Commutativity

- Isomorphism also preserves Commutativity
  ↳ Both Cayley Tables must be symmetric w.r.t the main diagonal.

General Proof.

Suppose $G \cong G'$ $\qquad (g,h) \in G \quad (g', h') \in G'$

$g \leftrightarrow g'$ and $h \leftrightarrow h'$

then

$gh \leftrightarrow g'h'$ and $hg \leftrightarrow h'g'$

Since G is commutative

$\Rightarrow gh = hg$

$\Rightarrow g'h' = h'g'$ ← This is valid $\forall (g,h) \in G$

$\Rightarrow$ Isomorphism preserves commutativity.

$\Rightarrow$ If G is commu. $\Rightarrow$ G' is also commu. provided the isomorphism exists.

2) Prove that Z_6 is not isomorphic to $S(\Delta)$

- Both have order 6 $\Rightarrow$ Order cannot be used.

We know Z_6 is abelian and $S(\Delta)$ is not

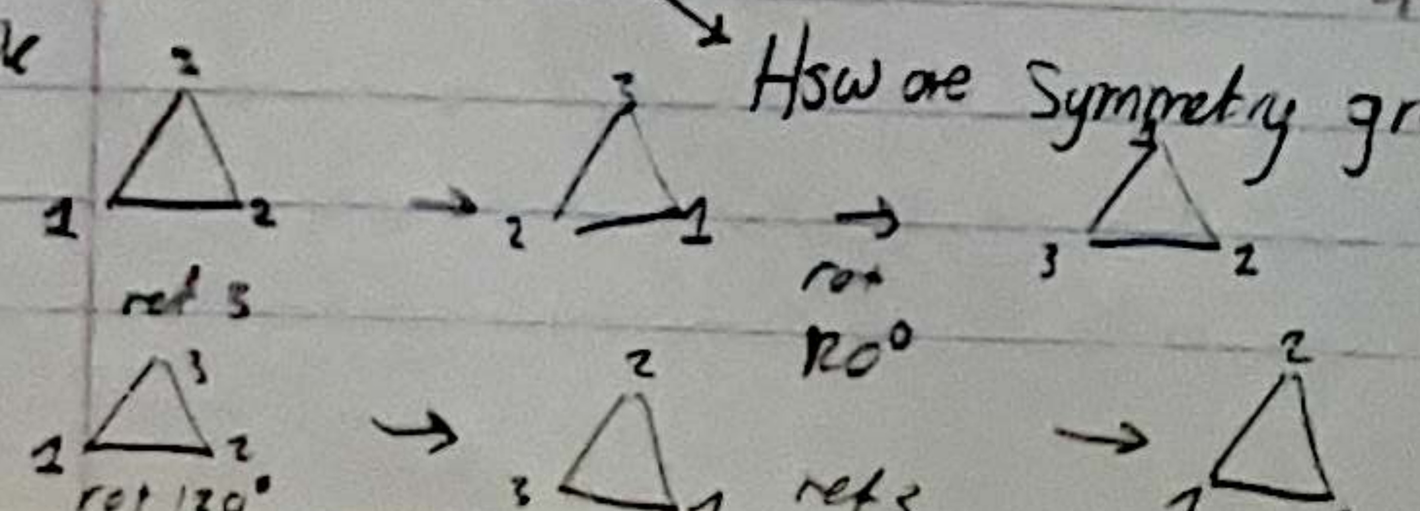
$\Rightarrow Z_6 \not\cong S(\Delta)$

Figure always look the same
- This is a symmetry group.

However orientations of labels are different.

How are Symmetry groups not commutative.

However, If we choose ~~rot.~~ reflect to 3 in the new posn of 3 we get the first one.



Not Commutative

Subgroups

↗ In 3 steps

Prove isomorphism preserves Subgroups.

Suppose $G \cong G'$ and an isomorphism φ ~~exists~~ $\varphi : G \rightarrow G'$ exists.

We know φ sends the identity in G to G'

↳ Proof

Suppose e is the identity in G and a be any element in G

$\varphi(e) = x'$

$\varphi(a) = a'$

We need to show $x' = e'$

$\varphi(ea) = x'a'$

But $ea = a$

$\varphi(a) = x'a'$

$\Rightarrow a' = x'a'$

$a' = e'a'$ where e' is the id in G'

$\Rightarrow e'a' = x'a'$

$\Rightarrow e' = x'$

i.e. $b = a'^{-1}$

Now, We need to show isomorphism map inverses.

Suppose $a \xrightarrow{\varphi} a'$

and $a^{-1} \xrightarrow{\varphi} b$

$aa^{-1} = e$

$\Rightarrow aa^{-1} \xrightarrow{\varphi} a'b$

We know $aa^{-1} = e$

$\Rightarrow e \xrightarrow{\varphi} a'^{-1} b$

But we know from ① that Isomorphism map identities

$\Rightarrow a'^{-1} b = e'$

Composing a'^{-1} on LHS

$\underbrace{a'^{-1}a'}_{e'} b = a'^{-1} e'$

$\Rightarrow b = a'^{-1}$

Now, a subgroup is defined as one which contains the identity element and all the elements present inside have an inverse.

$\Rightarrow$ We have just shown isomorphism preserve subgroups.

$\boxed{\text{Under isomorphism, subgroups of } G \text{ correspond to subgroups of } G'.}$

We did not have to prove closure and associativity as these are the properties of groups and not the mapping (isomorphism).

$\therefore$ If G has a certain no. of subgroups of ~~a~~ particular sizes, G' must also have the same no. of corresponding subgroups (of same sizes).

3) Prove that $\mathbb{Z}_4$ is not isomorphic to $S(R)$ $\longrightarrow$ Correspond to

- order is same
- Both are commutative. (from previous exersises) (Abelian)

We therefore try to inspect subgroups.

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

How to identify Subgroups??

$\circ$	e	x	y	s
e	e	x	y	s
x	x	e	s	y
y	y	s	e	x
s	s	y	x	e

no. of elements in subgroup must be less than in Grp.

$\Rightarrow$ Note: All subgroups must contain the group identity!!

$(\{0,2\}, +_4) \subseteq \mathbb{Z}_4$

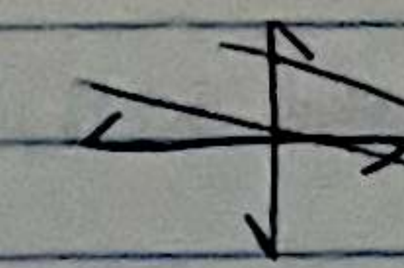
1 S.G of order 2

$(\{e,x\},\circ), (\{e,y\},\circ), (\{e,s\},\circ) \subseteq S(R)$

3 S.G of order 2.

No. subgroups is different and hence are not isomorphic.

14j) 1) $|S(\square)| = 8$



$|\mathbb{Z}_6| = 6$

$|\mathbb{Z}_9| = 9$

$|S(DOGLEG)| = \cancel{4} \longrightarrow$ e and s $\Rightarrow |S(DOGLEG)| = 2$

$|\mathbb{Z}_7| = 7$

$|S(R)| = 4$

~~{S(DOGLEG)} & S(R) have same order & both are abelian.~~

No group have same order and hence none are isomorphic.

Note: Investigate isomorphism between S(WINDMILL), S(R) & S(Plane)

2) Prove $\mathbb{Z}$ is not isomorphic to $\mathbb{Z}_{10}$

$|\mathbb{Z}| = \infty$

$|\mathbb{Z}_{10}| = 10$

$\Rightarrow$ Not isomorphic ??

3) Prove that $S(\square)$ is not isomorphic to either of $\mathbb{Z}$ or $\mathbb{Z}_8$

$|S(\square)| = 8$
$|\mathbb{Z}| = \infty$ } Not isomorphic (diff. orders)

$|\mathbb{Z}_8| = 8$

We know that Dihedral Group is non-Abelian

~~$|\mathbb{Z}_8|$ i~~ $\mathbb{Z}_8$ is ablian

$\Rightarrow S(\square) \ncong \mathbb{Z}_8$

~~Usefl Theromes~~

Useful Theorems

strict

① All groups with less than 6 elements are ~~ablian~~ abelian

② The Dihedral Group is Non - Abelian.

③ Non - Abelian group has order greater than 4.

4) Count the number of subgroups of order 2 in (a) $S(\triangle)$ (b) $\mathbb{Z}_6$ and hence find an alternative proof that these groups are not isomorphic.

(a) $S(\triangle)$

Borrowing from first exercise.

