Last time, we talked about the cyclic group $C_m$:

$$C_m = \{ 1, x, x^2, \ldots, x^{m-1} \} \quad (x^m = 1)$$
caveat! the ... notation means the cases listed
to see the pattern may not all occur.

(Any group isomorphic to \( C_n \) is also called
a cyclic group.) an isomorphism is a renaming
of the element which makes
the group table will work the same way. (e.g. replace x by another letter, but less obvious remaining may also occur; we proved that every group of order 2 is isomorphic to \( \mathbb{Z}_2 \).)

with 2 element

HW: Every group of order 3 is isomorphic to \( \mathbb{Z}_3 \). Write a group multiplicatively (mental element) →

\[
\begin{array}{ccc}
1 & a & b \\
a & a & a \\
b & b & b \\
\end{array}
\]

only
<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>x</th>
<th>x^2</th>
<th>x^3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>x^2</td>
<td></td>
<td></td>
<td>x^2</td>
<td></td>
</tr>
<tr>
<td>x^3</td>
<td>x^2</td>
<td>x</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>x^4</td>
<td>x^3</td>
<td>1</td>
<td>1</td>
<td>x</td>
</tr>
</tbody>
</table>

The infinite cyclic group: \( \mathbb{Z} \)

Moves: shift by the length of a
natural number to the right or to the left.

Let \( x \) be the move of shifting by the length 1 to the right. But the group also contains \( x^{-1} \) : shift by 1 to the left.

By the inverse axiom

\[
\begin{array}{cccccc}
\ldots & x^{-1} & x^{-1} & 1 & x & x^2 & \ldots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\
& x^{-1} & x^2 & x^{-1} & 1 & x & \phantom{x^2} \\
& 1 & x^{-1} & 1 & x & x^2 & \phantom{x^2} \\
x & 1 & x^{-1} & x & \phantom{x^2} & \phantom{x^2} & \phantom{x^2} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\
\end{array}
\]

\[ m - n = m + (-n) \]

\[ x - x = x \]
What symbol can we use for the group operation?

Basically, any symbol: \( *, \#, \circ, \cdot \ldots \).

~ multiplicative notation

**Can we also use \( + \)?**

Yes, with caution.

If we use \( + \), the neutral element should be denoted \( 0 \).

\( \text{blackboard bold} \)
Example: The integers: \((\mathbb{Z}, +)\)

\((-m) + m = 0\)

we write the inverse as \(-x\) (instead of \(x^{-1}\)).

Note: The infinite cyclic group \((\mathbb{Z}, \cdot)\) is isomorphic to \((\mathbb{Z}, +)\).

\(1 \leftrightarrow 0\)

\(x^n \leftrightarrow n\)
\[ x^m \cdot x^m = x^{m+m} \]

\[ x^m \cdot x^m \leftrightarrow m+m \]

The additive notation for \( C_m \) (the finite\( (\mathbb{Z}/m,+) \) group):

\[ x^m = 1(C_m: \{0, 1, \ldots, m-1\}) \]

\[ \{1, x, \ldots, x^{m-1}\} \]

\[ 1 \leftrightarrow 0 \]

\[ k + l = \text{remainder of } k+l \text{ after} \]
In $\mathbb{Z}/10$. What is $8 + 5 = 3$?

$8 + 8 = 6$

In $\mathbb{Z}/24$. What is $17 + 18 = 11$?

$17 + 18 = 35$.

A group which is also commutative
\[ x \cdot y = y \cdot x \] (this is not true in all groups !!)

is called **Abelian**. (ABEL)

**USUALLY**, the additive notation is reserved for **Abelian groups**.

Why are cyclic groups so important?

Because we see them in every group when we take the powers (back to multiplicative
notation) of one element $x$ (or its inverse).

**Theorem:** The set of all powers of a single element $x$ in any group $G$ (written multiplicatively) forms a cyclic group (finite or infinite).

excluded when $G$ is finite.

for some $n$

Example \((\mathbb{Z} \times \mathbb{Z})^n = I\) on Rubik's cube

HW: 1 Calculate in $\mathbb{Z}/55$:

\[ 46 + 3 = \]
27 + 42 =

1 + 54 =

(note: not the neutral element, we are in additive notation)

2) Find an example of a group with 2 elements other than $\mathbb{Z}_2$, $\mathbb{Z}/2$. (Ideally, in math!)

Hint: try for "times" as the operation.