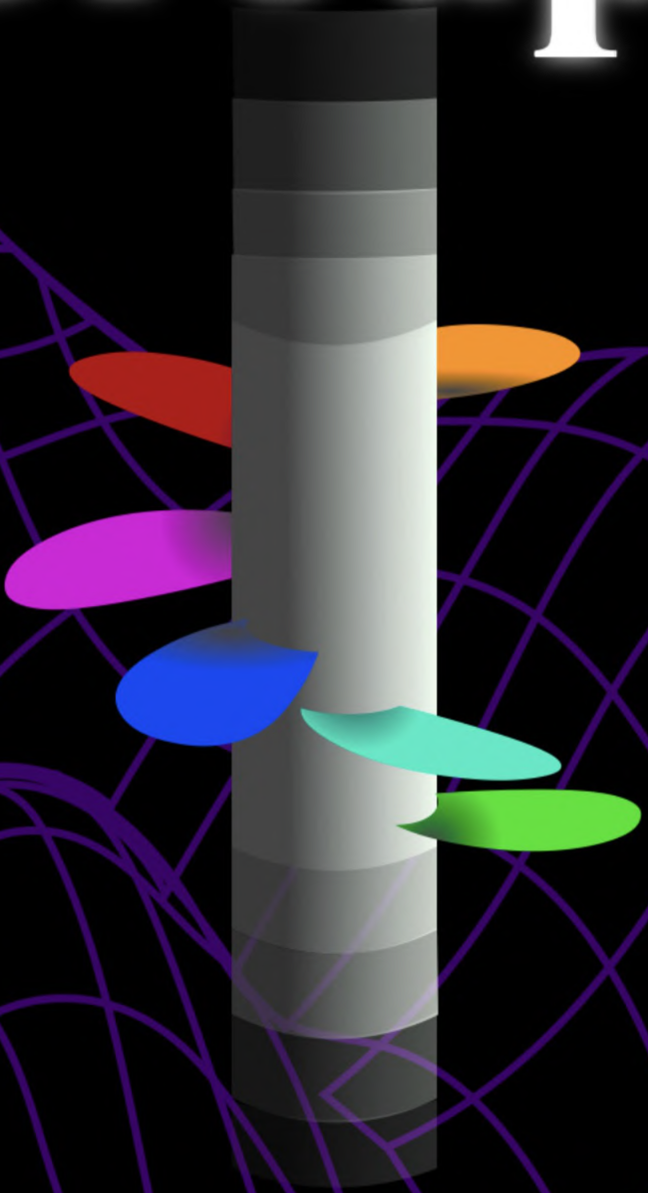
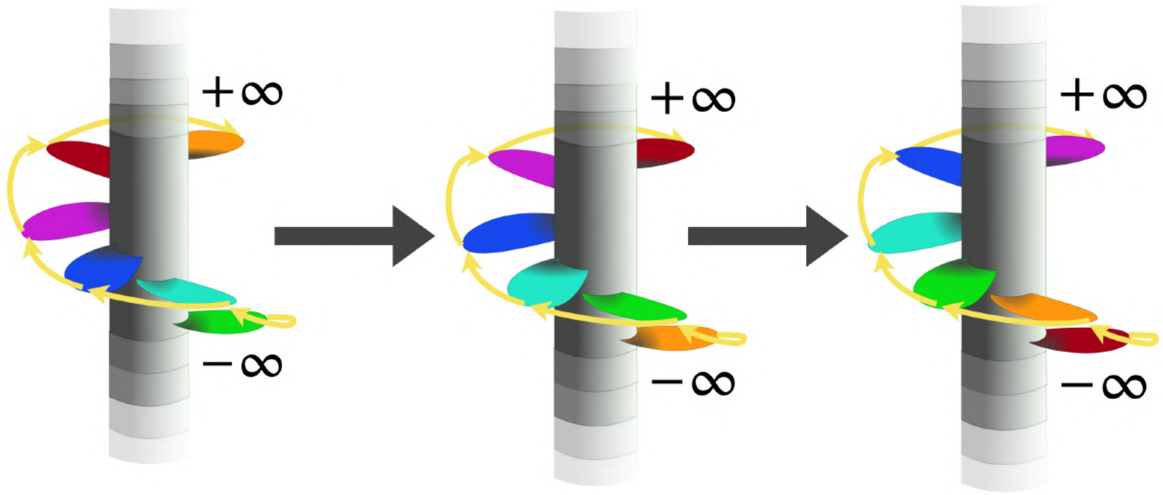
Cyclic Groups



The Best Way to Learn Group Theory

by DIBEOS

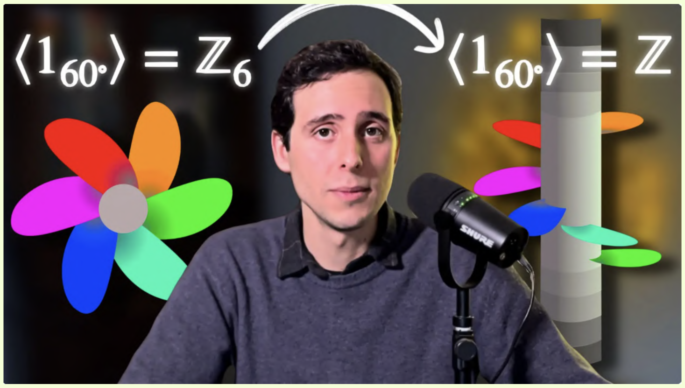


"Mathematics is the study of patterns." – **Lynn Steen**

If you want to support our work, please, consider becoming a **member** *of our YouTube channel! We'd like to keep our videos free of interruptions and sponsors, so that the sole focus is the subject at hand. But in order to do that we need your help. Thanks for supporting us. Also, members have free access to* **all of our PDFs***, including the full versions.*