$S(\triangle)$ is non-Abelian while $\mathbb{Z}_6$ is. $\Rightarrow S(\triangle) \ncong \mathbb{Z}_6$

$\underbrace{(\{e,a\},\circ), (\{e,b\},\circ), (\{e,c\},\circ)}_{\text{Order 2}}, (\{e,r,s\},\circ) \subseteq S(\triangle)$

$3! \to 2^3$

(b) $\mathbb{Z}_6$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$(\{0,3\}, +_6)$

$(\{0,1,5\}, +_6)$ ← ??

$(\{0,2,4\}, +_6)$

$1 +_6 1 = 2 \notin \{0,1,5\}$

$\therefore$ No closure

$\Rightarrow$ Not a subgroup.

Why is this not a subgroup of $\mathbb{Z}_6$

General Subgroups of $\mathbb{Z}_n$

$(\{0, \frac{n}{2}\}, +_n)$

for higher order

$(\{0, m, (n-m)\}, +_n)$ for $m < n$ ← More general

??

0, 2, 4, 5

~~0, 2, 3, 5~~

0, 2, 4, 5

$i^3 = -1 \times i = -i^2$

$\boxed{i^2 = j^2 = k^2 = ijk = -1}$

5) The group Q of 'unit quaternions' is a group of order 8 with the following table:

	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	j	-j
-i	-i	i	1	-1	-k	k	-j	j
j	j	-j	k	-k	-1	1	i	-i
-j	-j	-1	-i	i	j	-j	-k	k
k	k	-k	-j	j	i	-i	1	-1
-k	-k	k	-j	j	-i	i	1	-1

Prove that Q is not isomorphic to either (a) $\mathbb{Z}_8$ (b) $S(\square)$

Non!! - Cannot use order.

→ Q is Abelian ⇒ $Q \not\cong S(\square)$

However $\mathbb{Z}_8$ is also abelian

⇒ $Q \not\cong \mathbb{Z}_8$

⇒ Must use subgroups

$\cancel{1}, 2, 4, \cancel{8}$

Subgroups of order 2

Quaternions correspond to ~~rotation~~ symmetry of sphere

$S(\square)$ correspond to symmetry of sphere.

$\mathbb{Z}_8 \to (\{0,4\}, +_8), (\{0,2,4,6\}, +_8)$

How many sub-groups of order 2 does $\mathbb{Z}_8$ have?

$Q \to (\{1,-1\}, \circ)$

~~$(\{-1, i\}, \circ)$~~

⇒ We must use Subgroups to check for Q & $S(\square)$

$8 \to \cancel{1}, \underline{2, 4}, \cancel{8}$

$S(\square)$

↳ $(\{e,a\}, \circ), (\{e,b\}, \circ), (\{e,c\}, \circ), (\{e,d\}, \circ)$

$(\{e,r,s,t\}, \circ), (\{e,s\}, \circ) \leq S(\square)$

~~i, j, k, -1~~

1 subgroup order 4

Subgroups of ~~$S(\square)$~~ Q

$(\{1,-1\}, \circ)$ ← Order 2.

1 = id

~~$(\{1, i, -i\}, \circ)$~~

$\left.\begin{array}{l} (\{1,-1,i,-i\}, \circ) \\ (\{1,-1,j,-j\}, \circ) \\ (\{1,-1,k,-k\}, \circ) \end{array}\right\}$ 3 Subgroups order 4

⇒ No isomorphism

∘ corresponds to multiplication.

The Order of an element.

- Suppose we have an element a of $(G, \circ)$ and suppose we list the powers of a &

ie. $a^0 = e$, $a^1 = a$, a^2, a^3, ...

where $a^2 = a \circ a$

$a^3 = a \circ a \circ a$

$\vdots$

then either all these elements of G are different elements (in which case G must be an infinite group) and we say a has infinite order

or at least two of these powers must be the same (if G is finite this must happen) and we say a has finite order.

Suppose a does have finite order, then a to a certain power must be the same as a raised to another power.

$\rightarrow$ $a^p = a^q$ where $0 \leq p < q$

Not equal as we define p to be different to q.

$a^p a^{-p} = a^q a^{-p}$

$e = a^{q-p}$

$\boxed{a^n = e}$

~~No of times~~ n takes values of which occurs when a operated with itself n times yield a again.

$\Rightarrow a^{q-p} = a^n$

$n = q - p \quad p > 0$

The smallest number n $(n > 0)$ s.t $a^n = e$ is called the order of a.

0 would yield the identity trivially.

eg. Consider the element r ($120°$ cc/w rotation) in $S(\triangle)$

$r^0 = e \qquad r^1 = r \qquad r^2 = s \qquad r^3 = \overset{sr}{\cancel{rs}} = e$

r^0 : Do not do r $\quad \Rightarrow r$ has order 3

$\cancel{r^0 = r^3} =$

$r^0 = e$

$r^3 = e$

Let $r^n = e$

$n = 3 - 0$

$= 3 \leftarrow$ order

More general

Consider r^1 & r^4 $\longrightarrow$ We can also do for $r^2 = s$ & $r^5 = es$

$5 - 2 = 3 \leftarrow$

$\downarrow \quad \downarrow$

$r \quad r$

$4 - 1 = 3 \leftarrow$ order 3

Since an isomorphism preserves products, it must preserve powers as well:

$a \leftrightarrow a' \qquad a^2 \leftrightarrow (a')^2 \qquad a^3 \leftrightarrow (a')^3$ ...

$\Rightarrow$ it must preserve order of an element as well

An Isomorphism preserves the order of an element.

ex. 1 Find the order of the elements of $S(\square)$. Find the order of the element 1 in $\mathbb{Z}_8$. Deduce from those that these 2 groups are not isomorphic.

$S(\square)$

How many times we must compose an element with itself to first get e.

$e^0 = e \quad e^1 = e \Rightarrow n = 1-0 = 1 \Rightarrow e$ has order 1.

$a^0 = e \quad a^1 = a \quad a^2 = e \quad n = 2-0 = 2 \Rightarrow a$ has order 2

$a \circ a$

reflect twice is same as doing nothing.

Same for b, c, d

$r^0 = e \quad r^1 = r \quad r^2 = s \quad r^3 = sr \quad r^4 = e \Rightarrow r$ has order 4.

90° cc/w rot.

$s^0 = e \quad s^1 = s \quad s^2 = e \Rightarrow s$ has order 2

180° cc/w rot.

$t^0 = e \quad t^1, \quad t^2, \quad t^3, \quad t^4 = e$

$270° \quad 540° \quad 810° \quad 1080°$

$\left(\frac{1080}{360}\right) =$ integer

270° cc/w rot.

$\cong$ 90° c/w rot.

$\Rightarrow t$ has order 4.

$S(\square)$ has: 1 element of order 1,
5 elements of order 2,
2 elements of order 4.

$\mathbb{Z}_8$ or $\mathbb{Z}/8\mathbb{Z}$

Note the group operation in $\mathbb{Z}_8$ is $+_8$

$\Rightarrow (1)^n$ means $1 +_8 1 +_8 1 \ldots$ (n times)

$\Rightarrow (1)^n$ is $(n \times 1) \bmod 8$

We need to solve n for $n \bmod 8 \equiv 0$

where n is the least non-zero value to satisfy the congruence relation

$\Rightarrow n = 8$

$\Rightarrow 1$ has order 8 in $\mathbb{Z}_8$

Since $S(\square)$ has no elements of order 8 $\Rightarrow S(\square) \not\cong \mathbb{Z}_8$

ex. 1 Find the order of all the elements in $S(\triangle)$ and find the order of 1 in $\mathbb{Z}_6$. Deduce from those that the groups are non-isomorphic.

$S(\triangle)$	$\mathbb{Z}_6$
$e^n = e$ — e has order 1	$n \bmod 6 = 0$
$a^n, b^n, c^n = e$ ← a, b, c have order 2	$n = 6$
$r^n = e$ ← r has order 3	$\Rightarrow 1$ has order 6 in $\mathbb{Z}$
s has order 3	
$s^n = e$	

$\Rightarrow S(\triangle) \not\cong \mathbb{Z}_6$

2) Find the orders of all the elements in $S(R)$ and $S(W_4)$ and deduce from those that the groups are non-isomorphic.

$S(R) = (\{e, x, y, s\}, \circ)$	$S(W_4) = (\{e, r, s, t\}, \circ)$
e has order 1	e has order 1
x, y, s have order 2	r has order 4
	s has order 2
	t has order 4

$S(W_4) \not\cong S(R)$ as the latter lacks elements of order 4.

