Group Theory
There are few concepts in mathematics that are more primitive than the composition law.

- Nicolas Bourbaki
Group Theory

Study of symmetries and transformations of mathematical objects.

Also, the study of abstract algebraic objects called ‘groups’.

(of which $\mathbb{Z}_N$ and $\mathbb{Z}_N^*$ are special cases)
What is group theory good for?

In theoretical computer science:

- Checksums, error-correction schemes
- Minimizing randomness-complexity of algorithms
- Cryptosystems
- Algorithms for quantum computers
- Hard instances of optimization problems
- Ketan Mulmuley’s approach to P vs. NP
- Laci Babai’s graph isomorphism algorithm
What is group theory good for?

In puzzles and games:

“15 Puzzle”

Rubik’s Cube

SET
What is group theory good for?

In math:

There’s a quadratic formula:

\[ x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \]
What is group theory good for?

In math:

There's a cubic formula:

\[
x_1 = -\frac{b}{3a} - \frac{1}{3a} \sqrt[3]{\frac{1}{2} \left[ 2b^3 - 9abc + 27a^2d + \sqrt{(2b^3 - 9abc + 27a^2d)^2 - 4(b^2 - 3ac)^3} \right]} - \frac{1}{3a} \sqrt[3]{\frac{1}{2} \left[ 2b^3 - 9abc + 27a^2d - \sqrt{(2b^3 - 9abc + 27a^2d)^2 - 4(b^2 - 3ac)^3} \right]}
\]

\[
x_2 = -\frac{b}{3a} + \frac{1 + i\sqrt{3}}{6a} \sqrt[3]{\frac{1}{2} \left[ 2b^3 - 9abc + 27a^2d + \sqrt{(2b^3 - 9abc + 27a^2d)^2 - 4(b^2 - 3ac)^3} \right]} + \frac{1 - i\sqrt{3}}{6a} \sqrt[3]{\frac{1}{2} \left[ 2b^3 - 9abc + 27a^2d - \sqrt{(2b^3 - 9abc + 27a^2d)^2 - 4(b^2 - 3ac)^3} \right]}
\]

\[
x_3 = -\frac{b}{3a} + \frac{1 - i\sqrt{3}}{6a} \sqrt[3]{\frac{1}{2} \left[ 2b^3 - 9abc + 27a^2d + \sqrt{(2b^3 - 9abc + 27a^2d)^2 - 4(b^2 - 3ac)^3} \right]} + \frac{1 + i\sqrt{3}}{6a} \sqrt[3]{\frac{1}{2} \left[ 2b^3 - 9abc + 27a^2d - \sqrt{(2b^3 - 9abc + 27a^2d)^2 - 4(b^2 - 3ac)^3} \right]}
\]
What is group theory good for?

In math:

There’s a quartic formula:
What is group theory good for?

In math:

There is **NO** quintic formula.
What is group theory good for?

In physics:

Predicting the existence of elementary particles before they are discovered.
So: What *is* group theory?

Let’s start with an example from

Head-to-Toe flip
Q: How many positions can it be in?

A: Four.
Group theory is not so much about objects (like mattresses).

It’s about the transformations on objects and how they (inter)act.
\begin{align*}
F(R(\text{mattress})) &= H(\text{mattress}) \\
H(F(\text{mattress})) &= R(\text{mattress}) \\
R(F(H(\text{mattress}))) &= \text{Id}(\text{mattress}) \\
F \circ R &= H \\
H \circ F &= R \\
R \circ F \circ H &= \text{Id} \\
R \circ \text{Id} \circ H \circ F \circ H &= H
\end{align*}
The kinds of questions asked:

What is $R \circ \text{Id} \circ H \circ F \circ H$?

Do transformations $A$ and $B$ “commute”?  
I.e., does $A \circ B = B \circ A$?

What is the “order” of transformation $A$?  
I.e., how many times do you have to apply $A$ before you get to $\text{Id}$?
Definition of a group of transformations

Let $X$ be a set.

Let $G$ be a set of bijections $p : X \rightarrow X$.

We say $G$ is a group of transformations if:

1. If $p$ and $q$ are in $G$ then so is $p \circ q$.
   
   $G$ is “closed” under composition.

