian group as integer addition is commutative
ie $-2 + 3 = 3 + -2 = 1$

Cayley Table

$\circ$	x	y
x		$y \circ x$
y	$x \circ y$	

$\Rightarrow$ Cayley Table for Abelian groups are symmetric about the diagonal.

Permutations

(A well defined set)
A set is defined to be a collection of un-ordered, unique and immutable elements. (no duplicates)

A permutation on a set is a function which reorders the members of a set.

Consider the function f defined as follows

$$\begin{array}{ccc} 1 & \xrightarrow{f} & 2 \\ 2 & \longrightarrow & 1 \\ 3 & \longrightarrow & 3 \end{array}$$

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$ $\longrightarrow$ Permutation Symbol for f.

$$f : \begin{array}{ccc} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{array}$$

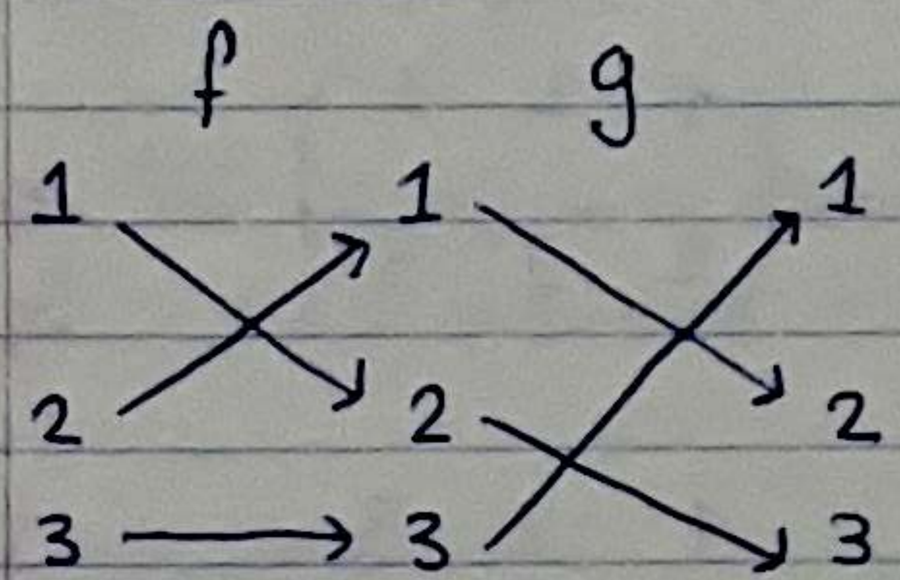
Note: Each element in a row appears only once in a permutation symbol.

↳ What if there is 2 similar elements in a set?

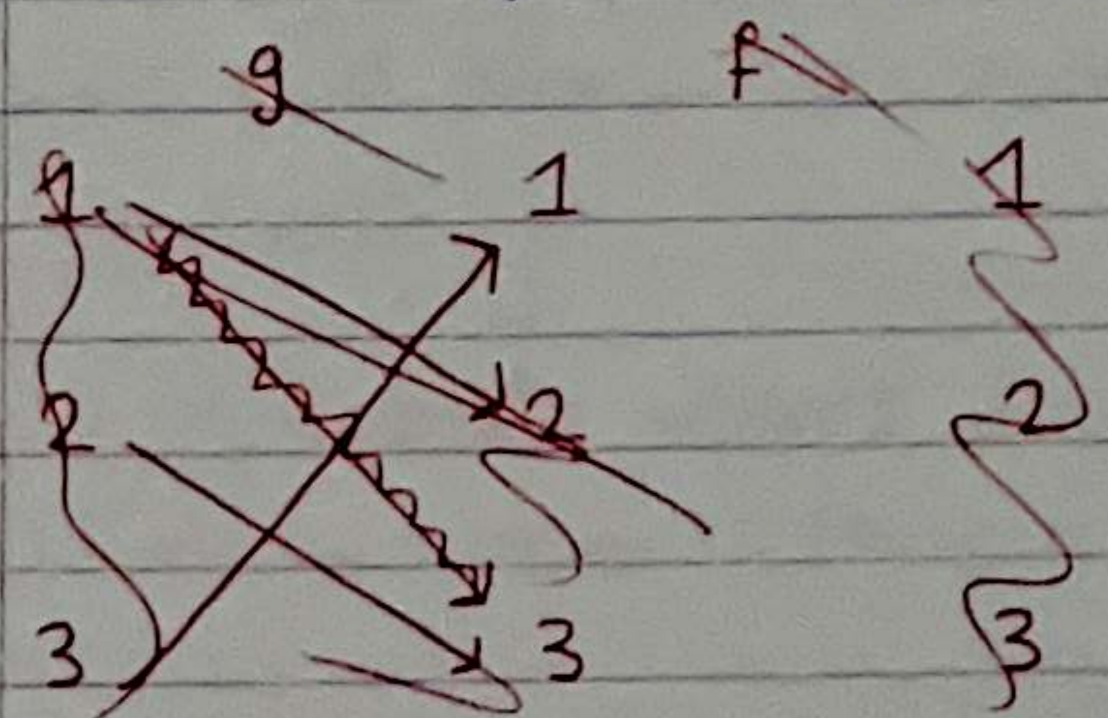
ie. $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 2 \end{pmatrix}$ is NOT a valid permutation.