3) Find the order of the following elements (or state if they have infinite order) in the given group:

i) 1 in $\mathbb{Z}$ $\longrightarrow$ Addition becomes product...

$1^n = e = 1$ $1 + 1 + 1$ (n times) same as $(n \times 1)$

$(n \times 1) \bmod 1 = 0$

$n \bmod 1 \equiv 0$

$\forall n \in \mathbb{Z}$ congruence relation is zero

$\Rightarrow$ ~~A has~~ 1 has ~~infinite~~ order infinite in $\mathbb{Z}$.

ii) 3 in $\mathbb{Z}_8$

$3^n = e$

$3n \bmod 8 = 0$ or $3 + 3 + 3 \ldots$ mod 8 How many times yield 0?

$24 \bmod 8 = 0$

$n = 8$

$\Rightarrow$ 3 has order 8 in $\mathbb{Z}_8$

(c) 5 in $\mathbb{Z}_{10}$

5 has order 2 in $\mathbb{Z}_{10}$

$5n \bmod 10 = 0$

$n = 2 \Rightarrow 5n = 10$ least non-zero value.

(d) $\frac{1}{2}$ in ~~$\mathbb{Q}$~~ $\mathbb{Q}$

$\left(\frac{1}{2}\right)^n = e = 0$

$\frac{1}{2} + \frac{1}{2} + \frac{1}{2} \ldots \neq 0$ $\prod_{n=}$

$\Rightarrow \frac{1}{2}$ has infinite order in $\mathbb{Q}$

(e) $\frac{1}{2}$ in $(\mathbb{Q}^*, \times)$

set of rationals excluding 0.

$\frac{1}{2} * \frac{1}{2} * \frac{1}{2} \ldots$ $\longrightarrow$ Study pi notation

~~$\prod$~~ $\left(\frac{1}{2}\right)^n$

Actually denotes exponentiation in this case.

as $\frac{1}{2} \times \frac{1}{2} \times \frac{1}{2}$ n times same as $\left(\frac{1}{2}\right)^n$

~~Ne~~ $n = \infty$ for soln

$\Rightarrow \frac{1}{2}$ has Order infinite order in $\mathbb{Q}$

(f) 1 in $(\mathbb{R}^+, \times)$

1 has order 1 in $\mathbb{R}^+$

(g) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ in S_4

id in S_4 is $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

$\cancel{(1\,2\,3\,4)\circ(1\,2\,3\,4)} = \cancel{(3\,4}$

$\cancel{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (}$

1st order $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

$= (1\,3)\,(2,4)$ ✓

2nd order $\cancel{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}}$

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

$(1\,4\,3\,2)$ ✓

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

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

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

3rd order $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = id$

$\Rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ has order 3.

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

(h) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}$ in S_5

$(1\,3\,2)\boxed{(4)\,(5)}$

$[(4)\,(5)]$

1st order $(1\,3\,2)\circ(1\,3\,2) = (1\,2\,3)\ [(4)\ (5)]$

2nd order $(1\,3\,2)\circ(1\,2\,3) = (1)\,(2)\,(3)\,[(4)\,(5)]$

$\Rightarrow (1\,3\,2)$ has order 2 in S_5

4) Prove that an element $g \neq e$ in a group G has order 2 if and only if e appears on the diagonal in row g of the group table.

Suppose g has order 2

$\therefore g^2 = e \Rightarrow g = g^{-1}$.

The diagonals in a Cayley table correspond to the composition of an element with itself.

g' corresp. to the single operation g.

The entry e in that diagonal can be shown to be unique in both row and column g "more rigorous"

e appears on the diagonal $\Leftrightarrow g^2 = e$

Since $g = g^{-1} \neq e$ (given)

this is equivalent to g having order 2.

Groups defined by equations.

It is often more convinient to specify groups with 'equations'.

eg. Construct a table for the group $G = \{a \mid a^5 = e\}$. To which familliar group is it isomorphic to?

The notation means that the group consists of all powers of a subjected to the restriction $a^5 = e$.

ie. $a^6 = a^5 a = ea = a$ and $a^{-1} = a^5 a^{-1} = a^4$

$\Rightarrow$ the elements are e, a, a^2, a^3, a^4

Other powers can also be calculated

eg. $a^7 = a^5 a^2 = ea^2 = a^2$

$a^2 a^4 = a^6 = aa^5 = ae = a$

Table

$\circ$	e	a	a^2	a^3	a^4
e	e	a	a^2	a^3	a^4
a	a	a^2	a^3	a^4	e
a^2	a^2	a^3	a^4	e	a
a^3	a^3	a^4	e	a	a^2
a^4	a^4	e	a	a^2	a^3

$\Rightarrow \boxed{G \cong \mathbb{Z}_5}$

2) How many distinct elements are there in the group

$$\{a, b \mid a^3 = b^2 = e \quad ab = ba^{-1}\} ?$$

$\rightarrow$ Group consists of all powers of a & b subjected to the given restrictions.

Simplify ① a^2baba^{-1} ② $ba^{-1}ba^{-1}ba^2$

① a^2baba^{-1}

$ab = ba^{-1}$

$= a^2bba^{-1}a^{-1}$

$= a^2b^2a^{-2}$

$b^2 = e$

a^2ea^{-2}

$= a^2a^{-2}$

$= e$

② $ba^{-1}ba^{-1}ba^2$

$ba^{-1} = ab$

$ababba^2$

$abab^2a^2$

$b^2 = e$

$abaea^2$

aba^3

$a^3 = e$

$= abe$

$= ab$

Why??

$ba^{-1}ba^{-1}ba^2$

$a^3 = e \Rightarrow a^2 = a^{-1}$ (from $a^3a^{-1} = ea^{-1}$)

~~$ba^2ba^2ba^2$~~

$\Rightarrow ba^2ba^2ba^2$

move b left across a^2 using $ab = ba^{-1}$

~~ba^2ba~~

ba^2baaba^2

$ba^{-1}ba^{-1}ba^2$

$a^3 = e \Rightarrow a^2 = a^{-1}$

$= ba^2 ba^2 ba^2$

$ab = ba^{-1}$

$= ba^2 baba^{-1}a^2$

$ab = ba^{-1}$

$= ba^2 \underbrace{\cancel{b}^2}_{e} a^{-2} a^2$

$= ba^2 e a^{-2} a^2$

$= ba^2 \leftarrow$

Why is this one correct?

We need to simplify $\underline{ba^{-1}ba^{-1}ba^2}$

We want to remove a^{-1} terms

We know $a^3 = e \Rightarrow a^{-1} = a^2$

$\therefore ba^2ba^2ba^2$

We cannot compose / simplify further as there are no given eqns to satisfy that expression.

Note: We CANNOT move the terms as We do not know if group operation is Commutative.

However we know $ab = ba^{-1}$

We can try to use this to get a term which is validated by the eqns.

↳ $a^3 = e$ & $b^2 = e$ cannot help in this case,

$ba^2ba^2ba^2$

we target this part to try and move b across a^2 to get a b^2 term.

$ba^2 baaba^2$

$= ba^2 baba^{-1}a^2$

again

$= ba^2 bba^{-1}a^{-1}a^2$

$= ba^2 \underbrace{\cancel{b}^2}_{e} a^{-2}a^2$

$= ba^2 \leftarrow$

Why did the first method fail?

Method: $ba^{-1}ba^{-1}ba^2$

Using $ba^{-1} = ab$ (twice)

We get $ababba^2$

$aba\underbrace{b^2}_{e}a^2$

$ab\underbrace{a^3}_{e}$

$= ab$!! X

Why is ab not the simplest form?

ab

$= ba^{-1}$

$a^{-1} = a^2$

(three)

$\cancel{ba^{-1}}$ $\underline{\underline{ababba^2}} = ba^2$

$a^2 = a^{-1}$

$ababba^{-1}$

$ba^{-1} = ab$

$ababab$

$abba^{-1}ab$

$ab^2a^{-1}ab$ X

$\cancel{ba^{-1}ba^{-1}ba^2}$

$\cancel{a^{-1} = a^2}$

$b = b^{-1}$

Use $ab = ba^{-1}$ twice

$ba^{-1}ba^{-1}ba^2$

$abab ba^2$

$abaea^2$

aba^3

$ba^{-1}a^3$

$ba^2 \leftarrow$ ✓✓

We could have used $ba^{-1} = ab$ once.