2. The ‘do-nothing’ bijection $\text{Id}$ is in $G$.

3. If $p$ is in $G$ then so is its inverse, $p^{-1}$.
   
   $G$ is “closed” under inverses.
Example: Rotations of a rectangular mattress

\[ X = \text{set of all physical points of the mattress} \]

\[ G = \{ \text{Id, Rotate, Flip, Head-to-toe} \} \]

Check the 3 conditions:

1. If \( p \) and \( q \) are in \( G \) then so is \( p \cdot q \).

2. The ‘do-nothing’ bijection \( \text{Id} \) is in \( G \).

3. If \( p \) is in \( G \) then so is its inverse, \( p^{-1} \).
Example: Symmetries of a directed cycle

\[ X = \text{labelings of the vertices by } 1,2,3,4 \]

\[ |X| = 24 \]

\[ G = \text{permutations of the labels which don’t change the graph} \]

\[ |G| = 4 \]

\[ G = \{ \text{Id, Rot}_{90}, \text{Rot}_{180}, \text{Rot}_{270} \} \]
Example: Symmetries of a directed cycle

\[ G = \{ \text{Id}, \text{Rot}_{90}, \text{Rot}_{180}, \text{Rot}_{270} \} \]

\[ X = \text{labelings of directed 4-cycle} \]

Check the 3 conditions:

1. If \( p \) and \( q \) are in \( G \) then so is \( p \cdot q \).

2. The ‘do-nothing’ bijection \( \text{Id} \) is in \( G \).

3. If \( p \) is in \( G \) then so is its inverse, \( p^{-1} \).

“Cyclic group of size 4”
Example: Symmetries of undirected n-cycle

\[ X = \text{labelings of the vertices by } 1, 2, \ldots, n \]

\[ G = \text{permutations of the labels which don't change the graph} \]

\[ |G| = 2^n \]
Example: Symmetries of **undirected** n-cycle

\[ X = \text{labelings of the vertices by } 1, 2, \ldots, n \]

\[ G = \text{permutations of the labels which don't change the graph} \]

\[ |G| = 2n \]

+ one clockwise twist
Example: Symmetries of \textbf{undirected} n-cycle

$X = \text{labelings of the vertices by } 1, 2, \ldots, n$

$G = \text{permutations of the labels which don’t change the graph}$

$|G| = 2n$

+ one clockwise twist
Example: Symmetries of *undirected* $n$-cycle

$X =$ labelings of the vertices by $1, 2, \ldots, n$

$|X| = n!$

$G =$ permutations of the labels which don’t change the graph

$|G| = 2n$

$G = \{ \text{Id}, \ n-1 \text{ ‘rotations’}, \ n \text{ ‘reflections’} \} \quad \text{‘Dihedral group of size 2n’}$
Effect of the 16 elements of $D_8$ on a stop sign
Example: “All permutations”

\[ X = \{1, 2, \ldots, n\} \]

\[ G = \text{all permutations of } X \]

e.g., for \( n = 4 \), a typical element of \( G \) is:

\[
\begin{pmatrix}
1 & 2 & 3 & 4 \\
\downarrow & \downarrow & \downarrow & \downarrow \\
4 & 2 & 1 & 3
\end{pmatrix}
\]

“Symmetric group, Sym(n) or \( S_n \)”
More groups of transformations

Motions of 3D space: translations + rotations
(preserve laws of Newtonian mechanics)

Translations of 2D space by an integer amount horizontally and an integer amount vertically

Rotations which preserve an old-school soccer ball (icosahedron)
The group of mattress rotation

\[ G = \{ \text{Id, R, F, H} \} \]

<table>
<thead>
<tr>
<th></th>
<th>Id</th>
<th>R</th>
<th>F</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Id</td>
<td>R</td>
<td>F</td>
<td>H</td>
</tr>
<tr>
<td>R</td>
<td>R</td>
<td>Id</td>
<td>H</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>H</td>
<td>Id</td>
<td>R</td>
</tr>
<tr>
<td>H</td>
<td>H</td>
<td>F</td>
<td>R</td>
<td>Id</td>
</tr>
</tbody>
</table>

\[ \begin{align*}
\text{Id} \circ \text{Id} &= \text{Id} \\
\text{Id} \circ \text{R} &= \text{R} \\
\text{Id} \circ \text{F} &= \text{F} \\
\text{Id} \circ \text{H} &= \text{H} \\
\text{R} \circ \text{Id} &= \text{R} \\
\text{R} \circ \text{R} &= \text{Id} \\
\text{R} \circ \text{F} &= \text{H} \\
\text{R} \circ \text{H} &= \text{F} \\
\text{F} \circ \text{Id} &= \text{F} \\
\text{F} \circ \text{R} &= \text{H} \\
\text{F} \circ \text{F} &= \text{Id} \\
\text{F} \circ \text{H} &= \text{R} \\
\text{H} \circ \text{Id} &= \text{H} \\
\text{H} \circ \text{R} &= \text{F} \\
\text{H} \circ \text{F} &= \text{R} \\
\text{H} \circ \text{H} &= \text{Id} \end{align*} \]
The laws of the dihedral group of size 10

\[ G = \{ \text{Id, } r_1, r_2, r_3, r_4, f_1, f_2, f_3, f_4, f_5 \} \]