Contents

This PDF is a deeper look at the material discussed in the following YouTube video:

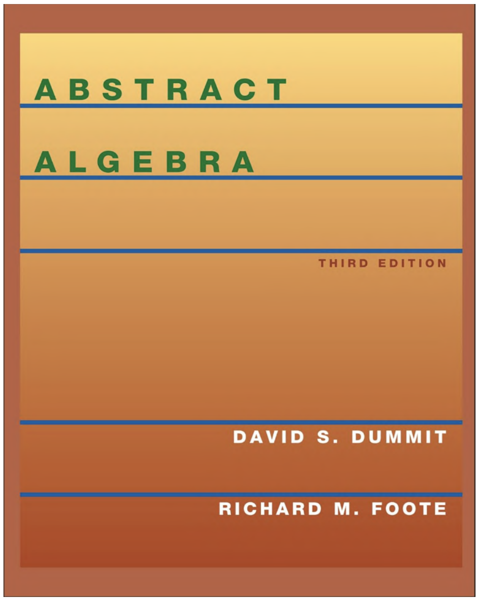

$\langle 1_{60^\circ} \rangle = \mathbb{Z}_6$
$\langle 1_{60^\circ} \rangle = \mathbb{Z}$
SHURE

The Best Way of Learning Group Theory.

We highly recommend watching the video first to get a basic understanding, and then reading this PDF.

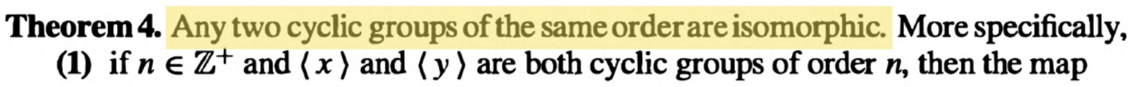
Introduction

"Abstract Algebra by Dummit & Foote" is one of the most recommended books on Abstract Algebra. I didn't study all of it, but based on the few pages I read, I can definitely say that it is complete and rigorous, but not easy to follow at all…



Let me explain what I mean.

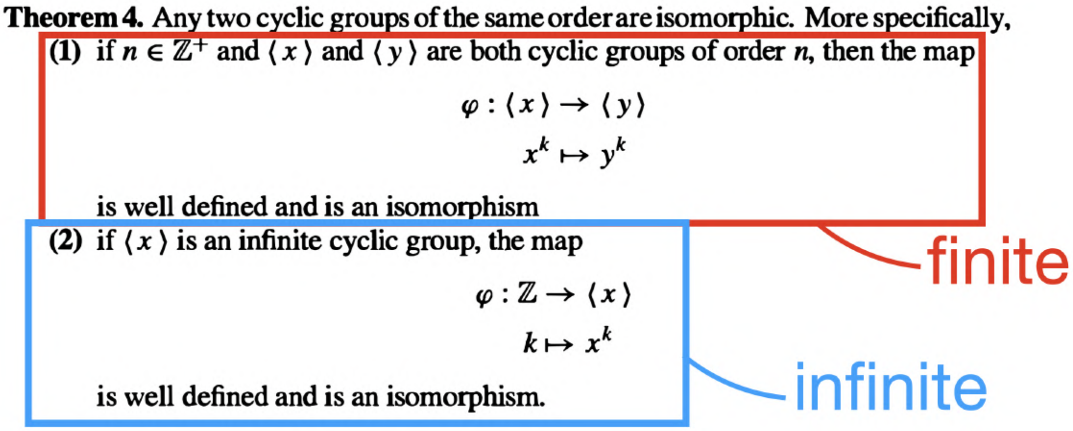
Theorem: Isomorphism of Cyclic Groups of the Same Order



Theorem 4. Any two cyclic groups of the same order are isomorphic. More specifically,

(1) if $n \in \mathbb{Z}^+$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n, then the map

If we go to page 56, for example, we will find *"Theorem 4: Any two cyclic groups of the same order are isomorphic."* And then they explain in more detail what this sentence means for *finite and infinite cyclic groups*.



Theorem 4. Any two cyclic groups of the same order are isomorphic. More specifically,

(1) if $n \in \mathbb{Z}^+$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n, then the map

$$\begin{aligned} \varphi : \langle x \rangle &\to \langle y \rangle \\ x^k &\mapsto y^k \end{aligned}$$