Composition of Permutations

given : $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

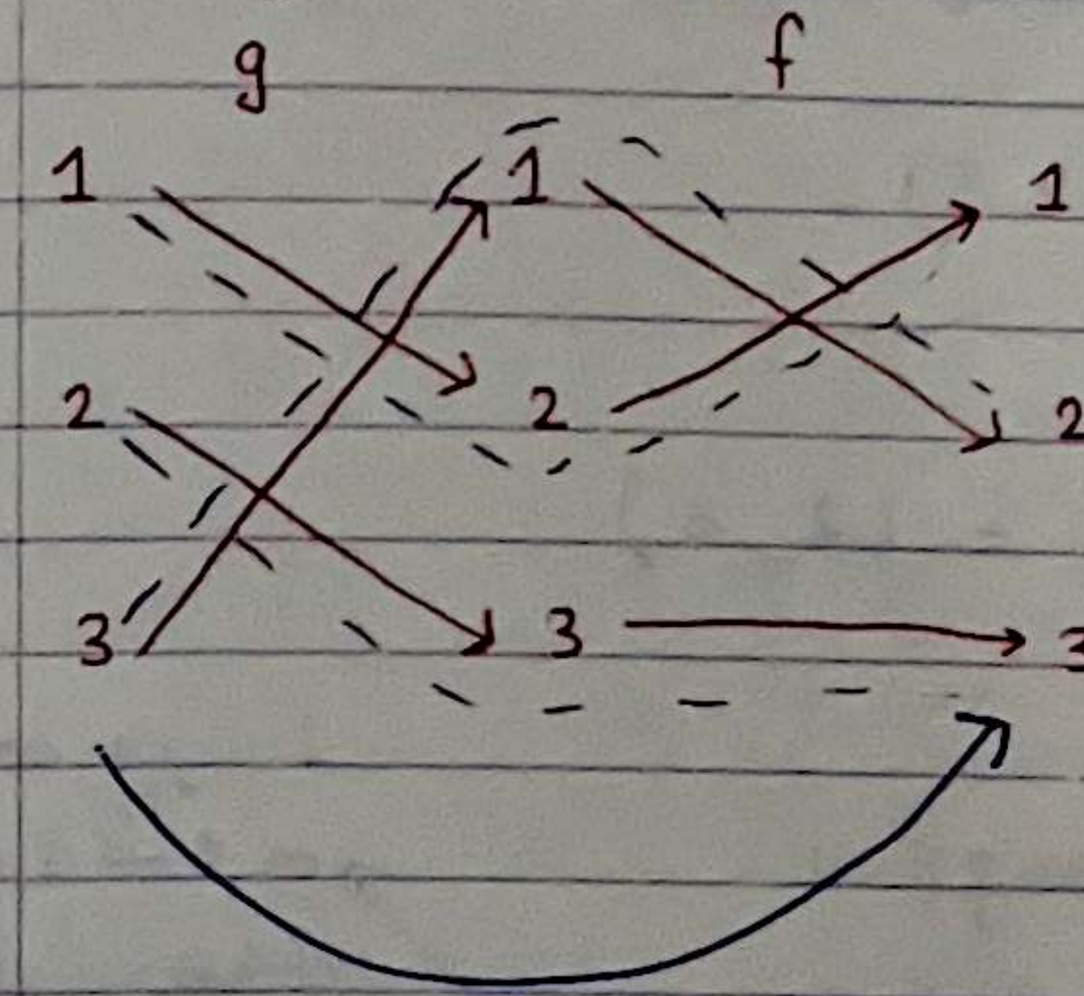


$\Rightarrow f \circ g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ ✗ We Compose g first



$\binom{3}{2} = \frac{3!}{2! \times 1!}$

$f \circ g$



$f \circ g$

$= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ ← A new Permutation.

Cycle Notation

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

↓ ↓

$(1\ 2)(3)$ $(1\ 2\ 3)$

↑

transposition

or 2-cycle

$f \circ g = (1\ 2) \circ (1\ 2\ 3) = \cancel{(1)}(3\ 2)$

Composition of Permutations in Cycle notation.