<table>
<thead>
<tr>
<th></th>
<th>Id</th>
<th>(r_1)</th>
<th>(r_2)</th>
<th>(r_3)</th>
<th>(r_4)</th>
<th>(f_1)</th>
<th>(f_2)</th>
<th>(f_3)</th>
<th>(f_4)</th>
<th>(f_5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Id</td>
<td>(r_1)</td>
<td>(r_2)</td>
<td>(r_3)</td>
<td>(r_4)</td>
<td>(f_1)</td>
<td>(f_2)</td>
<td>(f_3)</td>
<td>(f_4)</td>
<td>(f_5)</td>
</tr>
<tr>
<td>(r_1)</td>
<td>(r_1)</td>
<td>(r_2)</td>
<td>(r_3)</td>
<td>(r_4)</td>
<td>Id</td>
<td>(f_4)</td>
<td>(f_5)</td>
<td>(f_1)</td>
<td>(f_2)</td>
<td>(f_3)</td>
</tr>
<tr>
<td>(r_2)</td>
<td>(r_2)</td>
<td>(r_3)</td>
<td>(r_4)</td>
<td>Id</td>
<td>(r_1)</td>
<td>(f_2)</td>
<td>(f_3)</td>
<td>(f_4)</td>
<td>(f_5)</td>
<td>(f_1)</td>
</tr>
<tr>
<td>(r_3)</td>
<td>(r_3)</td>
<td>(r_4)</td>
<td>Id</td>
<td>(r_1)</td>
<td>(r_2)</td>
<td>(f_5)</td>
<td>(f_1)</td>
<td>(f_2)</td>
<td>(f_3)</td>
<td>(f_4)</td>
</tr>
<tr>
<td>(r_4)</td>
<td>(r_4)</td>
<td>Id</td>
<td>(r_1)</td>
<td>(r_2)</td>
<td>(r_3)</td>
<td>(f_3)</td>
<td>(f_4)</td>
<td>(f_5)</td>
<td>(f_1)</td>
<td>(f_2)</td>
</tr>
<tr>
<td>(f_1)</td>
<td>(f_1)</td>
<td>(f_3)</td>
<td>(f_5)</td>
<td>(f_2)</td>
<td>(f_4)</td>
<td>Id</td>
<td>(r_3)</td>
<td>(r_1)</td>
<td>(r_4)</td>
<td>(r_2)</td>
</tr>
<tr>
<td>(f_2)</td>
<td>(f_2)</td>
<td>(f_4)</td>
<td>(f_1)</td>
<td>(f_3)</td>
<td>(f_5)</td>
<td>(r_2)</td>
<td>Id</td>
<td>(r_3)</td>
<td>(r_1)</td>
<td>(r_4)</td>
</tr>
<tr>
<td>(f_3)</td>
<td>(f_3)</td>
<td>(f_5)</td>
<td>(f_2)</td>
<td>(f_4)</td>
<td>(f_1)</td>
<td>(r_4)</td>
<td>(r_2)</td>
<td>Id</td>
<td>(r_3)</td>
<td>(r_1)</td>
</tr>
<tr>
<td>(f_4)</td>
<td>(f_4)</td>
<td>(f_1)</td>
<td>(f_3)</td>
<td>(f_5)</td>
<td>(f_2)</td>
<td>(r_1)</td>
<td>(r_4)</td>
<td>(r_2)</td>
<td>Id</td>
<td>(r_3)</td>
</tr>
<tr>
<td>(f_5)</td>
<td>(f_5)</td>
<td>(f_2)</td>
<td>(f_4)</td>
<td>(f_1)</td>
<td>(f_3)</td>
<td>(r_3)</td>
<td>(r_1)</td>
<td>(r_4)</td>
<td>(r_2)</td>
<td>Id</td>
</tr>
</tbody>
</table>
God created the integers. All the rest is the work of Man.

- Leopold Kronecker

Integers $\mathbb{Z}$ are closed under $+$:

- $a + b = b + a$
- $(a + b) + c = a + (b + c)$

$a + 0 = 0 + a = a$

$a + (\neg a) = 0$

Remainders mod 5:

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

$+_5 = \text{addition modulo 5}$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>
The power of algebra:
Abstract away the inessential features of a problem
Let’s define an abstract group. 

Let $G$ be a set.

Let $\diamond$ be a “binary operation” on $G$; think of it as defining a “multiplication table”.

E.g., if $G = \{ a, b, c \}$ then...

$\diamond$ is a binary operation.

This means that $c \diamond a = b$. 