$ba^{-1}\underline{ab}ba^2$

$= ba^{-1}ab^2a^2$

$= ba^{-1}a^3$

$= ba^2$

Problem comes from $\boxed{a^{-1} = a^2}$

Something wrong in using $ab = ba^{-1}$?? X

$ba^{-1}ba^{-1}ba^2$

Use once

$a\underbrace{bb}_{e}a^{-1}ba^2$

$\underbrace{\cancel{aa^{-1}}}_{e}ba^2$

$\cancel{ababba^2}$

$\cancel{aba^3}$

Study This Group in details

Note: For a general element in the group, the eqn $ab = ba^{-1}$ can be used to move all powers of b to the left and all the elements can be expressed as $b^p a^q$ then the eqn $a^3 = e$ and $b^2 = e$ can be used to reduce p to 1 or 0 (b has order 2) and q to 0, 1, 2 (a has order 3)

Thus the distinct elements are: e
a
a^2
b
$\cancel{b}\ ba$
ba^2

HOW? ← $\left.\begin{matrix} ba \\ ba^2 \end{matrix}\right\}$ → Composition of the previously found elements.

Complete the Cayley Table for this group and verify that it is isomorphic to $S(\Delta)$.

Group: $\{a, b \mid a^3 = b^2 = e,\ ab = ba^{-1}\}$

1

	e	a	a^2	b	ba	ba^2
e	e	a	a^2	b	ba	ba^2
a	a	a^2	e	ba^2	b	b
a^2	a^2	e	a	ba	b	ba
b	b	ba	ba^2	e	a^2	a^2
ba	ba	ba^2	b	a^2	e	a
ba^2	ba^2	b	ba	a	a^2	e

2

Given ba^2

Compare with $ba^{-1} = ab^2$

2 0 1

ba^2b

Inverse of $a^2 = a$

$\Rightarrow ba^2 = ab$ ←

bab $baab$

$bba^{-1}baba^{-1}$

e bba^{-2}

Now | $ab \circ ba = abba = a^2$ bba $ba^2 \circ ba$

ba^2ba

$b^2a^{-1}a^{-1}$. $ba = a^2b$ $baaba$

$baba$ $baba^2$ a ba^2a^2b $b^2a^{-2}a$ ba^2ba^2

$b^2a^{-1}a$ $bba^{-1}a^2$ bab ba^{-1}

e $\cancel{b}ba^{-1}$

$baba$

$b^2a^{-1}a$

bab

b^2a^{-1} a^2 abb

$a^{-1} = a^2$ ←

verify order of operations from back

2) Write down the distinct elements of $\{a, b \mid a^2 = b^2 = e,\ ab = ba\}$

$e, a, b, ab\ (=ba)$ a : 0, 1
b : 0, 1

Construct the group table.

3 Write down the distinct elements of $\{a, b \mid a^3 = b^2 = e,\ ab = ba\}$

$e, a, a^2, b, ab(=ba), a^2b\ (=ba^2)$

Construct a group table and show that the group is isomorphic to Z_6.

Denotes Commutativity.

4) Write down the distinct elements of $\{a, b \mid a^4 = b^2 = e,\ ab = ba\}$

$e, a, a^2, a^3, b, ab, a^2b, a^3b$

$ab = ba$, $a^2b = ba^2$, $a^3b = ba^3$

$a^2b = ba^2$

$\underbrace{a \circ (a \circ b)}$ $\quad$ $b \circ \underbrace{(a \circ a)}$

Treat as Symbols.

Construct a group table and prove that the group is not isomorphic to any of

(a) $\mathbb{Z}_8$ (b) $S(\square)$ (c) Q

Direct Product

Suppose we have two groups $(G, \circ)$ and $(H, *)$ then we can construct a new group which is called the direct product of G and H and is written as $G \times H$. The elements of $G \times H$ are pairs (g, h) where $g \in G$ and $h \in H$.

This set is the Cartesian Product.

The group operation is defined as follows:

$$(g, h)(g', h') = (g \circ g', h * h')$$

Consider the groups $(G, \circ)$ and $(H, *)$ where G and H are the sets underlying the respective groups

Also $g, g' \in G$ and $h, h' \in H$

We define the Cartesian Product of the sets of the 2 groups as follows

$$G \times H = \{\underbrace{(g, h)}_{\text{Ordered Pair}} \mid g \in G,\ h \in H\}$$

Note: $H \times G = \{(h, g) \mid \dots\}$

We now define the direct product group operation on the set $G \times H$ of (ordered) 2-tuples as follows

$$\forall (g, h) \in G \times H \quad (g, h) \otimes (g', h') = (g \circ g', h * h') (\in G \times H)$$

Direct Product Operator

Place holder - Symbol

Group operations in their respective groups

Note: When working with sets, the Cartesian product is the direct product. They hence share the same symbol X.

& we usually omit the direct product symbol.

We should now show that the direct product forms a group ie. $(G \times H, \oplus)$ is a group

For $G \times H$ to be a group it needs to obey the group Axioms

1) Closure $\quad (G, \circ) \quad (H, *)$

Suppose $g, g' \in G$ and $h, h' \in H$

$G \times H = \{(g,h) \mid g \in G, h \in H\}$

$(g,h) \otimes (g',h') = (g \circ g', h \circ h')$

$(g \circ g') \in G \quad (h \circ h') \in H$

$\Rightarrow (g \circ g', h \circ h')$ can be expressed as (g,h)
$\Rightarrow$ There is closure under direct product of groups.

2) Existence of an identity element in $G \times H$

$id = (e_G, e_H) \quad e_G$ is id in G.
e_H is id in H.

$\forall (g,h) \in G \times H$

$$\left.\begin{aligned} (g,h) \otimes (e_G, e_H) &= (g \circ e_G, h * e_H) = (g,h) \\ (e_G, e_H) \otimes (g,h) &= (e_G \circ g, e_H * h) = (g,h) \end{aligned}\right\}$$

3) Invertibility

The inverse of (g,h) is (g^{-1}, h^{-1})

$\exists x \in G \times H \mid x(g,h) = (g,h)x = (e_G, e_H)$

$(g^{-1}, h^{-1}) \otimes (g,h) = (g^{-1} \circ g, h^{-1} * h) = (e_G, e_H)$

$(g,h) \otimes (g^{-1}, h^{-1}) = (g \circ g^{-1}, h * h^{-1}) = (e_G, e_H)$

4) Associativity

$$[(g,h) \otimes (g',h')] \otimes (g'',h'') \stackrel{?}{=} (g,h) \otimes [(g',h') \otimes (g'',h'')] \quad -①$$

$(g \circ g', h \circ h') \otimes (g'', h'') \qquad (g,h) \otimes (g' \circ g'', h' * h'')$

$(g \circ g' \circ g'', h * h' * h'') \qquad (g \circ g' \circ g'', h * h' * h'') \quad -②$

Since ② = ①
$\Rightarrow$ Direct product is Associative.

We know $\circ$ and $*$ are associative operations since G & H are Groups else (we need to show) NOT really $g \circ (g' \circ g'') = (g \circ g') \circ g''$ which is shown trivially in this case.

Since all 4 Group axioms are Satisfied $\Rightarrow G \times H$ forms a group (under direct product) operation.

ex 1) Write down the group table for $\mathbb{Z}_2 \times \mathbb{Z}_2$. To which familliar group is it isomorphic to?

Incorrect notation??

$$\mathbb{Z}_2 = (\{0,1\}, +_2)$$

$\cancel{\mathbb{Z}_2 =}$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = (\{(0,0),(0,1),(1,0),(1,1)\}, \otimes)$$

$\otimes$	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,0)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

$(1 +_2 0, 1 +_2 1)$

$$\boxed{\mathbb{Z}_2 \times \mathbb{Z}_2 \cong S(R)}$$

Symmetric Group of the Rectangle

2) Describe how to combine elements in $\mathbb{R} \times \mathbb{R}$. ~~Interpre~~ This group has a very familliar interpretation. What is it?

Note: the operation in $\mathbb{R}$ is addition.

$$\mathbb{R} \times \mathbb{R} = \{(r,s) \mid r,s \in \mathbb{R}\}$$

$$(r,s) \otimes (r',s') = (r+r', s+s')$$

$\mathbb{R} \times \mathbb{R}$ is the group of 2-dimensional vectors under addition.

Usually denoted as:

$(r_1,s_1) + (r_2,s_2)$

inverse is $(-r_1,-s_1) \rightarrow -(r,s)$

Identity is $(0,0)$

14m) Construct a group table for $\mathbb{Z}_4 \times \mathbb{Z}_2$ and verify that the group is isomorphic to the group constructed in 14l Q4.