$f = (1\ 2)\cancel{(3)}$ $g = (1\ 2\ 3)$

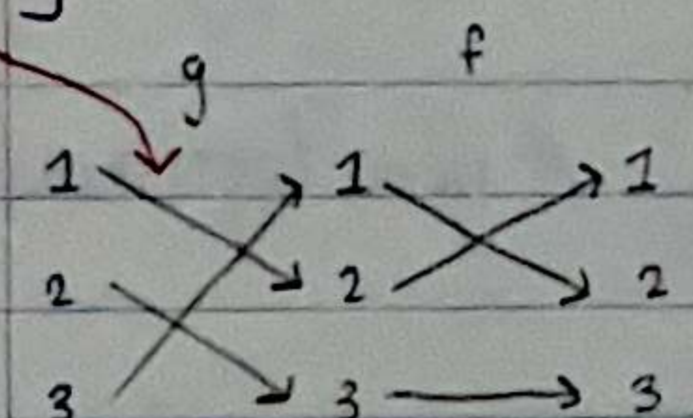
$f \circ g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3)$

We note: We must Compose g first

1-cycles are excluded as $1 \overset{f\circ g}{\mapsto} 1$ we do not consider it when writing cycle notation

1^{st} g sends 1 to 2 and f sends 2 to 1.

$g = (1\ 2\ 3)$



we only concern ourself with the action of g on one member

ie. For $1 \overset{g}{\mapsto} 2 \overset{f}{\mapsto} 1$

2^{nd} ~~3rd~~ g sends $\underset{=*}{2}$ to 3 and f sends 3 to $\underset{=*}{3}$

Consider these when writing cycle notation.

3^{rd} g sends $\underset{*}{\underline{\underline{3}}}$ to 1 and f 1 to $\underset{=*}{2}$

$\Rightarrow f \circ g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ ✓✓ $= (2\ 3)$

1^{st} 2^{nd} 3^{rd}

compont

14d 1

(a) $\overset{a}{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}} \circ \overset{b}{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} =$

1^{st} entry (1) 2^{nd} entry (2)

$(1\ 2\ 3) \circ (2\ 3)(1) = (2\ 1)(3)$

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

↑ If n is returned to itself after composition, then it is a 1-cycle.

Brackets denote a complete cycle. after composition.

$= \cancel{(1)}$

(b) $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2)$

$(1)(2)(3) \circ (1\ 3\ 2)$ ~~Equivalent??~~ YES

$= \cancel{13}\ (3\ 2\ 1)\ \cancel{(3\ 2\ 1)}\ \cancel{1\ 2}$

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

$\cancel{13}$

$\cancel{12}$

(a) $\cancel{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}}$

(b) $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2)$

$\cancel{(1)}\,\cancel{(2)}\,\cancel{(3)} \circ (1\,3\,2) = (1\,3\,2)$

$(1)(2)(3)$

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

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

Note: Order defined between the elements

eg. for $(1\,3\,2)$

1 follows 3 which follows 2 is what matters

ie. $(1\,3\,2) \equiv (2\,1\,3) \equiv (3\,2\,1)$

Order of cycle Changes the permutation.

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

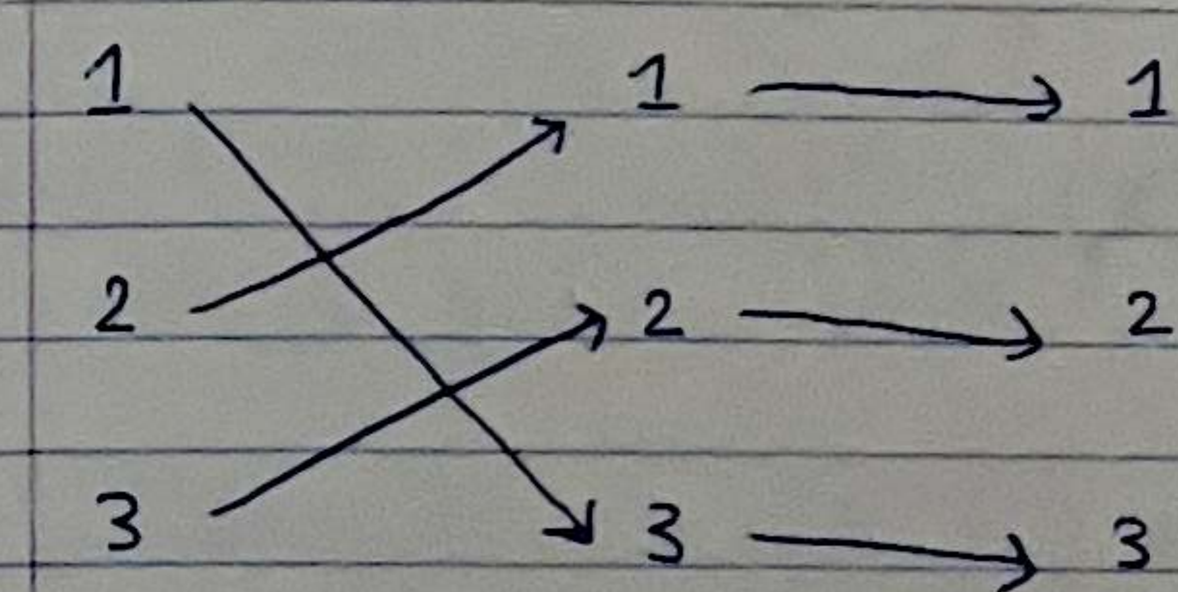
as 1 follows 3 in the first case and 1 follows 2 in the 2nd case.