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>c</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>b</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>c</td>
<td>b</td>
<td>c</td>
<td>a</td>
</tr>
</tbody>
</table>
Definition of an (abstract) group

We say \( G \) is a “group under operation \( \bullet \)” if:

0. [Closure] \( G \) is closed under \( \bullet \)
   i.e., \( a \bullet b \in G \quad \forall \ a, b \in G \)

1. [Associativity] Operation \( \bullet \) is associative:
   i.e., \( a \bullet (b \bullet c) = (a \bullet b) \bullet c \quad \forall \ a, b, c \in G \)

2. [Identity] There exists an element \( e \in G \)
   (called the “identity element”) such that
   \( a \bullet e = a, \ e \bullet a = a \quad \forall \ a \in G \)

3. [Inverse] For each \( a \in G \) there is an element \( a^{-1} \in G \)
   (called the “inverse of \( a \)”) such that
   \( a \bullet a^{-1} = e, \ a^{-1} \bullet a = e \)
Examples of (abstract) groups

Any group of transformations is a group.

(Only need to check that composition of functions is associative.)

E.g., the ‘mattress group’ (AKA Klein 4-group)

<table>
<thead>
<tr>
<th></th>
<th>Id</th>
<th>R</th>
<th>F</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Id</td>
<td>R</td>
<td>F</td>
<td>H</td>
</tr>
<tr>
<td>R</td>
<td>R</td>
<td>Id</td>
<td>H</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>H</td>
<td>Id</td>
<td>R</td>
</tr>
<tr>
<td>H</td>
<td>H</td>
<td>F</td>
<td>R</td>
<td>Id</td>
</tr>
</tbody>
</table>

identity element is Id

\[ R^{-1} = R \]
\[ F^{-1} = F \]
\[ H^{-1} = H \]
Examples of (abstract) groups

Any group of transformations is a group.

\( \mathbb{Z} \) (the integers) is a group under operation \(+\)

Check:

0. \( + \) really is a binary operation on \( \mathbb{Z} \)
1. \( + \) is associative: \( a+(b+c) = (a+b)+c \)
2. “e” is \( 0 \): \( a+0 = a, \ 0+a = a \)
3. “\( a^{-1} \)” is \( -a \): \( a+(-a) = 0, \ (-a)+a = 0 \)
Examples of (abstract) groups

Any group of transformations is a group.

\( \mathbb{Z} \) (the integers) is a group under operation \(+\)

\( \mathbb{R} \) (the reals) is a group under operation \(+\)

\( \mathbb{R}^+ \) (the positive reals) is a group under \(\times\)

\( \mathbb{Q} \setminus \{0\} \) (non-zero rationals) is a group under \(\times\)

\( \mathbb{Z}_n \) (the integers mod \(n\)) is a group under \(+ \) modulo \(n\)
NONEXAMPLES of groups

\( G = \{\text{all odd integers}\}, \text{operation} + \)

+ is not a binary operation on \( G \)!

(Natural numbers, +)

No inverses!

\( \mathbb{Z}, \text{operation} - \)

- is not associative! & No identity!

\( \mathbb{Z} \setminus \{0\}, \text{operation} \times \)

1 is the only possible identity element;
but then most elements don’t have inverses!
Permutation property

In a group table, every row and every column is a permutation of the group elements.

Follows from “cancellation property” (which we will prove shortly).

### Dihedral group of size 10

<table>
<thead>
<tr>
<th></th>
<th>O</th>
<th>Id</th>
<th>r₁</th>
<th>r₂</th>
<th>r₃</th>
<th>r₄</th>
<th>f₁</th>
<th>f₂</th>
<th>f₃</th>
<th>f₄</th>
<th>f₅</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Id</td>
<td>r₁</td>
<td>r₂</td>
<td>r₃</td>
<td>r₄</td>
<td>f₁</td>
<td>f₂</td>
<td>f₃</td>
<td>f₄</td>
<td>f₅</td>
<td></td>
</tr>
<tr>
<td>r₁</td>
<td>r₁</td>
<td>r₂</td>
<td>r₃</td>
<td>r₄</td>
<td>Id</td>
<td>f₄</td>
<td>f₅</td>
<td>f₁</td>
<td>f₂</td>
<td>f₃</td>
<td></td>
</tr>
<tr>
<td>r₂</td>
<td>r₂</td>
<td>r₃</td>
<td>r₄</td>
<td>Id</td>
<td>r₁</td>
<td>f₂</td>
<td>f₃</td>
<td>f₄</td>
<td>f₅</td>
<td>f₁</td>
<td></td>
</tr>
<tr>
<td>r₃</td>
<td>r₃</td>
<td>r₄</td>
<td>Id</td>
<td>r₁</td>
<td>r₂</td>
<td>f₅</td>
<td>f₁</td>
<td>f₂</td>
<td>f₃</td>
<td>f₄</td>
<td></td>
</tr>
<tr>
<td>r₄</td>
<td>r₄</td>
<td>Id</td>
<td>r₁</td>
<td>r₂</td>
<td>r₃</td>
<td>f₄</td>
<td>f₅</td>
<td>f₁</td>
<td>f₂</td>
<td>f₃</td>
<td></td>
</tr>
<tr>
<td>f₁</td>
<td>f₁</td>
<td>f₃</td>
<td>f₅</td>
<td>f₂</td>
<td>f₄</td>
<td>Id</td>
<td>r₃</td>
<td>r₁</td>
<td>r₄</td>
<td>r₂</td>
<td></td>
</tr>
<tr>
<td>f₂</td>
<td>f₂</td>
<td>f₄</td>
<td>f₁</td>
<td>f₃</td>
<td>f₅</td>
<td>r₂</td>
<td>Id</td>
<td>r₃</td>
<td>r₁</td>
<td>r₄</td>
<td></td>
</tr>
<tr>
<td>f₃</td>
<td>f₃</td>
<td>f₅</td>
<td>f₂</td>
<td>f₄</td>
<td>f₁</td>
<td>r₄</td>
<td>r₂</td>
<td>Id</td>
<td>r₃</td>
<td>r₁</td>
<td></td>
</tr>
<tr>
<td>f₄</td>
<td>f₄</td>
<td>f₁</td>
<td>f₃</td>
<td>f₅</td>
<td>f₂</td>
<td>r₁</td>
<td>r₄</td>
<td>r₂</td>
<td>Id</td>
<td>r₃</td>
<td></td>
</tr>
<tr>
<td>f₅</td>
<td>f₅</td>
<td>f₂</td>
<td>f₄</td>
<td>f₁</td>
<td>f₃</td>
<td>r₁</td>
<td>r₄</td>
<td>r₂</td>
<td>Id</td>
<td>r₃</td>
<td></td>
</tr>
</tbody>
</table>
Let’s connect back to Modular arithmetic
### Modular arithmetic