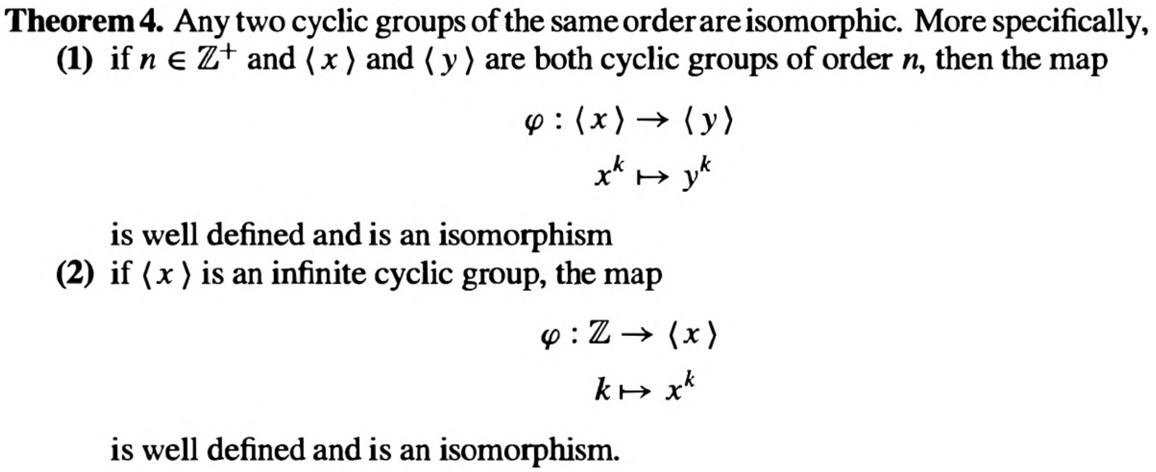
is well defined and is an isomorphism

(2) if $\langle x \rangle$ is an infinite cyclic group, the map

$$\begin{aligned} \varphi : \mathbb{Z} &\to \langle x \rangle \\ k &\mapsto x^k \end{aligned}$$

is well defined and is an isomorphism.

Please guys, tell me if it's just me: read it and let me know in the comments if you can fully understand it.



Theorem 4. Any two cyclic groups of the same order are isomorphic. More specifically,

(1) if $n \in \mathbb{Z}^+$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n, then the map

$$\begin{aligned} \varphi : \langle x \rangle &\to \langle y \rangle \\ x^k &\mapsto y^k \end{aligned}$$

is well defined and is an isomorphism

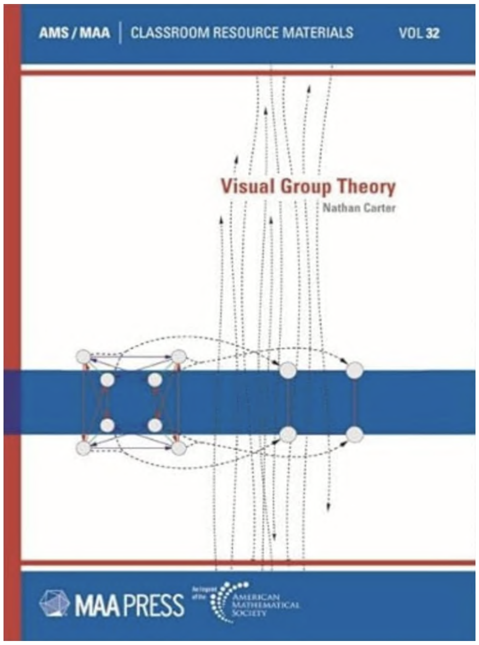
(2) if $\langle x \rangle$ is an infinite cyclic group, the map

$$\begin{aligned} \varphi : \mathbb{Z} &\to \langle x \rangle \\ k &\mapsto x^k \end{aligned}$$

is well defined and is an isomorphism.

Maybe you already studied Group Theory before, and this theorem seems obvious to you. But try to put yourself in the shoes of a beginner in the subject. Sure, with perseverance you can understand it, but my question is: *"Isn't there a better way. . . ?"*.

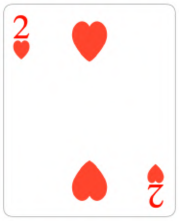
Well, I'm a huge fan of the book "Visual Group Theory by Nathan Carter". In this book (below), you will get exactly what the title promises, and it will really help anyone wanting to learn group theory, including this very theorem we just saw. Of course, it is not as rigorous as "Dummit & Foote", but for a person who's still in the stage of building intuition, it is perfect!

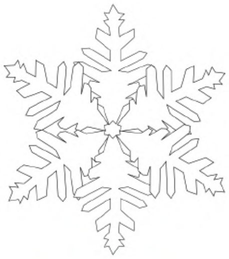

AMS / MAA | CLASSROOM RESOURCE MATERIALS VOL 32
Visual Group Theory
Nathan Carter
MAA PRESS
AMERICAN MATHEMATICAL SOCIETY

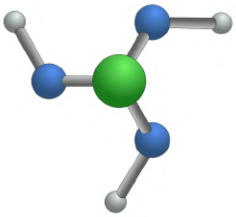
Let's study this theorem using the same style!

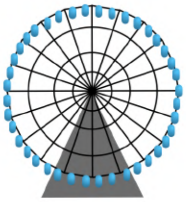
Visualizing Finite Cyclic Groups

There are so many objects that have cyclic symmetry, and therefore can be modeled by cyclic groups.

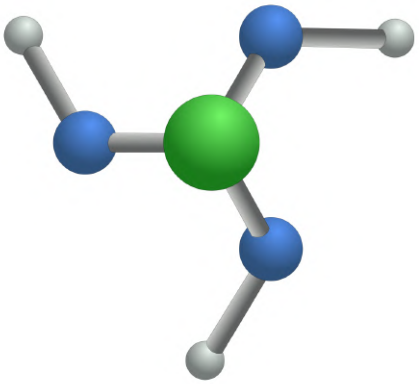






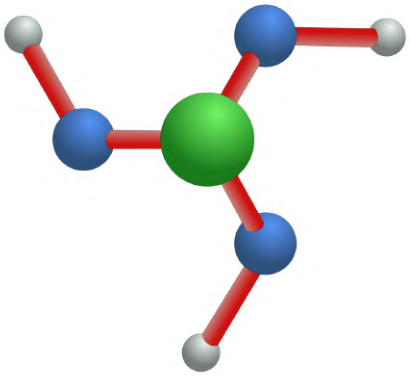


Imagine this molecule of boric acid (below), for example.