a b

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

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

$(1\,3\,2)$



b sends 1 to 3 and a sends 3 to 3.

b sends 3 to 2 and a sends 2 to 2.

b sends 2 to 1 and a sends 1 to 1.

$\Rightarrow a \circ b = (1\,3\,2)$

$$\begin{array}{c} \\ \text{(c)} \end{array}\ \begin{array}{c} c \\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \end{array} \circ \begin{array}{c} d \\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \end{array} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$(1\ 2)(3) \circ (1\ 3\ 2)$

$c \circ d = (\cancel{1}\ 3)$

$= (1\ 3)\cancel{(2)}$

$= (1\ 3)$

(d) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ ✓

$(1\ 2)(3) \circ (1\ 3)(2) = (1\ 3\ 2)$ ✓

(e) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \cancel{(1\ 2\ 3)}$

$= (1)(2)(3)$

$= (1\ 3\ 2) \circ (1\ 2\ 3)$

$= (\cancel{1}\ 2)\cancel{(3)}$

$= (1)(2)(3)$

(f) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3)(2)$

$(1\ 3)(2) \circ (1)(2)(3)$

$= (1\ 3)(2)$

$$\begin{array}{c} \\ 2\text{ (a)} \end{array}\ \begin{array}{c} f \\ \begin{pmatrix} a & b & c & d \\ a & c & b & d \end{pmatrix} \end{array} \circ \begin{array}{c} g \\ \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix} \end{array} = \begin{pmatrix} a & b & c & d \\ c & a & d & b \end{pmatrix}$$

$(b\ c) \circ (a\ b)(c\ d)$

$= (a\ c\ d\ b)$

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

Steps : ① Write a first.
Notice a is sent to b (in g)
~~② Write b~~
Notice b is sent to c (in f)
② Write c
Notice c is sent to d (in g)
Notice d is a 1 cycle in f
③ Write d
Notice d is sent to c (in g)
Notice c is sent to b (in f)
④ Write b
Notice b is sent to a (in g)
Notice a is sent to a (in f)
⑤ Complete cycle.

(b) $\begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix} \circ \begin{pmatrix} a & b & c & d \\ a & c & d & b \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ b & d & c & a \end{pmatrix}$ ✓

$(a\ b)\ (c\ d) \circ (a)\ (b\ c\ d)$

$(a\ b\ d)\ \cancel{a}\ (c)$

$= \begin{pmatrix} a & b & c & d \\ b & d & c & a \end{pmatrix}$ ✓

---

3 (a) $(i)(j)$ ie. $\begin{pmatrix} i & j \\ i & j \end{pmatrix}$

(b) $\begin{pmatrix} i & j \\ j & i \end{pmatrix}$ ie $(i\ j)$

(c) $(i\ j)$ ie $\begin{pmatrix} i & j \\ j & i \end{pmatrix}$

(d) $\begin{pmatrix} i & j \\ j & i \end{pmatrix} \circ \begin{pmatrix} i & j \\ j & i \end{pmatrix}$

$(i\ j) \circ (i\ j)$

$= \cancel{(i\ j)}\ (i)(j)$

$= \cancel{\begin{pmatrix} i & j \\ j & i \end{pmatrix}} \begin{pmatrix} i & j \\ i & j \end{pmatrix}$

