3.1 Two motivating examples of groups.

1. Integers modulo n.

e.g. modulo 12. The integers $\mathbb{Z}$ is partitioned into twelve congruence classes $[0], \ldots, [11]$

$$[m] = \{ x \in \mathbb{Z} : x \equiv m \pmod{12} \}$$

Let $\mathbb{Z}_n$ stand for the set of congruence classes. $|\mathbb{Z}_{12}| = 12$

There is a binary op $+$ on $\mathbb{Z}_{12}$.

defined by

$$[a]_{12} + [b]_{12} := [a+b]_{12}$$

Also there is the bin-op. $\times$ on $\mathbb{Z}_{12}$.

$$[a][b] := [ab].$$

Consider the structures/systems.

$(\mathbb{Z}_n, +)$ and $(\mathbb{Z}_n, \cdot)$.

eg. $(\mathbb{Z}_8, \cdot)$ as seen in Eg 3.2.

Prop 3.4 covered in N.T. lectures.
except maybe no. 6 - about
multiplicative inverses modulo n
(which do not always exist
see $(\mathbb{Z}_8, \cdot)$) $\leftarrow$

A multiplicative inverse for $a \in \mathbb{Z}_n$
is another element $a^{-1} \in \mathbb{Z}_n$
satisfying

$$a a^{-1} \equiv 1 \pmod{n}$$

$\Rightarrow$ eg. 2, 4, 6, 0 have no
multiplicative inverses in $\mathbb{Z}_8$.

Prop 3.4 (6)

Claim For $a \in \mathbb{Z}_n$, a has a

multiplicative inverse modulo n

iff $\gcd(a, n) = 1$.

Proof Observe the following chain of equivalences.

$a \in \mathbb{Z}_n$ has a mult. inverse.

$\iff \exists\, b \in \mathbb{Z}_n \quad ab \equiv 1 \pmod{n}$

$\iff n \mid ab - 1$, def of $\equiv$

$\iff \exists\, b \in \mathbb{Z}_n\ \exists\, q \in \mathbb{Z} \quad ab - 1 = nq$, def of div.

$\iff \exists\, b \in \mathbb{Z}\ \exists\, q \in \mathbb{Z} \quad 1 = ab - nq$

$\iff \gcd(a, n) = 1$, by def of gcd and by Bezout's / Euclidean Alg.

$\blacksquare$

We will see that $(\mathbb{Z}_8,+)$ is an example of a group and $(\mathbb{Z}_8,\cdot)$ is <u>not</u>. (as it lacks mult. inverses for <u>all</u> its elements).

Fix this by forming.

$$U(8) := \{x \in \mathbb{Z}_8 : \gcd(x,8)=1\}.$$
$$= \{1,3,5,7\}.$$

$(U(8),\cdot)$

will be a group.

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

(mult. mod 8).

2. A non-numerical example.

- Symmetries of a regular triangle (equilateral), i.e. all sides the same length.

- Transformations / isometries of the plane that preserve the triangle, i.e. are symmetries of the triangle

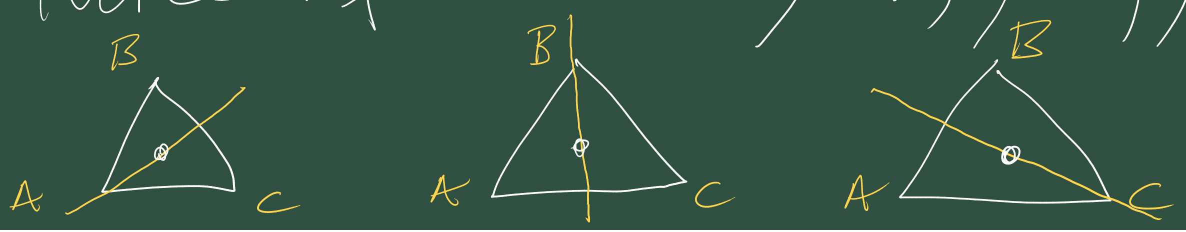
- (Rotations about points) or (Reflections in lines)

There are six such symmetries of $\triangle$

ρ_1 = rot. clockwise by 1/3 of a full turn
ρ_2 = " " " 2/3 " " " "

id., ρ_1, ρ_2, μ_1, μ_2, μ_3

Three reflections μ_1, μ_2, μ_3



μ_1 μ_2 μ_3

These are <u>all</u> the symmetries

We label the set of them as

$$D_3 = \{ id, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3 \}$$

The relevant operation on these $f: \mathbb{R}^2 \to \mathbb{R}^2$ is the operation of composition.