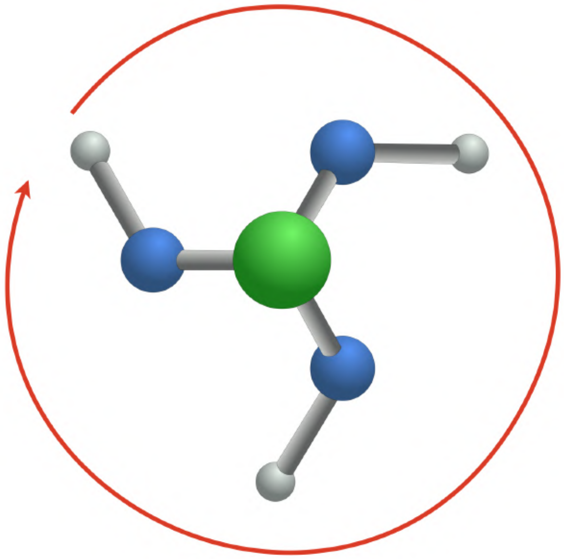
Boric acid

It has 3 sort of symmetric branches.

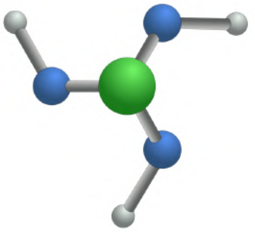


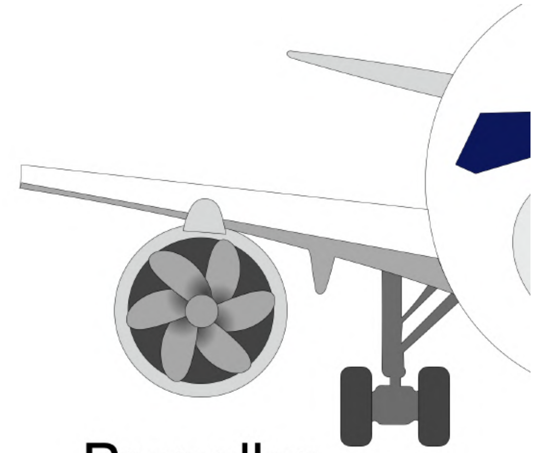
Boric acid

Every full rotation brings you back to the start.

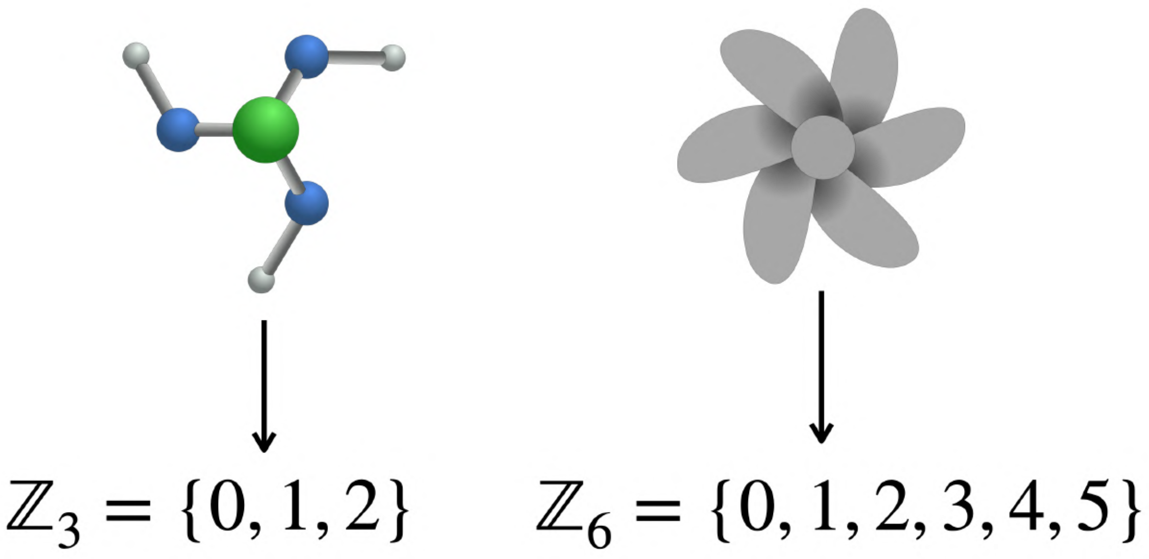


The same is true for this propeller (below), but this time it has 6 symmetric configurations.