4) № of Possible permutations $= 3! = 6$ in $\{1\ 2\ 3\}$

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

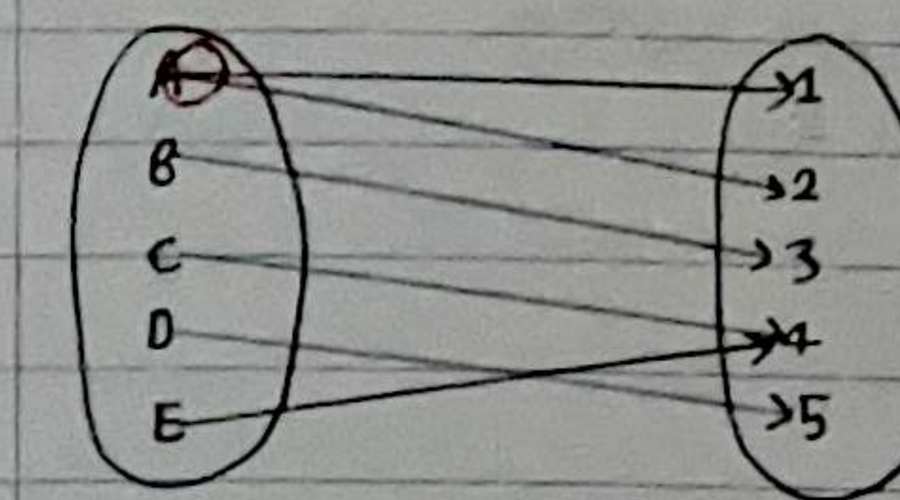
$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} (1)(2\ 3)$ $\quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} (1\ 2\ 3)$

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} (2)(1\ 3)$ Compose these Permutations

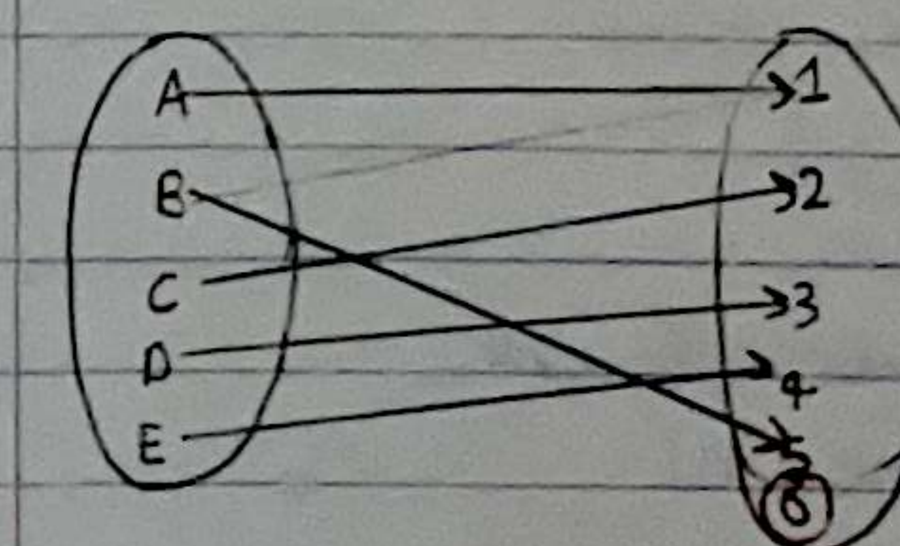
$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} (3)(1\ 2)$

