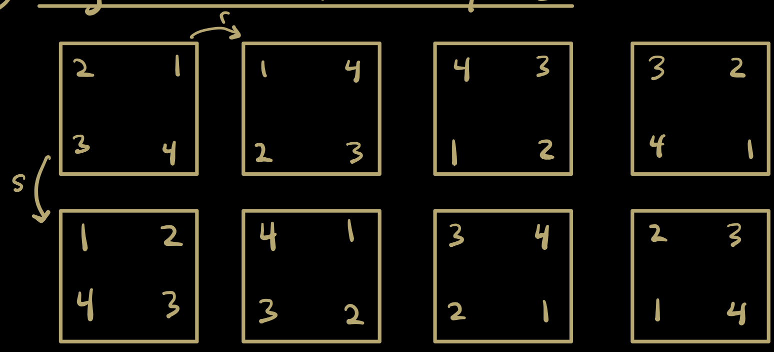
Symmetries

① Symmetries of a square



the group is not the collection of positions, but the operations we can perform

Notice: • we can compose operations, and this composition is associative.

• Not commutative.

• there's a symmetry which does nothing.

• every symmetry is invertible.

D_4

② Symmetries of Euclidean space

Recall: A linear transf. $T: \mathbb{R}^n \to \mathbb{R}^n$ can be rep'd by a matrix $A \in M_n(\mathbb{R})$. * using std. basis

Consider the set

$$SO(n) := \left\{ A \in M_n(\mathbb{R}) \;\middle|\; \begin{array}{c} \det A = 1 \\ A^T A = I \end{array} \right\}.$$

Such matrices satisfy

$$\langle A\vec{v}, A\vec{w} \rangle = \langle \vec{v}, \vec{w} \rangle.$$

So they preserve the Euclidean geometry of $\mathbb{R}^n$, since $\langle -,- \rangle$ gives angles & lengths.

• matrix mult. gives an assoc. composition

$$(AB)C = A(BC)$$ (again non-comm.)

• identity matrix does nothing

- $\det A \neq 0 \Rightarrow$ each $A \in SO(n)$ has an inverse A^{-1}.

  Check: $A^{-1} \in SO(n)$

Def'n of a group

A group is a pair $(G, \circ)$ consisting of a set G and a binary operation

$$\circ : G \times G \longrightarrow G$$

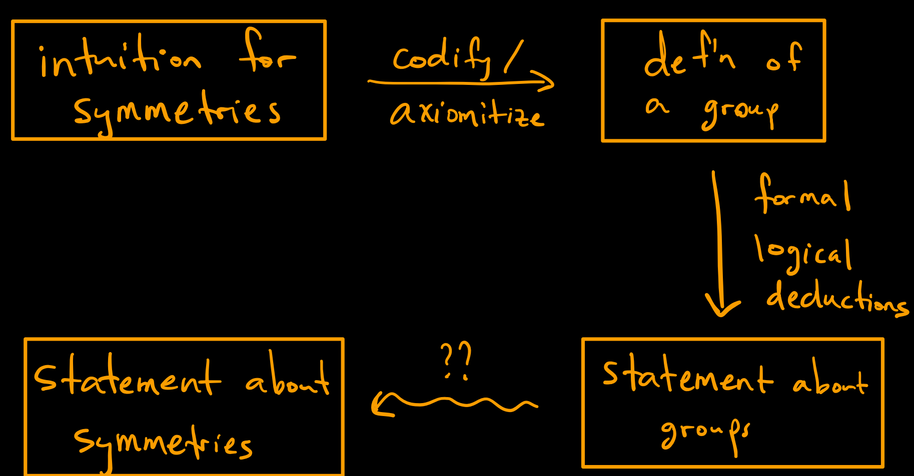
such that the following are satisfied:

- associativity: $(a \circ b) \circ c = a \circ (b \circ c)$, $\forall\, a, b, c \in G$;
- $\exists\, e \in G$ called the identity element, such that
$$a \circ e = e \circ a = a;$$
- $\forall\, a \in G$, $\exists$ an inverse element $a^{-1} \in G$ s.t.
$$a \circ a^{-1} = a^{-1} \circ a = e.$$

We'll call $(G, \circ)$ abelian or commutative if

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

Otherwise, non-abelian or non-commutative.



More examples

① $(\mathbb{Z}, +)$. identity : 0, inverse of a: $-a$

$(\mathbb{Z}_n, +)$. identity : 0, inverse of a: $-a$

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

orientation-preserving symm. of n-sided polygon

② Non-examples : $(\mathbb{Z}, \times)$ & $(\mathbb{Z}_n, \times)$

missing inverses

③ From $(\mathbb{Z}, \times)$ & $(\mathbb{Z}_n, \times)$ we can throw out all elements which fail to have inverses :

$(\mathbb{Z}^* = \{\pm 1\}, \times)$ is a group

$(\mathbb{Z}_n^* = \{\text{invertible elements of } \mathbb{Z}_n\}, \times)$

$=: (U(n), \times)$ is a group

group of units

④ $(M_n(\mathbb{R}), +)$ is a group. $e = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$.

$(M_n(\mathbb{R}), \times)$ is <u>not</u> a group. $e = I_n$.

Many matrices are not invertible.

group of units = invertible elements

$= (GL_n(\mathbb{R}), \times)$

$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}$.

This is the symmetry group for $\mathbb{R}^n$ as a vector space.