**Defn:** For integers $a, b$, and positive integer $n$, $a \equiv b \pmod{n}$ (read: “$a$ congruent to $b$ modulo $n$”) means $(a-b)$ is divisible by $n$, or equivalently $a \mod n = b \mod n$ (x mod n is remainder of x when divided by n, and belongs to $\{0,1,\ldots,n-1\}$)

Suppose $x \equiv y \pmod{n}$ and $a \equiv b \pmod{n}$. Then

1. $x + a \equiv y + b \pmod{n}$
2. $x * a \equiv y * b \pmod{n}$
3. $x - a \equiv y - b \pmod{n}$

So instead of doing $+,*,-$ and taking remainders, we can first take remainders and then do arithmetic.
Modular arithmetic

$(\mathbb{Z}_n, +)$ is group (understood that $+$ is $+n$)

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

What about $(\mathbb{Z}_5, *)$?

(* = multiplication modulo $n$)

NOT a group.

1 = candidate for identity, but 0 has no inverse.

Okay, what about $(\mathbb{Z}_5^*, *)$ where

$\mathbb{Z}_5^* = \mathbb{Z}_5 \setminus \{0\} = \{1, 2, 3, 4\}$

Turns out, it is a group.
Multiplication table mod 6 for \( \mathbb{Z}_6 \setminus \{0\} = \{1,2,3,4,5\} \)

2, 3, 4 have no inverse

NOT a group!
Theorem: For $a \in \{1,2,\ldots,n-1\}$, there exists $x \in \{1,2,\ldots,n-1\}$ such that $ax \equiv 1 \pmod{n}$ if and only if $\gcd(a,n) = 1$.

Proof (if) : Suppose $\gcd(a,n)=1$.

There exist integers $r,s$ such that $ra + sn = 1$ (Extended Euclid).

So $ar \equiv 1 \pmod{n}$.
Take $x = r \mod n$, $ax \equiv 1 \pmod{n}$ as well.
Multiplicative inverse in $\mathbb{Z}_n \setminus \{0\}$

Theorem: For $a \in \{1, 2, \ldots, n-1\}$, there exists $x \in \{1, 2, \ldots, n-1\}$ such that $ax \equiv 1 \pmod{n}$ if and only if $\gcd(a, n) = 1$

Proof (only if): Suppose $\exists x$, $ax \equiv 1 \pmod{n}$

So $ax - 1 = nk$ for some integer $k$.

If $\gcd(a, n) = c$, then $c$ divides $ax - nk$

Since $ax - nk = 1$, this means $c = 1$. 
Recall:

\[ \mathbb{Z}_n^* = \{ x \in \mathbb{Z}_n \mid \gcd(x, n) = 1 \} \]

Elements in \( \mathbb{Z}_n^* \) have multiplicative inverses

Exercise:

Check \((\mathbb{Z}_n^*, *)\) is a group

\(*\) is multiplication modulo \(n\)
$$Z_{12}^* = \{0 \leq x < 12 \mid \gcd(x, 12) = 1\} = \{1, 5, 7, 11\}$$

<table>
<thead>
<tr>
<th>* (12)</th>
<th>1</th>
<th>5</th>
<th>7</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>5</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>1</td>
<td>11</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>7</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>
$$Z_{15}^*$$