$\mathbb{Z}_4 = (\{0,1,2,3\}, +_4)$ $\quad \mathbb{Z}_2 = (\{0,1\}, +_2)$

$$\mathbb{Z}_4 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1),(2,0),(2,1),(3,0),(3,1)\}$$

$$(a,b) \otimes (a',b') = (a +_4 a', b +_2 b')$$

$(+_4, +_2)$	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)	(3,0)	(3,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)	(3,0)	(3,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)	(2,1)	(2,0)	(3,1)	(3,0)
(1,0)	(1,0)	(1,1)	(2,0)	(2,1)	(3,0)	(3,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(2,1)	(2,0)	(3,1)	(3,0)	(0,1)	(0,0)
(2,0)	(2,0)	(2,1)	(3,0)	(3,1)	(0,0)	(0,1)	(1,0)	(1,1)
(2,1)	(2,1)	(2,0)	(3,1)	(3,0)	(0,1)	(0,0)	(1,1)	(1,0)
(3,0)	(3,0)	(3,1)	(0,0)	(0,1)	(1,0)	(1,0)	(2,0)	(2,1)
(3,1)	(3,1)	(3,0)	(0,1)	(0,0)	(1,1)	(1,1)	(2,1)	(2,0)

~~Proff~~ ~~Proff~~ Proof of isomorphism

$a^2b \circ a^2$

$a^2 \circ a^2b$

ab

2) Construct a group table for $\mathbb{Z}_3 \times \mathbb{Z}_2$ and by observing that this group is essentially the same as the group of ex. 14.1 Q3, show that $\mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$.

$\mathbb{Z}_3 = (\{0,1,2\}, +_3)$ $\mathbb{Z}_2 = (\{0,1\}, +_2)$

$\mathbb{Z}_3 \times \mathbb{Z}_2 = (\{(0,0),(0,1),(1,0),(1,1),(2,0),(2,1)\}, (+_3, +_2))$

$(+_3, +_2)$	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)	(2,1)	(2,0)
(1,0)	(1,0)	(1,1)	(2,0)	(2,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(2,1)	(2,0)	(0,1)	(0,0)
(2,0)	(2,0)	(2,1)	(0,0)	(0,1)	(1,0)	(1,1)
(2,1)	(2,1)	(2,0)	(0,1)	(0,0)	(1,1)	(1,0)

$\exists f : \mathbb{Z}_3 \times \mathbb{Z}_2 \to G$ where $G = (\{a, b \mid a^3 = b^2 = e, ab = ba\}, \circ)$ and f is one-to-one and onto.

f: $e \to (0,0)$

$a \to (1,0)$

$a^2 \to (2,0)$

$b \to (0,1)$

$ab \to (1,1)$

$a^2b \to (2,1)$

G

row ∘ Column

$\circ$	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	ab	a^2b	e	a	a^2
ab	ab	a^2b	b	a	a^2	e
a^2b	a^2b	a	a^2b	b	ab	a

We now define g : $G \to \mathbb{Z}_6$ where g is one-to-one and onto.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$g: e \to 0$
$a \to 4$
$a^2 \to 2$
$b \to 3$
$ab \to 1$
$a^2b \to 5$

$$\begin{tikzcd} \mathbb{Z}_3 \times \mathbb{Z}_2 \arrow[r, "f"] \arrow[dr, "h"'] & G \arrow[d, "g"] \\ & \mathbb{Z}_6 \end{tikzcd}$$

$h : \mathbb{Z}_3 \times \mathbb{Z}_2 \to \mathbb{Z}_6$
Diagram ~~is commutative~~ Commutes
$\Rightarrow \mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$

3) Construct a table for $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (the set of ordered triples of elements of $\mathbb{Z}_2$) with operation defined in the same way as for $G \times H$ and prove that this group of order 8 is not isomorphic to any of the groups (a) $\mathbb{Z}_8$ (b) $\mathbb{Z}_4 \times \mathbb{Z}_2$ (c) $S(\square)$ (d) Q

0 1
0 1
0 1

$\mathbb{Z}_2 = (\{0,1\}, +_2)$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = (\{(0,0,0), (1,0,0), (0,1,0), (0,0,1), (0,1,1), (1,1,0), (1,0,1), (1,1,1)\}, (+_2, +_2, +_2))$

$(+_2,+_2,+_2)$	(0,0,0)	(0,1,0)	(0,0,1)	(0,1,1)	(1,0,0)	(1,0,1)	(1,1,0)	(1,1,1)
(0,0,0)	(0,0,0)	(0,1,0)	(0,0,1)	(0,1,1)	(1,0,0)	(1,0,1)	(1,1,0)	(1,1,1)
(0,1,0)	(0,1,0)	(0,0,0)	(0,1,1)	(0,0,1)	(1,1,0)	(1,1,1)	(1,0,0)	(1,0,1)
(0,0,1)	(0,0,1)	(0,1,1)	(0,0,0)	(0,1,0)	(1,0,1)	(1,0,0)	(1,1,1)	(1,1,0)
(0,1,1)	(0,1,1)	(0,0,1)	(0,1,0)	(0,0,0)	(1,1,1)	(1,1,0)	(1,0,1)	(1,0,0)
(1,0,0)	(1,0,0)	(1,1,0)	(1,0,1)	(1,1,1)	(0,0,0)	(0,0,1)	(0,1,0)	(0,1,1)
(1,0,1)	(1,0,1)	(1,1,1)	(1,0,0)	(1,1,0)	(0,0,1)	(0,0,0)	(0,1,1)	(0,1,0)
(1,1,0)	(1,1,0)	(1,0,0)	(1,1,1)	(1,0,1)	(0,1,0)	(0,1,1)	(0,0,0)	(0,0,1)
(1,1,1)	(1,1,1)	(1,0,1)	(1,1,0)	(1,0,0)	(0,1,1)	(0,1,0)	(0,0,1)	(0,0,0)

→ Order of groups cannot be used to disprove isomorphism.
Group is Commutative
All elements except the identity have order 2. → Not isomorphic to $S(\square)$ — 90° c/w rot. has order 4
Not isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$ — (1,0) order 4
Not isomorphic to $\mathbb{Z}_8$ → 1 has order 8
order of element
Not isomorphic to Q
↳ i has order 4

Subgroups?

4) Prove that every element other than the identity in $\mathbb{Z}_3 \times \mathbb{Z}_3$ has order 3.
Deduce that $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not isomorphic to $\mathbb{Z}_9$

$\mathbb{Z}_3 = (\{0,1,2\}, +_3)$

$\mathbb{Z}_3 \times \mathbb{Z}_3 = (\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}, (+_3,+_3))$

$\mathbb{Z}_3 \times \mathbb{Z}_3 = \{(n,m) \mid n,m \in \{0,1,2\}\}$

~~Order~~ $|(n,m)| = \operatorname{lcm}(|n|,|m|)$

$\forall n,m \in \mathbb{Z}_3 \times \mathbb{Z}_3$ and $(n,m) \neq 0$

$|0| = 1 \qquad 0^1 = 0$

$|1| = 3 \qquad 1^3 = 0$

$|2| = 3 \qquad 2^3 = 0$

lcm of the combinations (except $(0,0)$) $= 3$

$\Rightarrow$ All the elements of $\mathbb{Z}_3 \times \mathbb{Z}_3$ (except id) have order 3.

Arithmetic multiplication.

5) If G and H are finite groups then $G \times H$ is also finite. $\rightarrow |G| \times |H|$

Proof ??

$G \times H \neq H \times G$

6) Prove that if G and H are commutative then $G \times H$ is also commutative.

Shorter & More precise

Let $g, g' \in (G, \circ)$ and $h, h' \in (H, *)$

From Commutativity we have

$g \circ g' = g' \circ g$ in G and $h * h' = h' * h$ in H — ①

$G \times H = (\{(g,h) \mid g \in G, h \in H\}, \otimes)$

$(g,h) \otimes (g',h') = (g \circ g', h \circ h')$

Composition operation in set of Cartesian product.

But from ①

$g \circ g' = g' \circ g \qquad h * h' = h' * h$

$\Rightarrow (g \circ g', h * h') \Longleftrightarrow (g' \circ g, h' * h) = (g', h') \otimes (g, h)$

Hence Commutativity.

Two theorems of group theory.

-Cayley's Theorem

> Any finite group is isomorphic to a Subgroup of a permutation group.

* This is very powerful. Once permutation groups are understood, all finite groups are understood up to isomorphism.

Proof of Cayley's Theorem.

- The proof relies on the observation that ~~the~~ any row of the group table for a group contains each element of the group exactly once.

