In this course we'll study groups, rings and fields. 1.1
We will start with groups.

<u>Definition 1.1</u> A <u>group</u> is a set G together with two maps ("operations")

- $G \times G \to G$, $(a,b) \mapsto ab$ ("multiplication")
- $G \to G$, $a \mapsto a^{-1}$ ("inversion", "taking inverses")

and a distinguished element $e = e_G \in G$ ("unity", "identity").
so that

(i) $ea = a = ae$ for all $a \in G$
(ii) $aa^{-1} = e = a^{-1}a$ for all $a \in G$
(iii) "multiplication is associative": for all $a_1, a_2, a_3 \in G$
$$a_1(a_2 a_3) = (a_1 a_2) a_3$$

Examples and nonexamples of groups.

1. $G = (0, \infty)$ = positive real numbers
$e = 1$
"multiplication" is ordinary multiplication of real numbers.
"inversion" is taking reciprocals $a^{-1} := \frac{1}{a}$.
This is a group.

2. $G = \mathbb{Z}$ The set of all integers
$e = 0$
"multiplication" is ordinary addition $+$
$e = 0$
"inversion" is negation "a^{-1}" $= -a$.
This is a group

3. The set $\mathbb{R}^\times = \{x \in \mathbb{R} \mid x \neq 0\}$,
The set of <u>nonzero</u> real numbers
$e = 1$, "multiplication" = ordinary multiplication

"inversion" = ~~taking~~ reciprocal "a^{-1}" = $\frac{1}{a}$.

This is a group.

4. $G = \mathbb{R}$,

"multiplication" = ordinary multiplication

$e = 1$

This is <u>not</u> a group. What goes wrong?

5. $G = \mathbb{Z}^{\geq 0}$ the set of nonnegative integers

"multiplication" is ordinary addition.

$e = 0$.

This is <u>not</u> a group. What goes wrong?

6. $G = \mathbb{R}^2$ coordinate plane

$e = \vec{0} = (0,0)$

"multiplication" is vector addition +

"inversion" is negation "$(\vec{v})^{-1}$" $= -\vec{v}$

(ie. "$(a,b)^{-1}$" $= (-a,-b)$)

This is a group.

7. $G = GL(2,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \; a,b,c,d \in \mathbb{R} \quad ad-bc \neq 0 \right\}$

= the set of 2×2 real invertible matrices.

"multiplication" is matrix multiplication:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

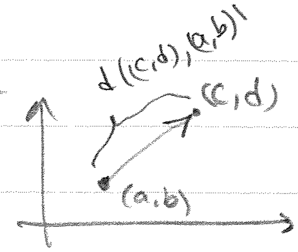
$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

"inversion" = taking the matrix inverse.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} := \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$GL(2, \mathbb{R})$ is a group, the general linear group.
(of size 2, real entries)

Rigid motions of the plane $\mathbb{R}^2$.



Recall: given two points $(a,b), (c,d) \in \mathbb{R}^2$ the distance

$$d((a,b),(c,d))$$

between them is the Euclidean distance

$$d((a,b),(c,d)) = ((c-a)^2 + (d-b)^2)^{1/2} = \|(c,d)-(a,b)\|$$

Definition A map $f: \mathbb{R}^2 \to \mathbb{R}^2$ is a rigid motion (or an isometry) if f preserves the distance d: for any $\vec{v}, \vec{w} \in \mathbb{R}^2$

$$d(f(\vec{v}), f(\vec{w})) = d(\vec{v}, \vec{w})$$
$$(\ \|f(\vec{v}) - f(\vec{w})\| = \|\vec{v} - \vec{w}\|\ )$$

Ex: • $f(\vec{v}) = \vec{v} + (1,2)$ is an isometry:

$$\|f(\vec{v}) - f(\vec{w})\| = \|(\vec{v} + (1,2)) - (\vec{w} + (1,2))\| = \|\vec{v} - \vec{w}\|$$

• $I(\vec{v}) = \vec{v}$ is a rigid motion.

• a rotation by angle θ (clockwise or counter-clockwise) is a rigid motion.

Note: if $f: \mathbb{R}^2 \to \mathbb{R}^2$ and $g: \mathbb{R}^2 \to \mathbb{R}^2$ are rigid motions then so is their composite $g \circ f: \mathbb{R}^2 \to \mathbb{R}^2$

Proof

Recall: $(g\circ f)(\vec{v}) = g(f(\vec{v}))$.

Now: $\|(g\circ f)(\vec{v}) - (g\circ f)(\vec{w})\| = \|g(f(\vec{v})) - g(f(\vec{w}))\|$
$= \|f(\vec{v}) - f(\vec{w})\|$ since g is an isometry
$= \|\vec{v} - \vec{w}\|$ since f is an isometry. $\square$

Theorem 1.1 The set $Euc(2) = \{f: \mathbb{R}^2 \to \mathbb{R}^2 \mid f \text{ is an isometry}\}$ of rigid motions of $\mathbb{R}^2$ is a group with the group operation = composition.

Proof. • The identity element of $Euc(2)$ is the identity map $I: \mathbb{R}^2 \to \mathbb{R}^2$, $I(\vec{v}) = \vec{v}$.
check that $I\circ f = f = f\circ I$ for all $f \in Euc(2)$.

• The composition of maps is associative $\Rightarrow$ the supposed group operation on $Euc(2)$ is associative.
(meaning "multiplication")

• To finish proving that $Euc(2)$ is a group we need to show that any isometry / rigid motion is invertible. We'll use:

Theorem (proved by Goodman in Ch 11)
Suppose $f: \mathbb{R}^2 \to \mathbb{R}^2$ is an isometry. Then there is a 2×2 matrix A and a vector $\vec{b} \in \mathbb{R}^2$ so that
$f(\vec{v}) = A\vec{v} + \vec{b}$ for all $\vec{v} \in \mathbb{R}^2$.
Moreover A is orthogonal: $A^T A = I = A A^T$.

Claim If $f(\vec{v}) = A\vec{v} + \vec{b}$ with $\vec{b} \in \mathbb{R}^2$, $A^T A = I$
then f^{-1} exists and $f^{-1}(\vec{w}) = A^T\vec{v} - A^T\vec{b}$.

We compute

$$f^{-1}(f(\vec{v})) = A^T(A\vec{v}+\vec{b}) - A^T\vec{b} = A^TA\vec{v} + A^T\vec{b} - A^T\vec{b}$$
$$= I\vec{v} = \vec{v}.$$

$$f(f^{-1}(\vec{w})) = A(A^T\vec{w} - A^T\vec{b}) + \vec{b} =$$
$$AA^T\vec{w} - AA^T\vec{b} + \vec{b} = I\vec{w} - \vec{b} + \vec{b} = \vec{w}.$$

Therefore $g(\vec{w}) := A^T\vec{w} - A^T\vec{b}$ is the inverse of $f(\vec{v}) = A\vec{v} + \vec{b}$.

We conclude that $Euc(2)$ is a group. $\square$