ρ rho

μ mu.

for $\alpha, \beta \in D_3$

$$\alpha \circ \beta := \alpha \text{ after } \beta.$$

i.e. $(\alpha \circ \beta)(\underline{x}) = \alpha(\beta(\underline{x}))$

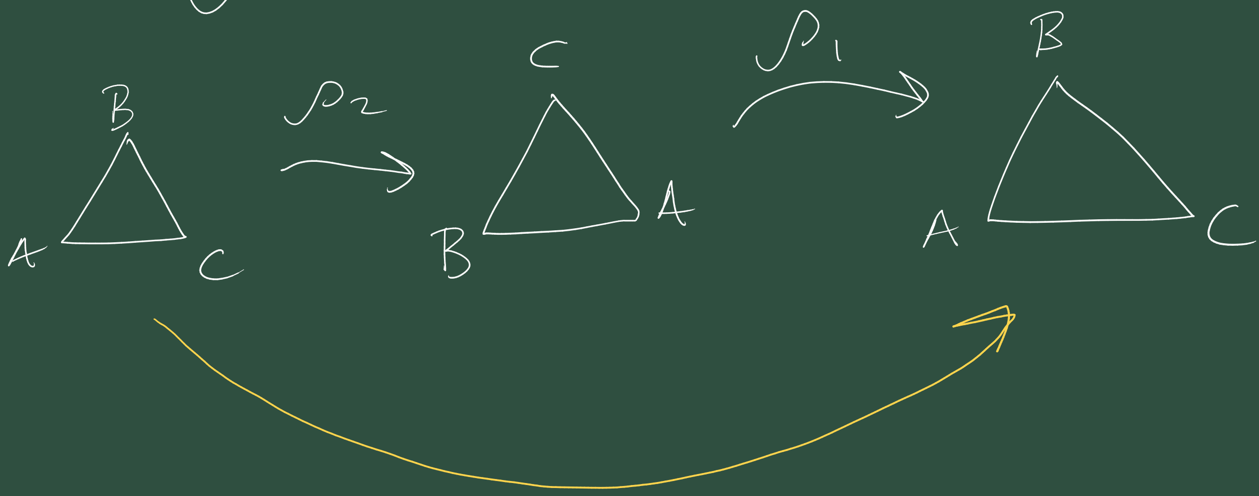
Composition is typically non-commutative

- Notice the composition of symmetries is always a symmetry.

i.e. $\circ$ is a binary operation on D_3

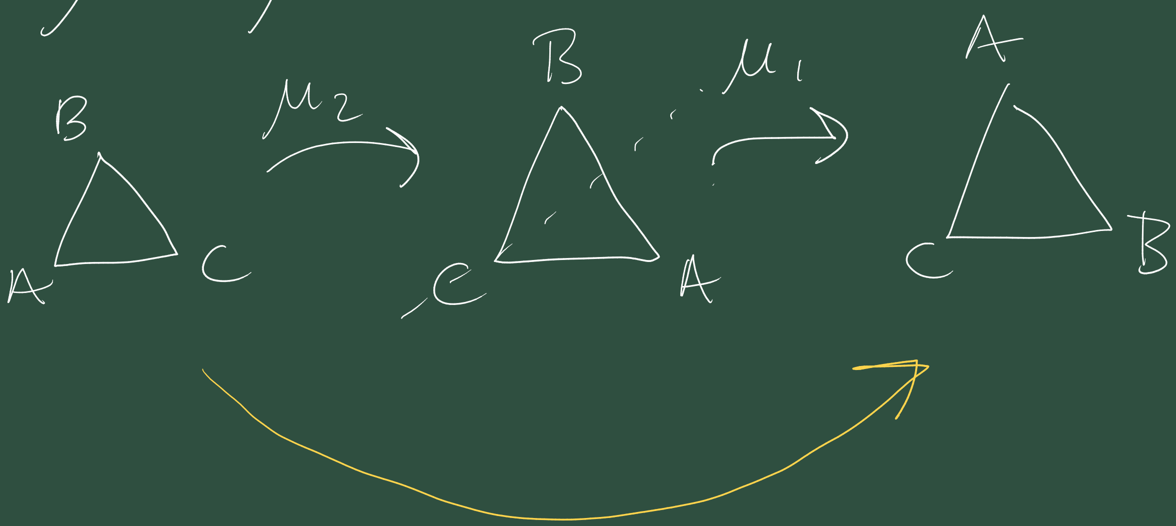
What does its multiplication table look like?

