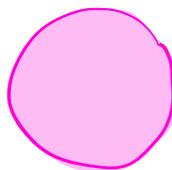
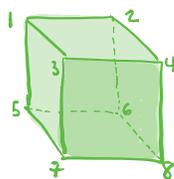
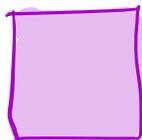


# Groups

## Motivation/Example:

### Symmetries of geometric objects



Here, we can rotate by fixed angles, or reflect over axes of symmetries, 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  $90^\circ$ ") 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 subtle: Composition of symmetries is associative.  $(f \circ g) \circ h = f \circ (g \circ h)$   
some symmetry

A group 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 identity element)

2.)  $\forall a \in G \exists a^{-1} \in G$  s.t.  $a * a^{-1} = a^{-1} * a = e$ .

( $a^{-1}$  is called an inverse of  $a$ )

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

**Def:**  $\langle G, * \rangle$  is abelian if  $*$  is commutative.

**Ex:**  $\langle \mathbb{Z}, + \rangle$  is a group:  $(a+b)+c = a+(b+c)$ , so it's associative.

$$0+a = a+0 = a \quad \forall a \in \mathbb{Z}, \text{ and } a+(-a) = (-a)+a = 0 \quad \forall a \in \mathbb{Z}.$$

However,  $\langle \mathbb{Z}_+, + \rangle$  is not a group.  $*$  is associative, but

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

**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 an identity, but there is no  $a \in \mathbb{Z} - \{0\}$  s.t.  $2 \cdot a = 1$ .

**Ex:**  $\langle \{f: \mathbb{R} \rightarrow \mathbb{R}\}, + \rangle$  is a group w/ identity  $f(x) = 0$ .

However, this is not a group w/ operations  $\cdot$  or  $\circ$  (HW problem)

**EX:** Let  $n \in \mathbb{Z}_+$ . Define an equivalence relation on  $\mathbb{Z}$  by  $a \sim b \Leftrightarrow n | (b-a)$ . i.e.  $a \sim b \Leftrightarrow a \equiv b \pmod{n}$ .

We write the equivalence classes  $\bar{0}, \bar{1}, \dots, \overline{n-1}$ . We call this set  $\mathbb{Z}/n\mathbb{Z}$ , and it forms a group under addition modulo  $n$ , i.e.  $\bar{a} + \bar{b} =$  the remainder of  $a+b \in \mathbb{Z}$  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.  
 $-1$  is its own inverse.

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

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

If  $S = \{1, 2\}$ , then  $G = \left\{ \text{id}, \begin{matrix} 1 \mapsto 2 \\ 2 \mapsto 1 \end{matrix} \right\}$ . This looks like the "same" group as  $\{-1, 1\}$ . In fact they are "isomorphic". 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  $b = c$ .

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

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

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

$$\Rightarrow e * b = e * c \Rightarrow b = c.$$

Similarly, by a symmetric argument, from  $b * a = c * a$  we can deduce  $b = c$ .  $\square$

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

$$\begin{aligned} \text{Define } x &= a^{-1} * b. \text{ Then } a * x = a * (a^{-1} * b) \\ &= (a * a^{-1}) * b \\ &= e * b = b. \end{aligned}$$

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

<sup>can</sup> 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  $\underbrace{x \cdot \dots \cdot x}_{n \text{ times}} = x^n$ , and  $\underbrace{x^{-1} \cdot \dots \cdot x^{-1}}_{n \text{ times}} = x^{-n}$ .

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

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:  $2\pi \leq \pi$ ,  $\{0, 2\} \leq \pi/4\pi$ .

We'll come back to subgroups soon.