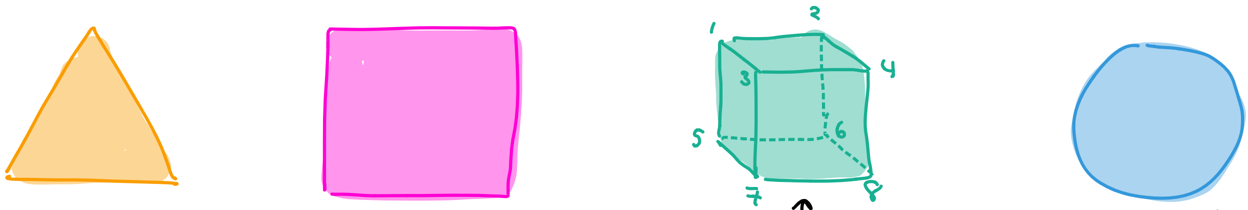
Groups (D+F 1.1)

Motivation/Example:

Symmetries of geometric objects



Here, we can rotate by fixed angles, or reflect over axes of symmetry, or some combination of the two

A little more complicated. There are as many symmetries as choices of "bottom square"

Way more symmetries. Infinitely many!

We can think of the set of symmetries (e.g. "rotate clockwise 90°) and the binary operation being composition — i.e. perform one followed by the other.

What properties should a set of symmetries satisfy?

1.) "Do nothing" is a symmetry (i.e. the identity)

2.) Every symmetry has a symmetry that undoes it (i.e. an inverse).

3.) Slightly more subtly: Composition of symmetries is associative. $\underbrace{(f \circ g)}_{\text{some symmetry}} \circ h = f \circ (g \circ h)$

A <u>group</u> generalizes the notion of a set of symmetries along w/ the composition operation.

Def: A group $\langle G, * \rangle$ is a set G along w/ a binary operation $*$ such that

1.) $\exists$ an element $e \in G$ s.t. $\forall\ x \in G$, $e * x = x * e = x$
   (e is called the <u>identity</u>).

2.) $\forall\ a \in G\ \exists\ a^{-1} \in G$ s.t. $a * a^{-1} = a^{-1} * a = e$.
   (a is called an <u>inverse</u> of a)

3.) $(a * b) * c = a * (b * c)\ \ \forall\ a, b, c \in G$ (associativity)

Def: $\langle G, * \rangle$ is <u>abelian</u> if $*$ is commutative.

Ex: $\langle \mathbb{Z}, + \rangle$ is a group:

- $(a + b) + c = a + (b + c)$, so it's associative,
- $0 + a = a + 0 = a\ \forall\ a \in \mathbb{Z}$, and
- $a + (-a) = (-a) + a = 0\ \ \forall\ a \in \mathbb{Z}$.

However, $\langle \mathbb{Z}_+, + \rangle$ is <u>not</u> a group. $*$ is associative,

the set of positive integers

but $e+a > a \quad \forall\, e, a \in \mathbb{Z}_+$. i.e. there's no identity.

Ex: $\langle \mathbb{Q} - \{0\}, \cdot \rangle$ is a group (1 is the identity)

$\langle \mathbb{Z} - \{0\}, \cdot \rangle$ is not a group: it has 1 as the only candidate for an identity, but there is no $a \in \mathbb{Z} - \{0\}$ s.t. $2a = 1$.

Ex: $\langle \{f : \mathbb{R} \to \mathbb{R}\}, + \rangle$ is a group w/ identity $f(x) = 0$. However, this is not a group w/ operations $\cdot$ or $\circ$.

Ex: Let $n \in \mathbb{Z}_+$. Define an equivalence relation on $\mathbb{Z}$ by $a \sim b \iff n \mid b-a$. i.e. $a \sim b \iff a \equiv b \pmod{n}$.

"divides"

Notice that every integer is equivalent to one of $0, 1, \ldots, n-1$. We write the equivalence classes as $\bar{0}, \bar{1}, \ldots, \overline{n-1}$. We call this set $\mathbb{Z}/n\mathbb{Z}$, and it forms a group under addition mod n.

i.e. $\bar{a} + \bar{b} = \overline{a+b}$ = the remainder of $a+b$ when dividing by n.

+ table for $\mathbb{Z}/4\mathbb{Z}$:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Ex: $\{-1,1\} \subseteq \mathbb{Z}$ w/ multiplication is a group.
(How does it compare to $\mathbb{Z}/2\mathbb{Z}$?)

Ex: (Harder) Fix a set S. Let $G = \{\varphi : S \to S \mid \varphi \text{ a bijection}\}$ where the operation is composition.

e.g. if $S = \{1, \dots, n\}$, G = set of permutations of n elements. How many elts in G? We'll come back to this example soon.