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>4</th>
<th>7</th>
<th>8</th>
<th>11</th>
<th>13</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>*</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>7</td>
<td>8</td>
<td>11</td>
<td>13</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>7</td>
<td>8</td>
<td>11</td>
<td>13</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>14</td>
<td>1</td>
<td>7</td>
<td>11</td>
<td>13</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>8</td>
<td>1</td>
<td>13</td>
<td>2</td>
<td>14</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>14</td>
<td>13</td>
<td>4</td>
<td>11</td>
<td>2</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>1</td>
<td>2</td>
<td>11</td>
<td>4</td>
<td>13</td>
<td>14</td>
<td>7</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>7</td>
<td>14</td>
<td>2</td>
<td>13</td>
<td>1</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
<td>11</td>
<td>7</td>
<td>1</td>
<td>14</td>
<td>8</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>14</td>
<td>14</td>
<td>13</td>
<td>11</td>
<td>8</td>
<td>7</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Fact: For prime $p$, the set $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$

Proof: It just follows from the definition!

For prime $p$, all $0 < x < p$ satisfy $\gcd(x,p) = 1$
Euler Phi Function $\phi(n)$

$\phi(n) = \text{size of } \mathbb{Z}_n^*$
= number of integers $1 \leq k < n$ that are relatively prime to $n$.

$p$ prime
$\iff \mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$
$\iff \phi(p) = p-1$
Back to abstract groups
Theorem 1:
If \((G, \bullet)\) is a group, identity element is unique.

Proof:
Suppose \(f\) and \(g\) are both identity elements.
Since \(g\) is identity, \(f \bullet g = f\).
Since \(f\) is identity, \(f \bullet g = g\).
Therefore \(f = g\).
Abstract algebra on groups

Theorem 2:
In any group \((G, \bullet)\), inverses are unique.

Proof:
Given \(a \in G\), suppose \(b, c\) are both inverses of \(a\).
Let \(e\) be \textit{the} identity element.
By assumption, \(a \bullet b = e\) and \(c \bullet a = e\).
Now: \(c = c \bullet e = c \bullet (a \bullet b)
\]
\[
= (c \bullet a) \bullet b \quad = e \bullet b \quad = b
\]
Theorem 3 (Cancellation): If $a \ast b = a \ast c$, then $b = c$

Proof: Multiply on left by $a^{-1}$

Similarly, $b \ast a = c \ast a$ implies $b = c$

So each row and each column of a group table are permutations of the group elements.
Theorem 3 (Cancellation): If \( a \blacklozenge b = a \blacklozenge c \), then \( b = c \)

Theorem 4:
For all \( a \) in group \( G \) we have \( (a^{-1})^{-1} = a \).

Theorem 5:
For \( a, b \in G \) we have \( (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} \).

Theorem 6:
In group \( (G, \cdot) \), it doesn’t matter how you put parentheses in an expression like \( a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_k \) (“generalized associativity”).
In abstract groups, it’s tiring to always write \( \bullet \). So we often write \( ab \) rather than \( a \bullet b \).

Sometimes write \( 1 \) instead of \( e \) for the identity. (When operation is “addition”, write \( 0 \) in place of \( e \)).

For \( n \in \mathbb{N}^+ \), write \( a^n \) instead of \( aaa \cdots a \) (\( n \) times). Also \( a^{-n} \) instead of \( a^{-1}a^{-1} \cdots a^{-1} \), and \( a^0 \) means \( 1 \). (again denote \( a+ a+ \cdots + a \) by \( na \) for additive groups)
Algebra practice

Problem: In the mattress group \{1, R, F, H\},
simplify the element \( R^2 (H^3 R^{-1})^{-1} \)

One (slightly roundabout) solution:

\[ H^3 = H \cdot H^2 = H \cdot 1 = H, \] so we reach \( R^2 (H \cdot R^{-1})^{-1} \).

\( (H \cdot R^{-1})^{-1} = (R^{-1})^{-1} \cdot H^{-1} = R \cdot H, \) so we get \( R^2 \cdot R \cdot H \).

But \( R^2 = 1, \) so we get \( 1 \cdot R \cdot H = R \cdot H = F. \)

Moral: the usual rules of multiplication, \textbf{except}...
Commutativity?

In a group we do **NOT NECESSARILY** have

\[ a \bullet b = b \bullet a \]

Actually, in the mattress group we **do** have this for all elements; e.g., \( RF = FR (=H) \).

**Definition:**

“\( a, b \in G \) commute” means \( ab = ba \).

“\( G \) is commutative” means **all** pairs commute.
In group theory, “commutative groups” are usually called **abelian** groups.