Functions

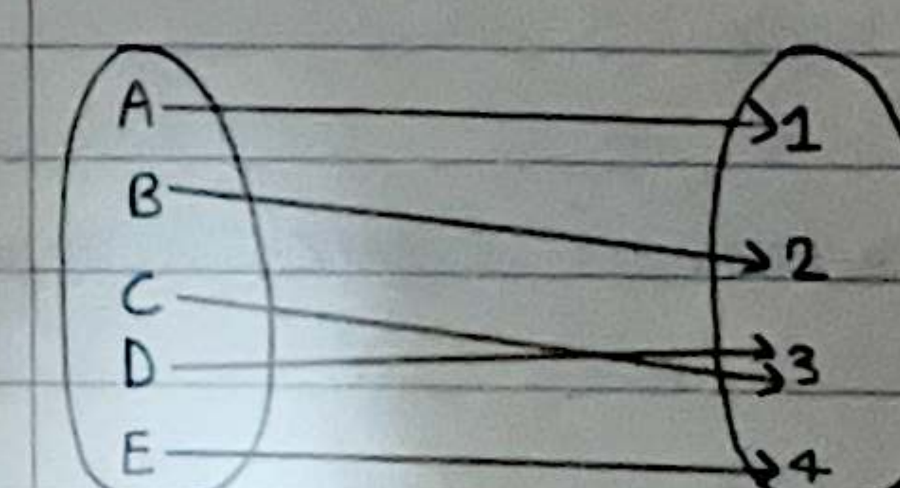
~~NOTE~~



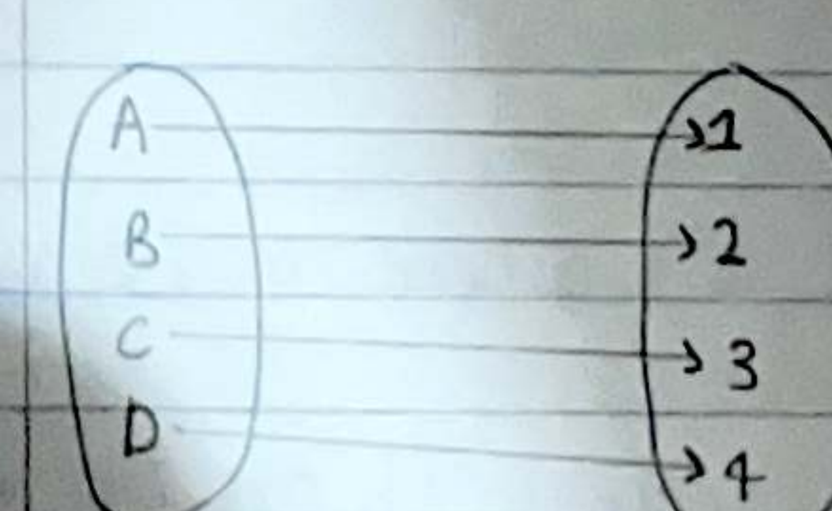
NOT A FUNCTION (one to many) as elements of domain maps to different ranges.



Injective (one-to-one correspondance) Only one domain is mapped to one a range.
ie. No 2 arrows pointing to an Image.
(NOT Surjective as an image has no corresponding domain.)



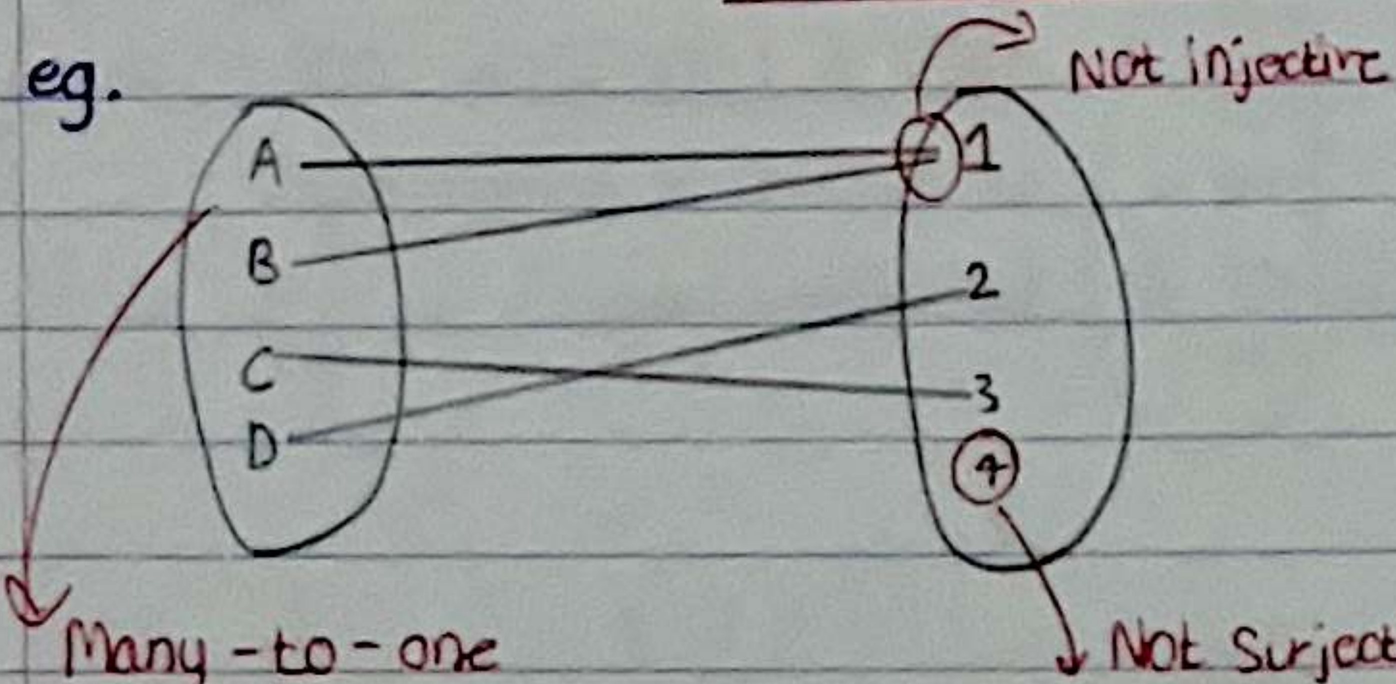
Surjective as all image has a corresponding domain.
Not injective as an image corresponds to 2 elements in the domain.
(No one is alone)



Bijective : Both injective and Surjective.