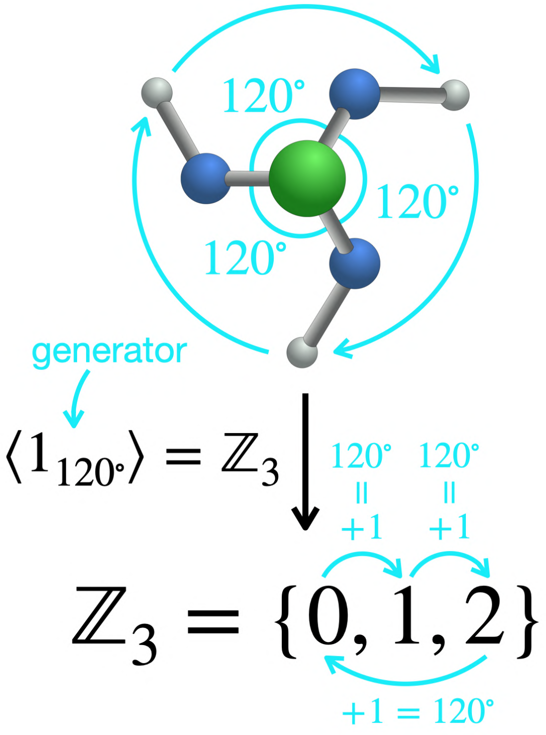




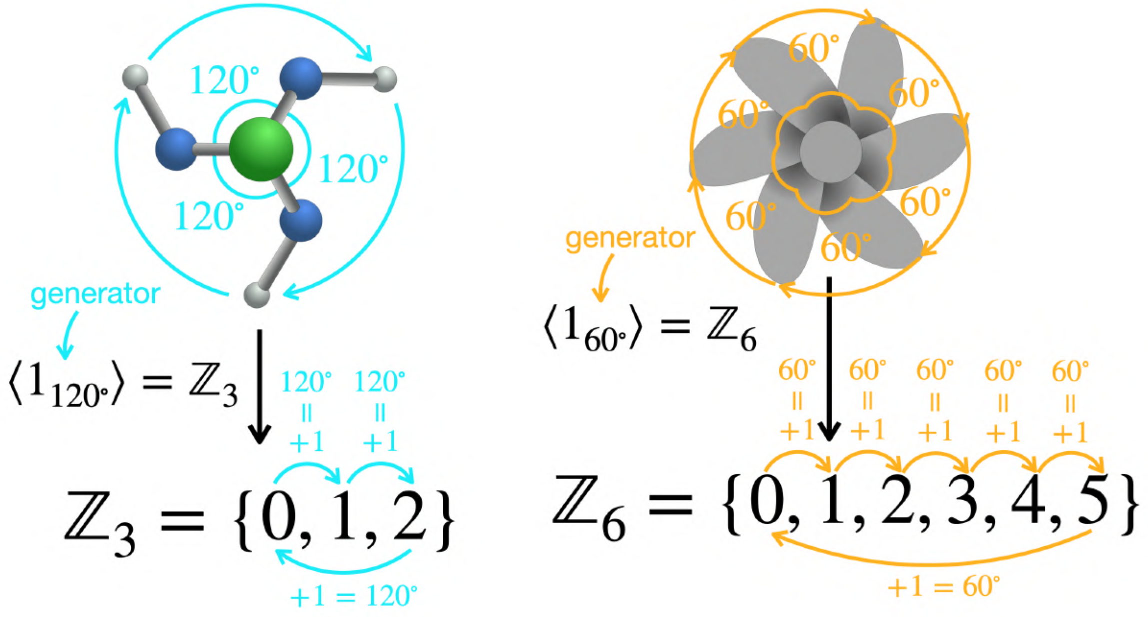
We say that the molecule can be modeled by the cyclic group $\mathbb{Z}_3$, and that the propeller by the cyclic group $\mathbb{Z}_6$.


$\mathbb{Z}_3 = \{0, 1, 2\}$
$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

For the molecule, the group operation is addition modulo 3. Adding 1 means rotating it by 120°. We say that the element 1 is the generator of this group, and we'll represent it here as this:


120°
120°
120°
generator
$\langle 1_{120°} \rangle = \mathbb{Z}_3$
120°
=
+1
120°
=
+1
$\mathbb{Z}_3 = \{0, 1, 2\}$
+1 = 120°

For the propeller, we have a similar situation, but this time the generator is a 60°-rotation:

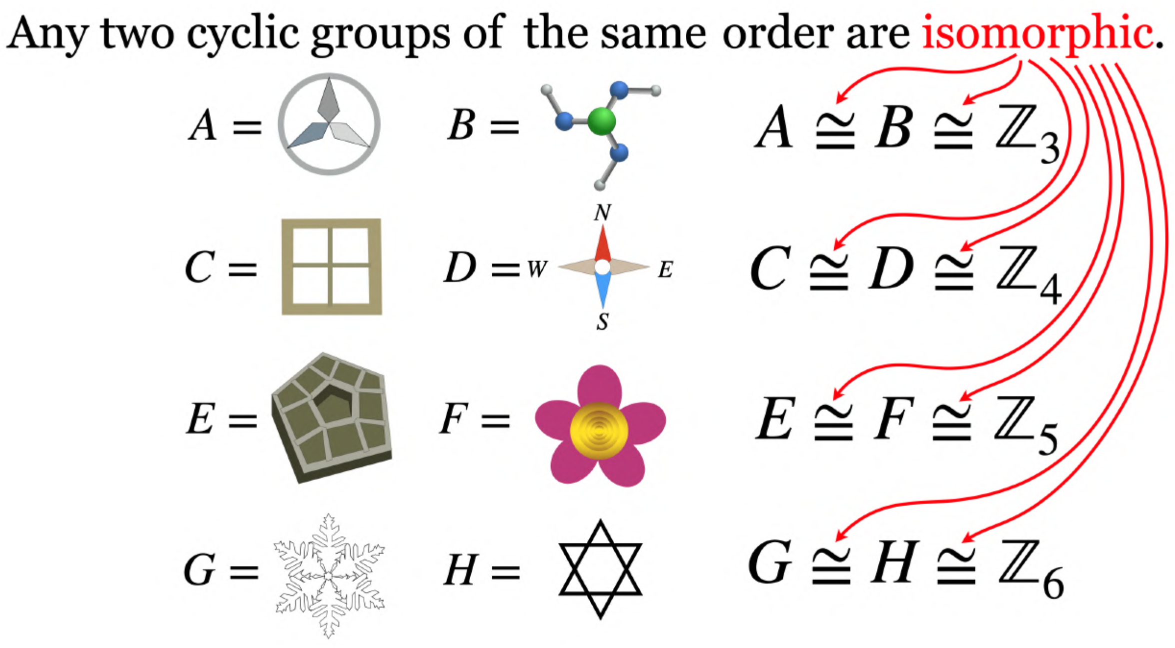

120°
120°
120°
generator
$\langle 1_{120^\circ} \rangle = \mathbb{Z}_3$
120° = +1
120° = +1
$\mathbb{Z}_3 = \{0, 1, 2\}$
+1 = 120°
60°
60°
60°
60°
60°
60°
generator
$\langle 1_{60^\circ} \rangle = \mathbb{Z}_6$
60° = +1
60° = +1
60° = +1
60° = +1
60° = +1
$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$
+1 = 60°

(take your time to ”digest” what is being represented in the image above)

So, essentially, that’s what the theorem says:

Any two cyclic groups of the same order are isomorphic.

Before we see what isomorphic means here, check out these examples of isomorphic cyclic groups:

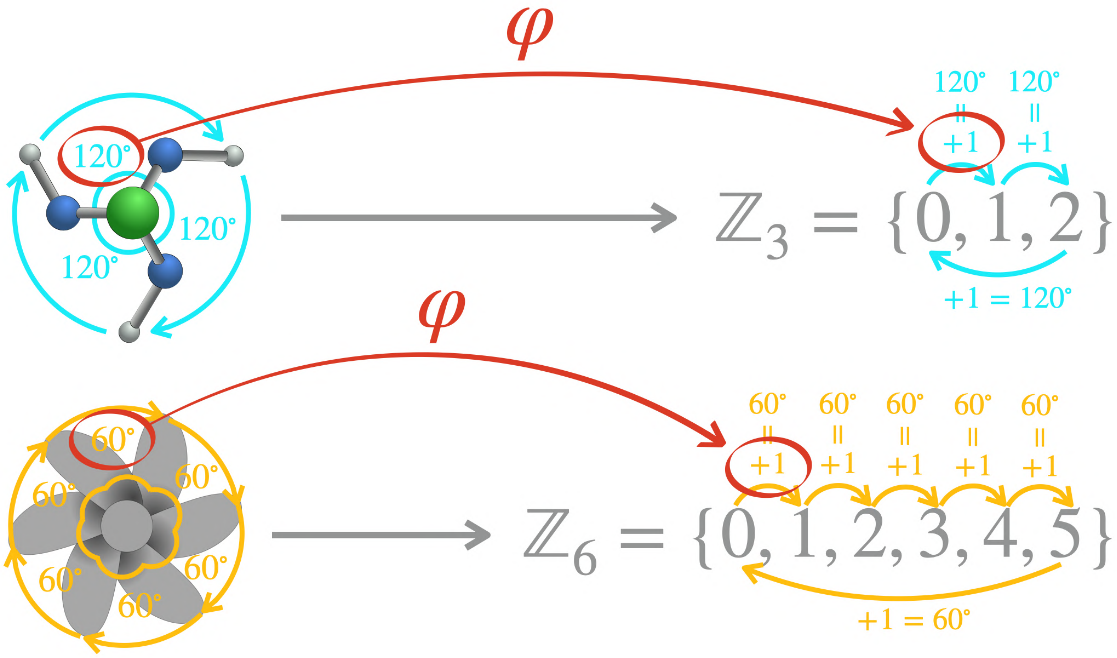

Any two cyclic groups of the same order are isomorphic.
$A =$
$B =$
$A \cong B \cong \mathbb{Z}_3$
$C =$
$D =$
N
W
E
S
$C \cong D \cong \mathbb{Z}_4$
$E =$
$F =$
$E \cong F \cong \mathbb{Z}_5$
$G =$
$H =$
$G \cong H \cong \mathbb{Z}_6$

Isomorphic means two things:

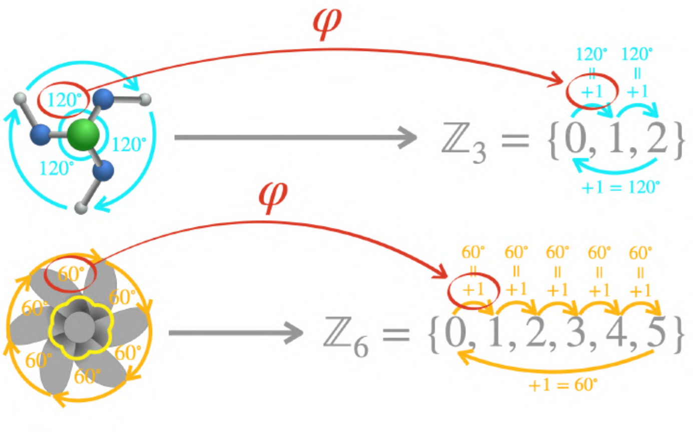
1. The mapping φ is *operation-preserving*. It associates each $120°$-rotation to a $+1$ addition in $\mathbb{Z}_3$. And it associates each $60°$-rotation to a $+1$ addition in $\mathbb{Z}_6$.