Niels Henrik *Abel* (1802–1829)
Norwegian
Died at 26 of tuberculosis 😞
Age 22: proved there is no quintic formula.
Evariste Galois (1811–1832)
French
Died at 20 in a dual 😞
Laid the foundations of group theory and Galois theory
Some abelian groups:

“Mattress group” ("Klein 4-group")
Symmetries of a directed cycle ("cyclic group")
(ℝ, +), (Zₙ*, ×)

Some nonabelian groups:

Symmetries of an undirected cycle ("dihedral group")
Permutation group Sₙ ("symmetric group on n elements")
Invertible n x n real matrices (under matrix product)
More fun groups:

Matrix groups

$SL_2(\mathbb{Z})$: Set of matrices

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

where $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$.

Operation: matrix mult.  Inverses:

$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Application: constructing expander graphs, ‘magical’ graphs crucial for derandomization.
Isomorphism

Here’s a group: \( V = \{ (0,0), (0,1), (1,0), (1,1) \} \)

\(+\) modulo 2 is the operation

There’s something familiar about this group…

<table>
<thead>
<tr>
<th>V</th>
<th>same after renaming:</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>00 01 10 11</td>
</tr>
<tr>
<td>00</td>
<td>00 01 10 11</td>
</tr>
<tr>
<td>01</td>
<td>01 00 11 10</td>
</tr>
<tr>
<td>10</td>
<td>10 11 00 01</td>
</tr>
<tr>
<td>11</td>
<td>11 10 01 00</td>
</tr>
</tbody>
</table>

The mattress group

<table>
<thead>
<tr>
<th>⋅</th>
<th>Id</th>
<th>R</th>
<th>F</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Id</td>
<td>R</td>
<td>F</td>
<td>H</td>
</tr>
<tr>
<td>R</td>
<td>R</td>
<td>Id</td>
<td>H</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>H</td>
<td>Id</td>
<td>R</td>
</tr>
<tr>
<td>H</td>
<td>H</td>
<td>F</td>
<td>R</td>
<td>Id</td>
</tr>
</tbody>
</table>
Groups \((G, \cdot)\) and \((H, \diamond)\) are “isomorphic” if there is a way to rename elements so that they have the same multiplication table.

Formally, bijection \(\sigma : G \rightarrow H\) such that
\[
\sigma(a \cdot b) = \sigma(a) \diamond \sigma(b) \quad \forall a, b \in G
\]

Fundamentally, they’re the “same” abstract group.
Isomorphism and orders

Obviously, if $G$ and $H$ are isomorphic we must have $|G| = |H|$.

$|G|$ is called the order / size of $G$.

E.g.: Let $C_4$ be the group of transformations preserving the directed 4-cycle.

$$|C_4| = 4$$

Q: Is $C_4$ isomorphic to the mattress group $V$?
Isomorphism and orders

Q: Is $C_4$ isomorphic to the mattress group $V$?

A: No!

$a^2 = 1$ for every element $a \in V$.

But in $C_4$, $\text{Rot}_{90}^2 = \text{Rot}_{270}^2 \neq \text{Rot}_{180}^2 = \text{Id}^2$

Motivates studying powers of elements.
Order of a group element

Let $G$ be a finite group. Let $a \in G$.

Look at 1, $a$, $a^2$, $a^3$, … till you get some repeat.

Say $a^k = a^j$ for some $k > j$.

Multiply this equation by $a^{-j}$ to get $a^{k-j} = 1$.

So the first repeat is always 1.

**Definition:** The order of $x$, denoted $\text{ord}(a)$, is the smallest $m \geq 1$ such that $a^m = 1$.

Note that $a$, $a^2$, $a^3$, …, $a^{m-1}$, $a^m=1$ all distinct.
Examples:

In mattress group (order 4),
\[ \text{ord}(\text{Id}) = 1, \quad \text{ord}(R) = \text{ord}(F) = \text{ord}(H) = 2. \]

In directed-4-cycle group (order 4),
\[ \text{ord}(\text{Id}) = 1, \quad \text{ord}(\text{Rot}_{180}) = 2, \quad \text{ord}(\text{Rot}_{90}) = \text{ord}(\text{Rot}_{270}) = 4. \]

In dihedral group of order 10
(symmetries of undirected 5-cycle)
\[ \text{ord}(\text{Id}) = 1, \quad \text{ord}(\text{any rotation}) = 5, \quad \text{ord}(\text{any reflection}) = 2. \]
**Order Theorem:** For a finite group $G$ & $a \in G$, $\text{ord}(a)$ always divides $|G|$.

Let $\text{ord}(a) = m$.

Claim: also of length $m$.

Because $xa^j = xa^k \Rightarrow a^j = a^k$. 
Order Theorem: \( \text{ord}(a) \) always divides \(|G|\).

Impossible.

Multiply on right by \( a^{-1} \).
Order Theorem: \( \forall a \in G, \; \text{ord}(a) \) divides \( |G| \).

G partitioned into cycles of size m.
**Order Theorem:** \( \text{ord}(a) \) always divides \(|G|\).