Note a function can be neither injective nor surjective

eg.



Many-to-one is a function.

Note: A permutation on a set is a bijection onto itself.

No of bijections = No of permutations = $n!$

~~Inverse Completion of the Naturals ($\mathbb{N}$)~~

Algebraic Structures - Ordered tuple

Not an algebraic structure

Set - S - Unordered collection of distinct, immutable objects

as operation is not defined onto members

Magma/Groupoid - $(S, \circ)$ where set S is closed under $\circ$

Semigroup - a magma $(S, \circ)$ where $\circ$ is associative

~~Group~~ Monoid - a Semi group with an id element

Group - A monoid with each element having an inverse.

Ringoid - It is a triple $(S, *, \circ)$
Where S is a set
$*$ and $\circ$ are binary operators on S
the operation $\circ$ distributes over $*$

ie. $\forall a,b,c \in S \quad a \circ (b * c) = (a \circ b) * (a \circ c)$

$\forall a,b,c \in S \quad (a * b) \circ c = (a \circ c) * (b \circ c)$

Note $\circ$ does not have to be associative

A Semiring is a ringoid $(S, *, \circ)$ in which
1) $(S, *)$ forms a semi-group
2) $(S, \circ)$ forms a semi-group

A ring is a Semi-ring in which $(R, *)$ forms an abelian group.
$(R, *, \circ)$

Closure
Associativity
Identity
Invertibility
Commutativity.

~~Ring theory~~

~~A ring is a Set R with 2 operations~~

~~$(R, +, \times)$~~

Permutation Groups

- The set of all permutations of set $\{1,2,3\}$ with the operation of composition forms a group called the permutation group on $\{1,2,3\}$

Axioms

1) Closure

$\forall_{f,g \in S} \mid f \circ g \in S$ where S is the permutation set.

2) Identity

The identity element is $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ or $(1)\ (2)\ (3)$

Note $(S, \circ)$

operation is composition : $f \circ g$ read as f compose g

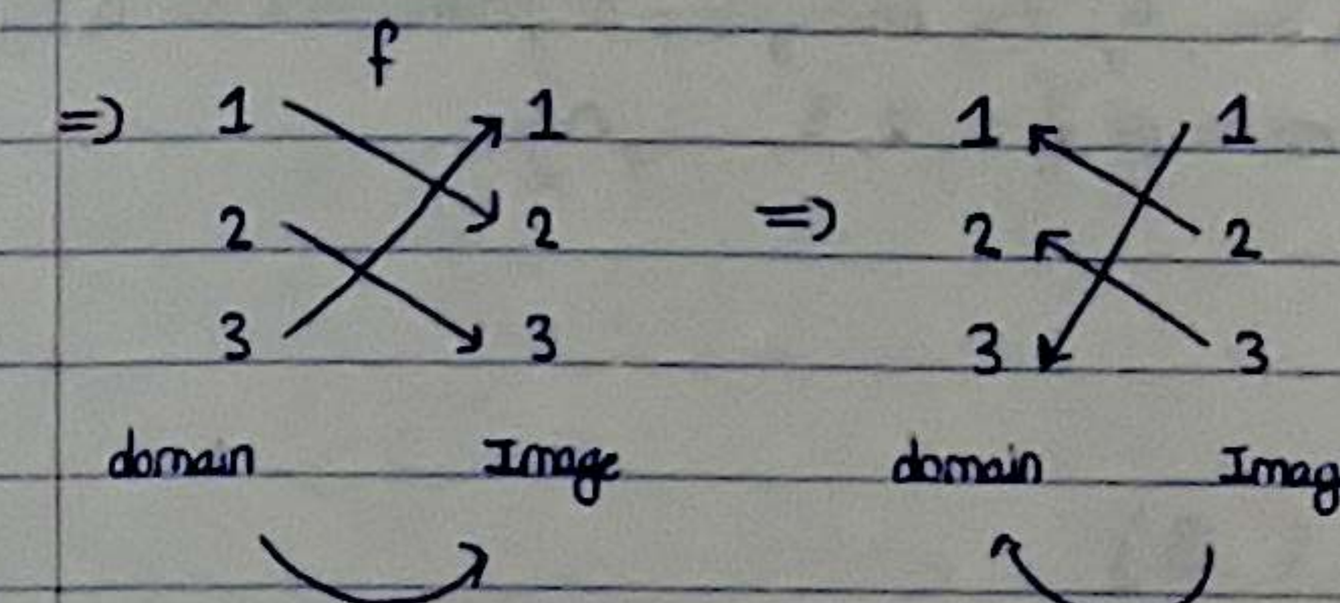
or generally as f operate g

3) Invertibility

Is the inverse element always commutative under composition.