isomorphic

1) φ is operation preserving



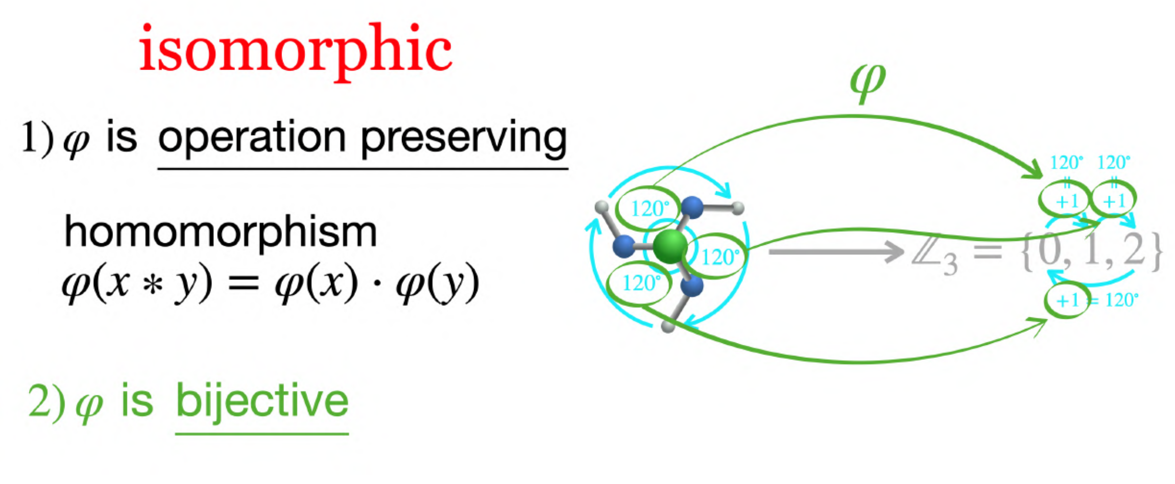
There is a fancy name for mappings that preserve operations between groups: **homomorphism**.



homomorphism

$$\varphi(x * y) = \varphi(x) \cdot \varphi(y)$$

2. The mapping φ is *bijective*. It associates one element of the first group to one element of the second group in a unique way (:= injective).



isomorphic

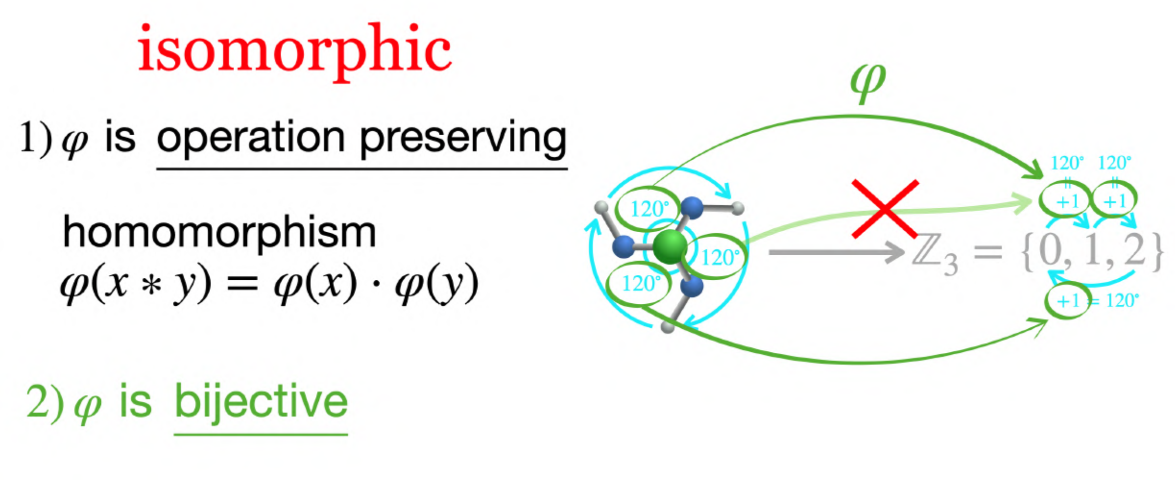
1) φ is operation preserving

homomorphism

$\varphi(x * y) = \varphi(x) \cdot \varphi(y)$

2) φ is bijective

So, this (below) cannot happen.



isomorphic

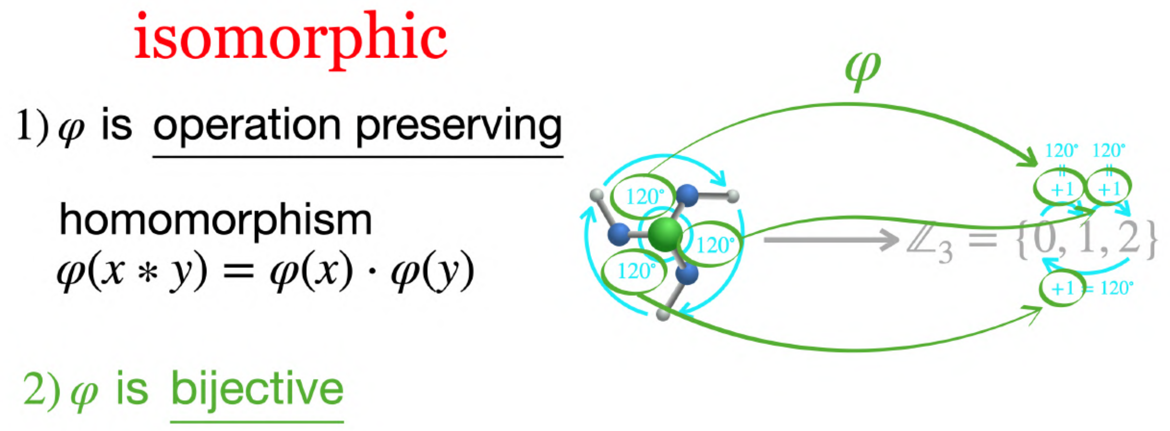
1) φ is operation preserving

homomorphism

$\varphi(x * y) = \varphi(x) \cdot \varphi(y)$

2) φ is bijective

And also, the map φ covers the entire target group, such that no element is left out (:= surjective).