This implies that we can associate to any element $g \in G$ a permutation: namely the permutation of the elements of G whose permutation symbol has the g-row of the table as its bottom line.

eg. Consider the group $(\{e,a,b\}, \circ)$ with table.

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

the a-row is $\boxed{a \mid b \mid e}$ which gives the permutation $\begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix}$

b-row gives $\begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix}$ e-row gives $\begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix}$

* It can be seen that an element of the set underlying the group induces a permutation on that set (the set underlying the group containing the element) based on the group composition laws.

Cause permutation onto the elements of the underlying set.

Trivially, we could say that the group 'acts' on the set underlying it

While studying Group Actions, we make a group act on another set ??

function.

Homomorphisms from the elements underlying the group to the other set ??

If we use the previous correspondences, the following table can be set up.

$\circ$	$\begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix}$	$\begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix}$	$\begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix}$
$\begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix}$	$\begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix}$	$\begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix}$	$\begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix}$
$\begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix}$	$\begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix}$	$\begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix}$	$\begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix}$
$\begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix}$	$\begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix}$	$\begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix}$	$\begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix}$

$G \cong P$ where $P \subseteq S_n$

It can be seen that

① a group is formed

② an element in a row permutes the group ie. eg a acting on the set sends e to a, a to b and b to e

③ in the 2nd table the elements of G are written in the form of the permutations that they repeat

ie. in row a $\sigma_a(b) = e$

Where $\sigma_a = \begin{cases} e \to a \\ a \to b \\ b \to e \end{cases}$

function of permutation induced by a

Since σ_a is one-to-one and onto, it is bijective (Inverse and no element left unpaired)

A row contains all elements

It satisfies the defn of permutation as a bijective homomorphism from the underlying set to itself.

In a general group, g determines the permutation $x \mapsto gx$ since gx is the entry in the g-row below x.

	e		x
e	e	...	x
	↓	---	↓
g	g	...	gx

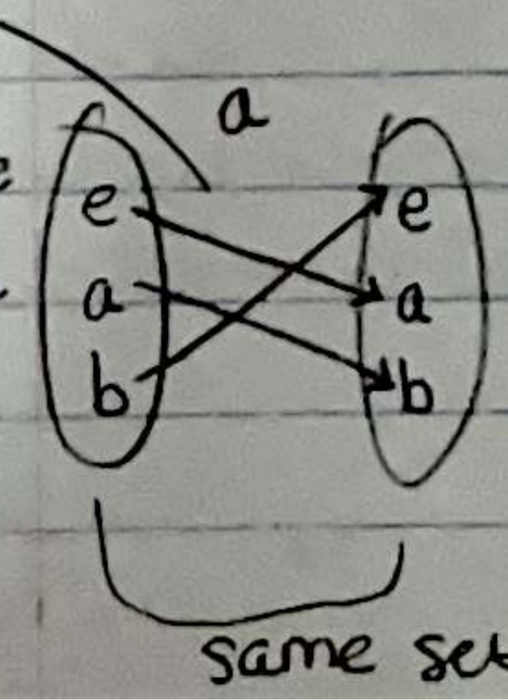
Let the notation $\hat{g}$ represent this permutation then $\hat{g}(x) = gx$
Notice : Different elements of G give rise to different permutations
Since $\hat{g} : e \mapsto g$ and $\hat{h} : e \mapsto h$: So the set of All permutations arising in this way is in one-to-one correspondence with G.
Notice also that $(\hat{h} \circ \hat{g})$ maps x to hgx Since $x \overset{\hat{g}}{\mapsto} gx \overset{\hat{h}}{\mapsto} hgx$ ie. the composition of the permutations correspond to the product of the correspondg elements of G. Thus the permutations form a group isomorphic to G and we have found the required subgroup of a permutation group isomorphic to G.

Permutation

(no morphisms on sets)
↳ morphisms preserve additional structures onto the set.

– It is defined as a ~~bijective~~ bijection from a set to itself.
↳ bijective map.
↳ one-to-one → Existence of inverse element
onto → no element is left alone.

a represents one possible permutation.



Some additional theorems

1) Regular representations

Let $(S, \circ)$ be a magma → Algebraic structure closed under a binary ?? operation $\circ$.

(i) The mapping $\lambda_a : S \to S$ is defined as
$\forall x \in S : \lambda_a(x) = a \circ x$ ⟶ Known as left-regular representations of $(S, \circ)$ w.r.t a.

(ii) The mapping $\rho_a : S \to S$ is defined as "
$\forall x \in S : \rho_a(x) = x \circ a$ ⟶ right-regular representation

2) Regular representation of invertible element is permutation

Let $(S, \circ)$ be a monoid → Semi-group with id ↳ magma with associative operation.
Let $a \in S$ be invertible ↳ a has an inverse within S ie $\exists b \in S \mid a \circ b = b \circ a = e_S$ (id in S)
Then left-reg-rep λ_a and right-reg-rep ρ_a are permutations of S.

proof
Suppose $a \in (S, \circ)$ is invertible
A permutation is a bijection from a set to itself.
As $\lambda_a : S \to S$ and $\rho_a : S \to S$ are defined from S to S all we need to show is that they are bijections (both injective and surjective).

Surjectivity

Let $y \in S$

Then

(1) $y = (a \circ a^{-1}) \circ y$ (a is invertible)

$= a \circ (a^{-1} \circ y)$ Associativity of $\circ$ in monoid.

$= \lambda_a \circ (a^{-1} \circ y)$ Defn of λ_a

✱ Surjectivity implies can be represented in form $y = f(x)$ in the above case $y = \lambda_a(a^{-1} \circ y)$ the argument is still a^{-1} and the y is treated as a constant as in $y = f(kx) \Rightarrow \lambda_a$ is Surjective. ??

(2) $y = y \circ (a^{-1} \circ a)$ (a is invertible)

$= (y \circ a^{-1}) \circ a$ Associativity

$= \underbrace{(y \circ a^{-1})}$ $\circ \rho_a$ Defn of ρ_a

✱

Does this Contain an invertible element? We defined only a to be invertible in the monoid (not y).

Thus both λ_a and ρ_a are surjective.

Can be represented in form $y = f(x)$. i.e. $y = f \circ x$??

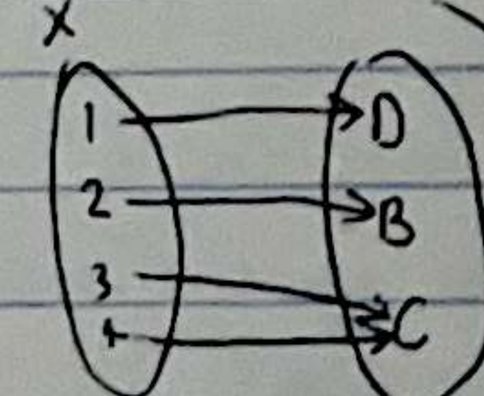
if $f : X \to Y$ then f is Surjective if

$\forall y \in Y, \exists x \in X : f(x) = y$

For All elements in the co-domain (all the ys) have at least one x whose arrow point towards them

x is not required to be unique.

All ys must be paired with (at least one)

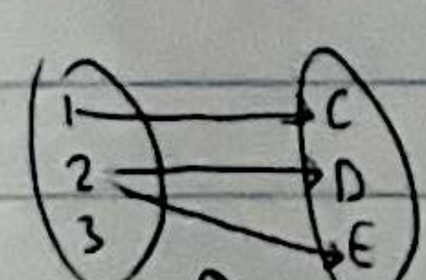


One y can have multiple x but all ys must be paired for surjectivity

Not injective

We have the atleast one x defn as one map from one x to y is the min. requirement for Surj.

Note



Can be said that

Note ~~also~~ it is surjective but not a function

Not a fnctin

one x cannot have multiple ys.

Injectivity

Invertible element of a monoid is Cancellable.

Corollary:
- The result follows from: Invertible element of associative Structure is cancellable.
- Since a monoid is associative, the proof follows from that.

Theorem

Let $(S, \circ)$ be an algebraic structure where $\circ$ is associative.

Let $(S, \circ)$ have identity e_s.

$\Rightarrow$ An element of $(S, \circ)$ which is invertible is also cancellable.