**Corollary:** If \(|G| = n\), then \(a^n = 1\) for all \(a \in G\).

**Proof:** Let \(\text{ord}(a) = m\). Write \(n = mk\).

Then \(a^n = (a^m)^k = 1^k = 1\).

**Corollary:** Euler’s Theorem: For \(a \in \mathbb{Z}_n^*\), \(a^{\phi(n)} = 1\)

That is, if \(\gcd(a,n) = 1\), then \(a^{\phi(n)} \equiv 1 \pmod{n}\)

**Corollary (Fermat’s little theorem):**

For prime \(p\), if \(\gcd(a,p) = 1\), then \(a^{p-1} \equiv 1 \pmod{p}\)
A finite group $G$ of order $n$ is cyclic if $G = \{e, b, b^2, \ldots, b^{n-1}\}$ for some group element $b$.

In such a case, we say the element $b$ "generates" $G$, or $b$ is a "generator" of $G$.

Examples:

- $(\mathbb{Z}_n, +)$ What is a generator?
- $C_4$ (Symmetries of directed 4-cycle)

Non-examples: Mattress group; any non-abelian group.
How many generators does \((\mathbb{Z}_n, +)\) have?

**Answer:** \(\phi(n)\)

b generates \(\mathbb{Z}_n\) \(\iff\) \(\exists a\ \text{s.t.} \ ba \equiv 1 \pmod{n}\)

\((ba = b+b+\ldots+b \ (a\ \text{times}))\)

Same holds for *any* cyclic group with \(n\) elements
Subgroups

Q: Is (Even integers, +) a group?
A: Yes. It is a “subgroup” of (\(\mathbb{Z},+\))

**Definition:** Suppose (G ,\(\bullet\)) is a group.

If H \(\subseteq\) G, and if (H,\(\bullet\)) is also a group,
then H is called a **subgroup** of G.

To check H is a subgroup of G, check:
1. H is closed under \(\bullet\)
2. \(e \in H\)
3. If \(h \in H\) then \(h^{-1} \in H\)

  • (3\textsuperscript{rd} condition follows from 1,2 if H is finite)
Every G has two trivial subgroups: \{e\}, G
Rest are called “proper” subgroups

Suppose \( k, 1 < k < n \), divides \( n \).

Q1. Is \( (\{0, k, 2k, 3k, \ldots, (n/k-1)k\}, +_n) \) subgroup of \( (\mathbb{Z}_n, +_n) \) ?
   Yes!

Q2. Is \( (\mathbb{Z}_k, +_k) \) a subgroup of \( (\mathbb{Z}_n, +_n) \)?
   No! it doesn’t even have the same operation

Q3. Is \( (\mathbb{Z}_k, +_n) \) a subgroup of \( (\mathbb{Z}_n, +_n) \)?
   No! \( \mathbb{Z}_k \) is not closed under \(+_n\)
Lagrange’s Theorem

**Theorem:** If $G$ is a finite group, and $H$ is a subgroup then $|H|$ divides $|G|$.

**Proof similar to order theorem.**

**Corollary (order theorem):** If $x \in G$, then $\text{ord}(x)$ divides $|G|$.

**Proof of Corollary:**

Consider the set $T_x = (x, x^2, x^3, \ldots)$

(i) $\text{ord}(x) = |T_x|$  

(ii) $(T_x, \cdot)$ is a subgroup of $(G, \cdot)$ \ (check!)
Definitions:
Groups; Commutative/abelian
Isomorphism; order of elements; subgroups

Specific Groups:
Klein 4-, cyclic, dihedral, symmetric, number-theoretic.

Doing:
Checking for “groupness”
Computations in groups

Theorem/proof:
Order Theorem; Lagrange Thm

Modular arithmetic
Euler theorem
More fun groups: 

Quaternion group

\[ Q_8 = \{ 1, -1, i, -i, j, -j, k, -k \} \]

**Multiplication**

1 is the identity defined by:

\[ (-1)^2 = 1, \quad (-1)a = a(-1) = -a \]
\[ i^2 = j^2 = k^2 = -1 \]
\[ ij = k, \quad ji = -k \]
\[ jk = i, \quad kj = -i \]
\[ ki = j, \quad ik = -j \]

**Exercise:** valid defn. of a (nonabelian) group.
Application to computer graphics

“Quaternions”: expressions like

\[ 3.2 + 1.4i −.5j +1.1k \]

which generalize complex numbers (\( \mathbb{C} \)).

Let \((x,y,z)\) be a unit vector, \(θ\) an angle, let

\[ q = \cos(θ/2) + \sin(θ/2)x i + \sin(θ/2)y j + \sin(θ/2)z k \]

Represent \(p=(a,b,c)\) in 3D space by quaternion \(P= a i + b j + c k\)

Then \(qPq^{-1}\) is its rotation by angle \(θ\) around axis \((x,y,z)\).