$\forall_{f \in S} \mid \exists_{g \in S} \mid g \circ f = f \circ g = e$ where $g = f^{-1}$

If $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3)$



$\Rightarrow f^{-1} : 1 \mapsto 3$

$2 \mapsto 1$

$3 \mapsto 2$

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

$\Rightarrow (1\ 3\ 2)$

$= (3\ 2\ 1)$

$\Rightarrow f^{-1} = [(1\ 2\ 3)]^{-1} = (3\ 2\ 1)$

Theorem : All (Almost) permutations can be written as a ~~Series~~ Product of transpositions $(i\ \ i+1)$

$(1\ 2\ 3)$

write cycle notation backwards to get the inverse ie $(3\ 2\ 1)$

→ put 1 in front for convention $(1\ 3\ 2)$

~~For permutation~~

Every permutation on n symbols can be written as the product of atmost $\frac{1}{2}n(n-1)$ transpositions.

If a permutation π can be written as the product of odd no of transposition $\Rightarrow$ it is called odd permutation. For even it is called even. $\Rightarrow$ We can define a sign of permutation

$\Rightarrow Sgn(\pi) \begin{cases} +1 & \text{if } \pi \text{ is even} \\ -1 & \text{if } \pi \text{ is odd} \end{cases}$

4) Associativity

↳ Permutation is associative for the same reason as Symmetries

$\forall f,g,h \in S \mid (f \circ g) \circ h = f \circ (g \circ h)$

We use the notation $(S_n, \circ)$ for the group of permutation on n symbols.
S_n is the set of permutation of $\{1,2,3,\dots,n\}$

Find the inverse of $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

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

$\Rightarrow f^{-1} = [(1\ 2)]^{-1} = (2\ 1)$

$= (1\ 2) \longleftarrow$ Inverse of transposition is itself.

(Involution)

$f = f^{-1}$

$\Rightarrow f(f(x)) = x$

(Involution)

Also, $(1\ 2) = (2\ 1)$

Compute the inverses for:

4e

1(a) $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2)$

$f^{-1} = (2\ 3\ 1)$

$= (1\ 2\ 3)$

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

(b) $g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3)$

$g^{-1} = (2\ 3)$

(c) $h = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3)$

$h^{-1} = (1\ 3)$

Check the associativity for:

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

$$= \underset{f}{(1\,3\,2)} \circ \underset{g}{(1\,2)} \circ \underset{h}{(1\,3)}$$

$$(f \circ g) \circ h = f \circ (g \circ h)$$

$(g \circ h) = (1\ 2) \circ (1\ 3)$

$= (1\ 3\ 2)$

$(f \circ g) = (1)(3\ 2)$

$(3\ 2) \circ (1\ 3)$

$= (\cancel{1\ 2})$

$= \underset{f \circ g}{(1)(3\ 2)} \circ \underset{h}{(2)(1\ 3)}$

$f \circ (1\ 3\ 2) = (1\ 3\ 2) \circ (1\ 3\ 2)$

$= (1\ 2\ 3)$

$\Rightarrow$ Associative.

$\cancel{(1\ 2)}($

$(1\ 2\ 3) \leftarrow$

1. write 1
2. 1 is sent to 3 (h) & 3 is sent to 2 ($f \circ g$) — $(n)^*$ sent to n
3. write 2 — $(n)^*$ write n
4. $(n)^*$ 2 is sent to 2 (h) and 2 is sent to 3 ($f \circ g$) — n is sent...
5. write 3
6. 3 is sent to 1 (h) and 1 is sent to 1 ($f \circ g$)
7. write 1/complete cycle

No need to be in numerical order just permutation order

3 Is $(S_3, \circ)$ a Commutative group?

ie. $\forall f, g \in S_3 \quad f \circ g = g \circ f$ True? where $f \wedge g \neq \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

Proof by Counter-example.

Let $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

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

$f \circ g = (3\ 2)$ $\quad g \circ f = (1\ 2) \circ (1\ 3\ 2)$

$= (1\ 3)(2)$

$= (1\ 3)$

Since $f \circ g \neq g \circ f$

$\Rightarrow (S_3, \circ)$ is non-Abelian.