Proof

Let $a \in S$ be invertible

Suppose $a \circ x = a \circ y$

Then

$x = e_s \circ x$ (behaviour of id)

$= (a^{-1} \circ a) \circ x$ (behaviour of inverse)

$= a^{-1} \circ (a \circ x)$ (Associativity of $\circ$)

$= a^{-1} \circ (a \circ y)$ (By hypothesis)

$= (a^{-1} \circ a) \circ y$ (Associativity)

$= e_s \circ y$ (Behaviour of inverse)

$= y$ (Behaviour of id)

$\Rightarrow a \circ x = a \circ y \Rightarrow x = y$

We know that a is cancellable as it is invertible and Invertible element of monoid is cancellable.

Logical Connective.

If p is true then q is true AND if q is true then p is true. (biconditional)

Theorem

- Cancellable iff Regular Representation is injective.

p iff q → $p \iff q$ ↘ if and only if.

Left Cancellable

Suppose $a \in S$ is left Cancellable

Then : $a \circ x = a \circ y \Rightarrow x = y$

From defn of reg-rep.

$\lambda_a(x) = a \circ x$

Thus $\lambda_a(x) = \lambda_a(y) \Rightarrow x = y$

and so left regular representation is injective.

□

Suppose $\lambda_a(x)$ is injective

Then : $\lambda_a(x) = \lambda_a(y) \Rightarrow x = y$

From defn of left reg-rep

$\lambda_a(x) = a \circ x$

Thus $a \circ x = a \circ y \Rightarrow x = y$

and so a is left Cancellable

■

Right Cancellable

Suppose $a \in S$ is right Cancellable

Then $x \circ a = y \circ a \Rightarrow x = y$

From defn of reg-rep.

$\rho_a(x) = x \circ a$

Thus $\rho(x) = \rho(y) \Rightarrow x = y$

and so right regular representation is injective.

□

Suppose $\rho_a(x)$ is injective

Then $\rho_a(x) = \rho_a(y) \Rightarrow x = y$

From defn of right reg-rep.

$\rho_a(x) = x \circ a$

Thus $x \circ a = y \circ a \Rightarrow x = y$

and so a is right Cancellable.

■

Injectivity

- From invertible element of monoid is cancellable, as a is ~~ca~~ invertible, it must be cancellable.
- From cancellable iff regular representation is injective, it follows that both λ_a and ρ_a are injective.

Since the regular representations are both one-to-one and ~~on to~~ onto, they are bijective.

From previous works it follows that regular representation of invertible element is permutation.

From this we can say that regular representations in groups are permutations.

Theorem

Let $(G, \circ)$ be a group
Let $a \in G$ be any element of G.
Then λ_a and ρ_a are permutations of G.

Proof

1) All elements of a group are by $\text{def}^{\underline{n}}$ invertible.

2) $\Rightarrow$ Regular representation of invertible element is permutation applies.

Composition of Mappings

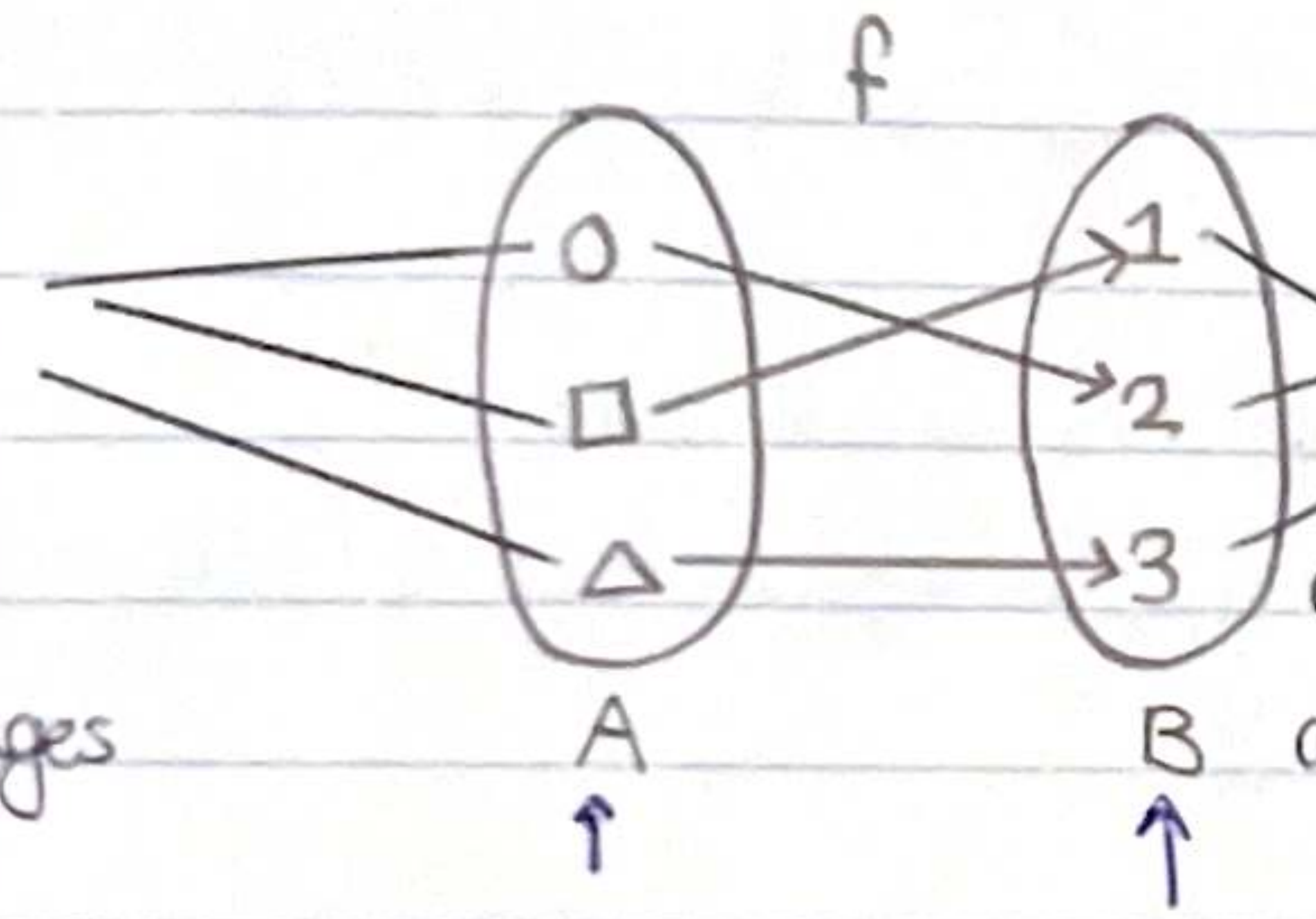
Note: Image is a subset of the codomain

Defn

Let S_1, S_2, S_3 be sets

Let $f_1 : S_1 \to S_2$ and $f_2 : S_2 \to S_3$ be mappings such that the domain of f_2 is the same set as the codomain of f_1.