e.g. $\rho_1 \circ \rho_2 = ?\ \mathrm{id}.$



$\rho_1 \circ \rho_2$
$= \mathrm{id}.$

$\mu_1 \circ \mu_2 = ?$



$\mu_1 \circ \mu_2$
$= \rho_1$

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

Calculate them all to find

	id.	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id.	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	id.	ρ_1
μ_3	μ_3	μ_1	μ_2.	ρ_1	ρ_2.	id.

$(D_3, \circ)$ will be a group.

Multiplication tables / Cayley tables.

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

	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

Def 3.2. Definition of a group.

(12:22 Continue).

A group is a system/pair $(G, \circ)$

G is a set with a binary operation
non-empty closed

$\circ$ on G.

i.e. $\forall\ a, b \in G \quad a \circ b \in G$.

Satisfying.

Associativity.

$\forall\ a, b, c \qquad a \circ (b \circ c) = (a \circ b) \circ c$.

Identity

$\exists\ e \in G \quad \forall\ a \in G \quad a \circ e = e \circ a = a$

Inverses

$\forall\ a \in G \quad \exists\ a^{-1} \in G \quad a \circ a^{-1} = a^{-1} \circ a = e$

An abelian group $(G, \circ)$ is where $\circ$ is commutative on G

i.e. $\forall\ a, b \in G \quad a \circ b = b \circ a$.

Lots of examples

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

$(\mathbb{Z}_n, +)$ finite.

$-[a] = [-a] = [n-a]$

$(\mathbb{Z}_m, \cdot)$ not neccessarily a group due to lack of inverses.

$U(m) := \{x \in \mathbb{Z}_m : \gcd(x, m) = 1\}$.

$(U(m), \cdot)$ is a group.

$(D_3, \circ)$ is a group.

Claim: function composition is always associative.

$[f \circ (g \circ h)](x)$

$= f([g \circ h](x))$

$$= f(g(h(x)))$$
$$= [f \circ g](h(x))$$
$$= [[f \circ g] \circ h](x)$$

$$M_2(\mathbb{R}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \ a, b, c, d \in \mathbb{R} \right\}$$

$(M_2(\mathbb{R}), +)$ is a group. $id = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$A, -A$

$(M_2(\mathbb{R}), \times)$ is not a group
lack of inverses

$I,$

<u>Fix</u>. $GL_n(\mathbb{R}) = \{ A \in M_n(\mathbb{R}) : \det(A) \neq 0 \}$.

General Linear.

$\boxed{Q7}$ from Exercises.

$S := \mathbb{R} \setminus \{-1\}$

define a bin. op. $*$ on S by.

$$a * b := a + b + ab.$$

Prove $(S, *)$ is an abelian gp.

Is this binary op $*$ closed on S.

ie. For $a, b \in S$ is $a * b \in S$?

$$a * b = a + b + ab \in \mathbb{R}$$

But could $a + b + ab = -1$?

$$a + b + ab = -1$$

$$\iff a + b(1 + a) = -1$$

$$\iff b(1 + a) = -1 - a$$

$$\iff b = \frac{-1 - a}{1 + a}, \quad \begin{array}{l} a \in S \\ \Rightarrow a \neq -1 \\ \text{so } 1 + a \neq 0 \end{array}$$

$$\iff b = -1$$

which contradicts the fact that $b \neq -1$ as $b \in S$.

So ~~a*~~ $a, b \in S \Rightarrow a * b \in S$

Associative?
Identity element?
Inverses?
Commutative?