If $S = \{1,2\}$, then $G = \{id, f\}$, where $f(1)=2$, $f(2)=1$. This looks like the "same" group as both $\{1,-1\}$ and $\mathbb{Z}/2\mathbb{Z}$. We'll formalize this notion soon.

Basic properties of groups

Theorem: If $\langle G, * \rangle$ is a group and $a, b, c \in G$, then if $a*b = a*c$, then $b=c$, and if $b*a = c*a$ then $b=c$.

"left cancellation" "right cancellation"

Proof: Assume $a*b = a*c$. Then $\exists\, a^{-1} \in G$ s.t. $a^{-1}*a = e$.
Thus $a^{-1}*(a*b) = a^{-1}*(a*c)$

$\Rightarrow (a^{-1}*a)*b = (a^{-1}*a)*c$

$\Rightarrow e*b = e*c$

$\Rightarrow b = c$.

By a symmetric argument, right cancellation holds as well. $\square$

Theorem: If $\langle G, * \rangle$ is a group and $a, b \in G$, then $\exists$ a unique $x \in G$ s.t. $a * x = b$, and a unique $y \in G$ s.t. $y * a = b$.

Proof: Let $a, b \in G$. Let $a^{-1} \in G$ s.t. $a^{-1} * a = a * a^{-1} = e$.

Define $x = a^{-1} * b$. Then
$$a * x = a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b.$$

Thus, such an element exists. Now we show it's unique.

Suppose $a * c = b$. Then $a * c = a * x \Rightarrow c = x$, so x is unique.

A similar argument shows that the second part of the statement holds. $\square$

Cor: If e is an identity of $\langle G, * \rangle$, then e is the unique identity.

Pf: $\exists$ unique x, y s.t. $a * x = a$ and $y * a = a$, so $x = e = y$. $\square$

Cor: If $x \in G$, then x has a unique inverse x^{-1}, and if $x * c = e$ or $c * x = e$, then $c = x^{-1}$.

Cor: $(a * b)^{-1} = b^{-1} * a^{-1}$

Pf: $(a * b) * (b^{-1} * a^{-1}) = ((a * b) * b^{-1}) * a^{-1}$

$$= (a * (b * b^{-1})) * a^{-1}$$

$$= (a * e) * a^{-1}$$

$$= a * a^{-1} = e.$$

Thus, since inverses are unique, $(a * b)^{-1} = (b^{-1} * a^{-1})$ $\square$

EX: Let $G = \{e, a, b\}$. What are the possible groups w/ G as the underlying set?

e is the unique identity, so we need to find

$a * a$, $a * b$, $b * a$, and $b * b$.

If $a * b = a$, then $b = e$, which isn't the case.

similarly, $a * b \neq b$, and $b * a \neq a$ or b. Thus $a * b = e$, $b * a = e$.

$a^2 = a * a \neq a$ (since $a \neq e$) and $a^2 \neq e$ (since $a \neq b = a^{-1}$)

Thus $a^2 = b$, and, similarly $b^2 = a$, so the table becomes

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

can Check that this is in fact a group (relabel $e = 0, a = 1, b = 2$, and this becomes $\mathbb{Z}/3\mathbb{Z}$). In fact, this is the only group w/ 3 elements "up to isomorphism" (we will see what this means later).

Def: The order of a group G, $|G|$, is the cardinality of G.
If $a \in G$, then the order of a, $|a|$, is the smallest $n \in \mathbb{Z}_+$ s.t. $a^n = e$. If $a^n \neq e$ $\forall n$, then $|a| = \infty$.

Example: • $e^1 = e$, so $|e| = 1$. The identity is the only elt of order 1.

• In $\mathbb{Z}/3\mathbb{Z}$, $|0| = 1$,
$1+1+1 = 0$, so $|1| = 3$, and $2+2 = 1$, $1+2 = 0$, so $|2| = 3$.

• In $\langle \mathbb{Z}, + \rangle$, $\forall$ $n \in \mathbb{Z}$ s.t. $n \neq 0$, $|n| = \infty$.

Notation: From now on, for a group G, we will usually write the operation as $\cdot$ instead of $*$, and for $a \cdot b$, we'll write just ab. We'll denote the identity by 1, and denote $\underbrace{x \cdot \ldots \cdot x}_{n \text{ times}} = x^n$, and $\underbrace{x^{-1} \cdot \ldots \cdot x^{-1}}_{n \text{ times}} = x^{-n}$

However, if the group is abelian, we will sometimes use $+$ as the operation, in which case the identity will be 0, and we write $\underbrace{x + \ldots + x}_{n \text{ times}}$ as nx.

Subgroups

Def: $H \subseteq G$ is a subgroup of G, denoted $H \leq G$ if H is a group w/ the same operation as G.

Ex: $2\mathbb{Z} \leq \mathbb{Z}$, $\{0,2\} \leq \mathbb{Z}/4\mathbb{Z}$.

We'll come back to subgroups later.