Day 2 May 29, 2024

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

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

such that:

- $\circ$ is associative — i.e.,
  $$(a \circ b) \circ c = a \circ (b \circ c),$$
  $\forall\, a, b, c \in G$;
- $\exists$ an identity element e satisfying
  $$e \circ a = a \circ e = a,$$
  $\forall\, a \in G$;
- every element $a \in G$ admits an inverse element $a^{-1} \in G$ satisfying $a \circ a^{-1} = a^{-1} \circ a = e$.

Rmk. We'll often suppress the $\circ$ notation.

Ex.

$k + m := k + m \pmod{n}$

① $(\mathbb{Z}, +)$ & $(\mathbb{Z}_n, +)$ are groups
$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

Are these symmetry groups for any structures?

② Neither $(\mathbb{Z}, \times)$ nor $(\mathbb{Z}_n, \times)$ is a group.
In $(\mathbb{Z}, \times)$, 0 is not invertible.
In fact, $\pm 1 \in \mathbb{Z}$ are the only invertible elts.
In $(\mathbb{Z}_n, \times)$, k is invertible iff
$$\gcd(k, n) = 1.$$

③ For each of $(\mathbb{Z}, \times)$ & $(\mathbb{Z}_n, \times)$ we can form the group of units:

$$\mathbb{Z}^* = \{\text{invertible elts of } (\mathbb{Z}, \times)\}$$
$$= \{\pm 1\}$$
$$U(n) = \mathbb{Z}_n^* = \{\, 0 \le k \le n-1 \mid \gcd(k,n) = 1 \,\}.$$

④ $M_n(\mathbb{R}) = \{n \times n \text{ matrices with real entries}\}$

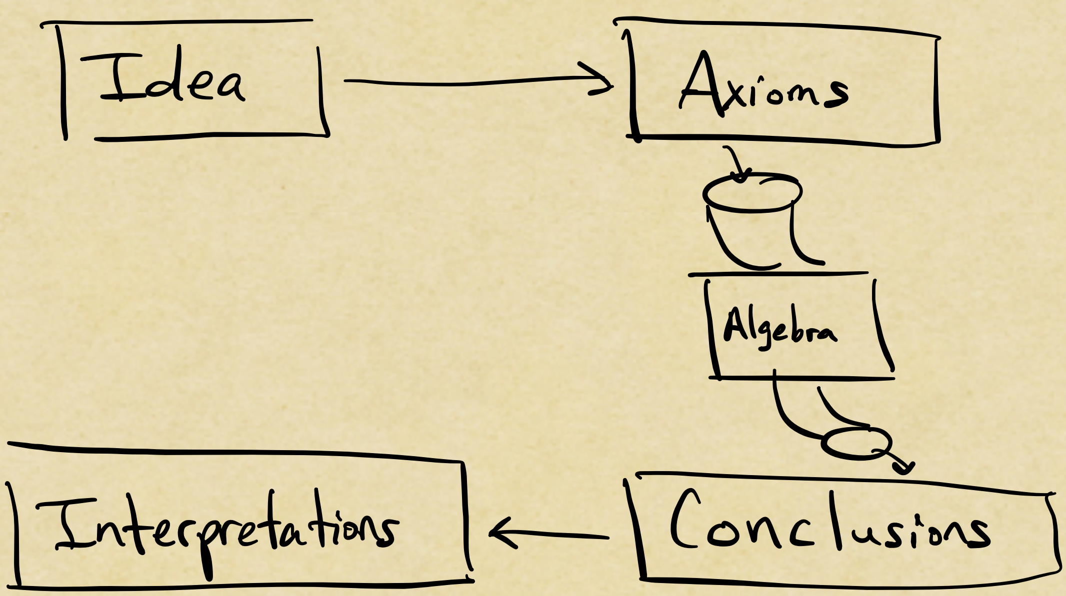
$(M_n(\mathbb{R}), +)$ is a group.

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

Taking the group of units gives

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

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



Basic properties of groups

Identities and inverses

<u>Prop</u>. Every group has a unique identity element.

Hint: Just need the identity property.

<u>Prop</u> Every element in a group has a unique inverse.

Hint: Associativity.

<u>Prop</u>. For any $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

(Proof.) B/c inverses are unique, we just NTS that $b^{-1}a^{-1}$ satisfies the inverse property for ab:

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb$$
$$= b^{-1}b = e.$$

Similarly, $(ab)(b^{-1}a^{-1}) = e$. ∎

<u>Prop</u>. For every $a \in G$, $(a^{-1})^{-1} = a$.

(Proof.) By definition, $a^{-1}(a^{-1})^{-1} = e$.

Left multiply by a to get $a a^{-1}(a^{-1})^{-1} = ae$

$\longrightarrow$ $(a^{-1})^{-1} = a$. ∎

Cancellation

$\exists$ unique

<u>Prop</u> For any fixed elements $a, b \in G$, $\exists!\ x, y \in G$ s.t. $ax = b$ and $ya = b$.

(Proof.) We'll prove that $ya=b$ has a unique sol'n.

Existence: Let $y=ba^{-1}$. Then

$$ya=(ba^{-1})a=b(a^{-1}a)=be=b \checkmark$$

Uniqueness: $\exists$ y_1 and y_2 satisfy

$y_1 a = b$ & $y_2 a = b$.

Suppose

Then

$$y_1 a = y_2 a.$$

Right multiply by a^{-1}:

$$(y_1 a)a^{-1} = (y_2 a)a^{-1}$$
$$y_1(aa^{-1}) = y_2(aa^{-1})$$
$$y_1 e = y_2 e$$
$$y_1 = y_2. \checkmark$$

$\blacksquare$

<u>Prop</u> (left cancellation) $\forall\ a,b,c \in G$,

$$ab=ac \Rightarrow b=c.$$

<u>Prop</u> (right cancellation) $\forall\ a,b,c \in G$,

$$ba=ca \Rightarrow b=c.$$

Exponential notation

We'll write $a^n = \underbrace{a \circ a \circ \cdots \circ a}_{n \text{ times}}$

& $a^{-n} = \underbrace{a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}}_{n \text{ times}}$

for any $n \geq 1$ and $a^0 = e$.

Prop For any $a, b \in G$ & $m, n \in \mathbb{Z}$,

① $a^m a^n = a^{m+n}$;

② $(a^m)^n = a^{mn}$;

③ $(ab)^n = (b^{-1}a^{-1})^{-n}$, with $(ab)^n = a^n b^n$ if G is abelian.

Subgroups

Recall:

$$SO(n) = \{A \in M_n(\mathbb{R}) \mid A^T A = I \text{ \& } \det A = 1\}$$
$$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}.$$

Each of $(SO(n), \times)$ and $(GL_n(\mathbb{R}), \times)$ is a group.

Symmetries of $\mathbb{R}^n$ as an oriented inner product space

Symmetries of $\mathbb{R}^n$ as a vector space

Notice: $SO(n) \subsetneq GL_n(\mathbb{R})$.

proper subgroup

Def'n. A subgroup of a group $(G, \circ_G)$ is a group $(H, \circ_H)$ such that H is a subset of G and $\circ_H$ is the restriction of $\circ_G$:

$$a \circ_H b = a \circ_G b,$$

$\forall\, a, b \in H$.

Ex

$$SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A = 1\} \subsetneq GL_n(\mathbb{R})$$
$$O(n) = \{A \in M_n(\mathbb{R}) \mid A^T A = I\} \subsetneq GL_n(\mathbb{R})$$

Check that these are subgroups under matrix mult.
What is $SL_n(\mathbb{R}) \cap O(n)$?