Nomenclature



Elements of domain are known as pre-images

Elements of Cdm are known as images

Domain (Departure Set) Dom

Codomain (Arrival Set) Cdm

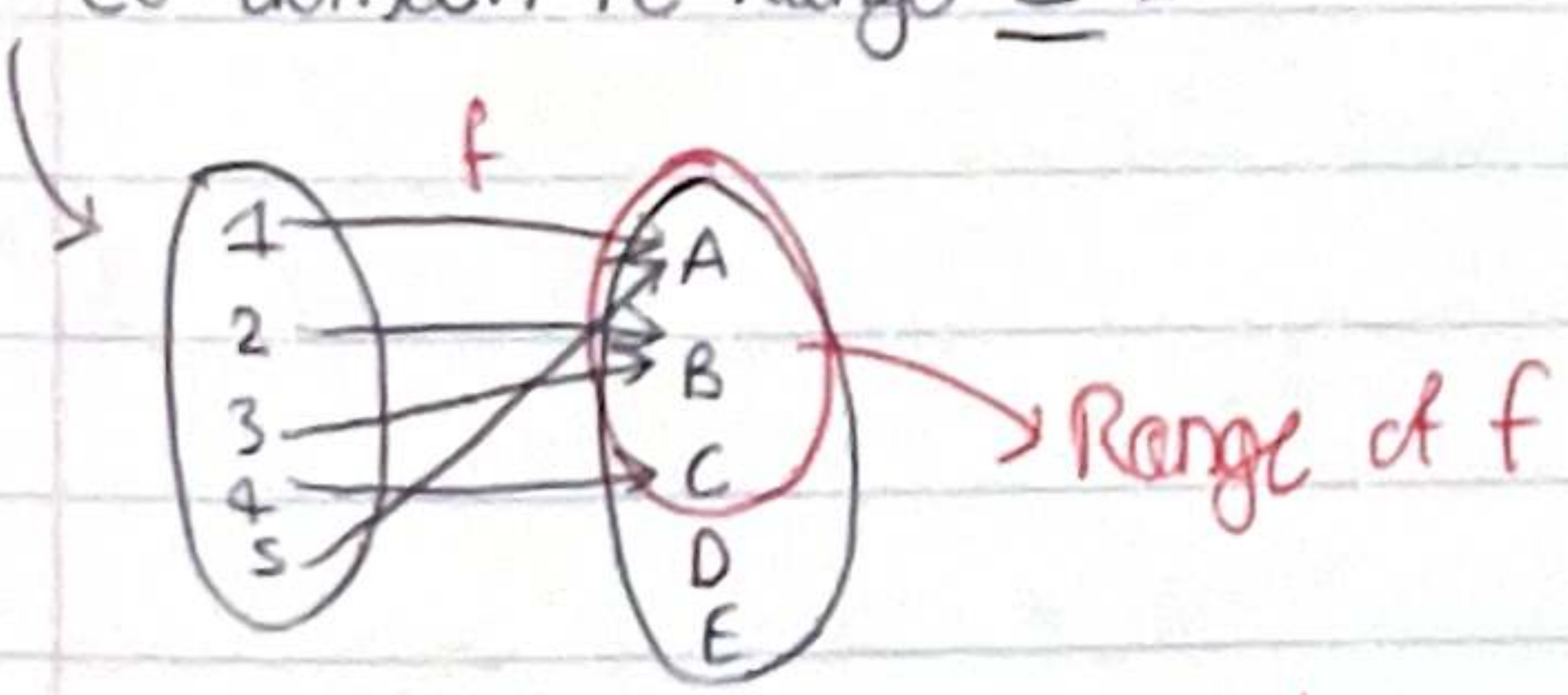
Note: The function f is a valid relation for both Sets and all their elements. ie. f is valid for o, □, △ and there is NO f_1 for o f_2 for □ . . .

A function is between sets

Similarly, a functor maps all algebraic structures in a category to another.

Is a natural transformation similar? ie. is only one N·T valid for all possible functors between categories or each pair of functors has a specific N·T?

Range is the subset of the co-domain ie Range $\subseteq$ B



In case of injectivity, Co-domain = Range?

$f : x \mapsto 1/x$

Note: $Cdm(f) = \mathbb{R}/\{0\}$

eg $f : \mathbb{R} \to \mathbb{R}$

$f : x \mapsto x^2$ ← chosen input values

$Dom(f) = \mathbb{R}$ ← where range lies

$Cdm(f) = \mathbb{R}$ ← value function achieves

$Range(f) = [0, \infty) \subseteq \mathbb{R}$ (Cdm)

Ambiguous — Image $Im(f)$ ← Image of element of domain 2.

1st defn $f(2) = 4$

2nd defn $f([2,3]) = [4, 9]$

* Pre-image is the sub-set of the domain that is completely mapped to the image subset of the co-domain.

Defn 1,

The composite mapping $f_2 \circ f_1$ is defined as :

✓ $\forall x \in S_1 \mid (f_2 \circ f_1)(x) := f_2(f_1(x))$

Note : The equivalance of those 3 defns can be shown and proved.

Defn 2,

The composite of f_1 and f_2 is defined and denoted as :

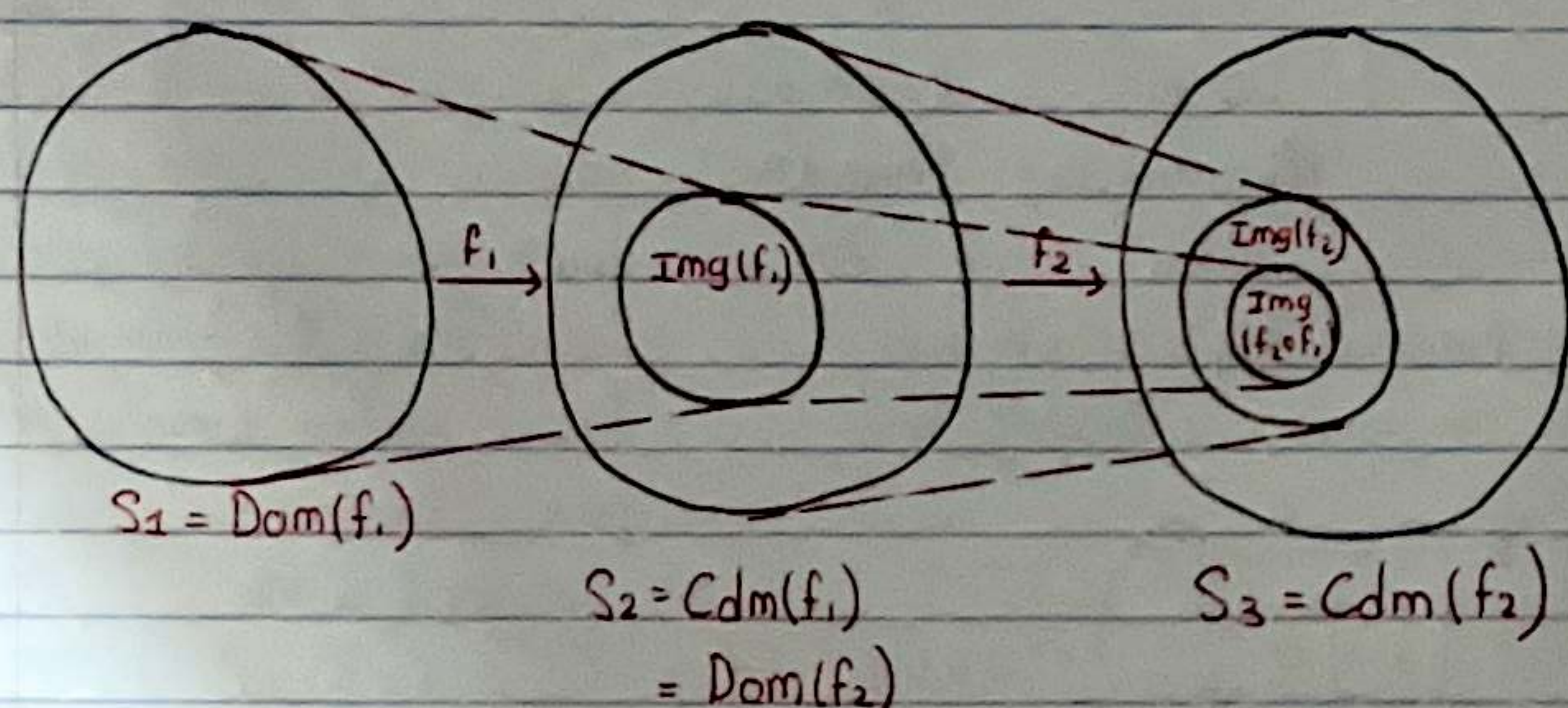
$f_2 \circ f_1 := \{(x, z) \in S_1 \times S_3 \mid (f_1(x), z) \in f_2\}$

input of $f_2 \circ f_1$ — output of $f_2 \circ f_1$ — input to f_2 — output of f_2

Defn 3

✓ The composite of f_1 and f_2 is defined and denoted as :

$f_2 \circ f_1 := \{(x, z) \in S_1 \times S_3 \mid \exists y \in S_2 \mid f_1(x) = y \land f_2(y) = z\}$



Composition of regular representations

1) Composition of left regular representations.

Theorem

Let $(S, *)$ be a semigroup $\longrightarrow$ Closure & Associativity.

Let λ_x be the left regular representation of $(S, *)$ with respect to x.

Let $\lambda_x \circ \lambda_y$ be defined as the composition of the mappings λ_x and λ_y

Then $\forall x, y \in S$

$\lambda_x \circ \lambda_y = \lambda_{x * y}$

Proof

Let $z \in S$

$(\lambda_x \circ \lambda_y)(z) = \lambda_x(\lambda_y(z))$ Defn Composition of mappings

$= \lambda_x(y * z)$ Defn Left reg. rep.

$= x * (y * z)$ Defn Left reg. rep.

$= (x * y) * z$ Semigroup Axiom (Associativity)

$= \lambda_{\underline{x * y}}(z)$ Defn Left reg. rep.

2) Composition of right regular representation.

Theorem

Let $(S, *)$ be a semigroup

Let ρ_x be the right regular representation of $(S, *)$ w.r.t x.

Let $\rho_x \circ \rho_y$ be defined as the composition of the mappings ρ_x and ρ_y.

Then $\forall x, y \in S$

$\rho_x \circ \rho_y = \rho_{\underline{y * x}}$