isomorphic

1) φ is operation preserving

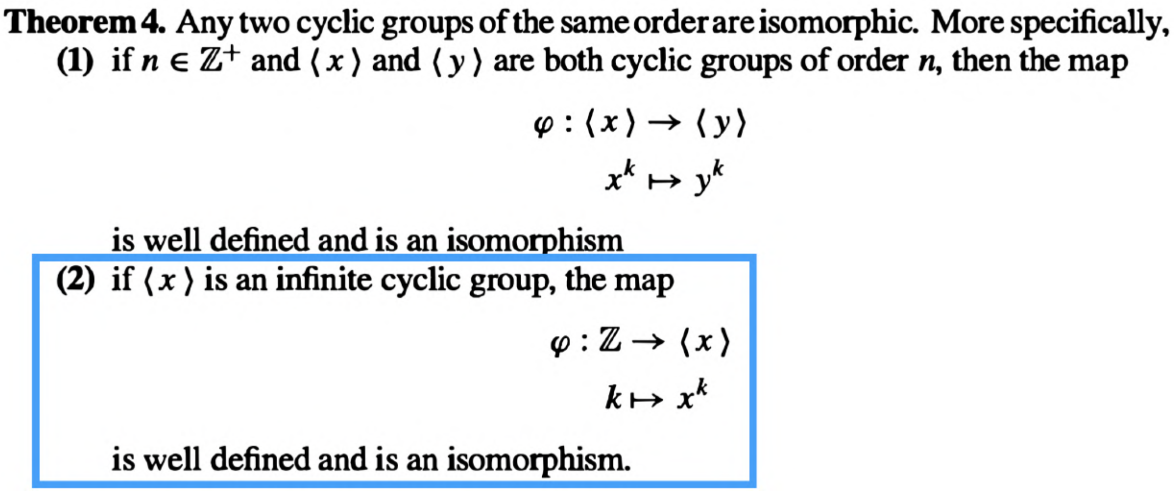
homomorphism
$\varphi(x * y) = \varphi(x) \cdot \varphi(y)$

2) φ is bijective

Great! That's the first part of the theorem! I think it is pretty easy to understand this way, right?!

If you want to have access to the FULL-PDF version, click on this link. We added a few exercises at the end (with the detailed solutions) and extra explanations throughout it. Also, I remind you guys that we provide the FULL-PDF version for free for all members of the channel. Just join us on YouTube! We'd like to keep our videos free of interruptions and sponsors, so that the sole focus is the subject at hand. But in order to do that we need your help. Thanks for supporting our work.

But what about the second part?



Theorem 4. Any two cyclic groups of the same order are isomorphic. More specifically,

(1) if $n \in \mathbb{Z}^+$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n, then the map

$$\begin{aligned} \varphi : \langle x \rangle &\to \langle y \rangle \\ x^k &\mapsto y^k \end{aligned}$$

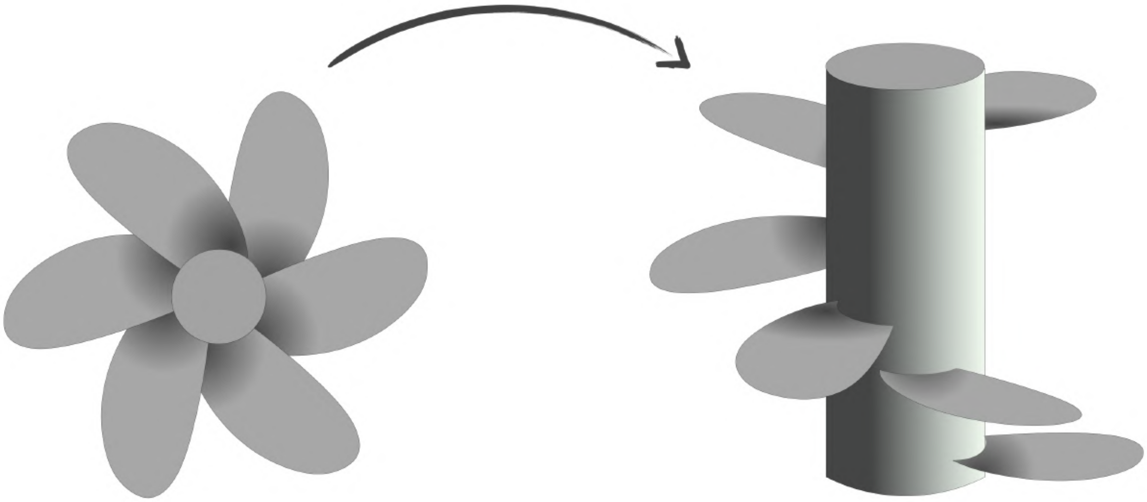
is well defined and is an isomorphism

(2) if $\langle x \rangle$ is an infinite cyclic group, the map

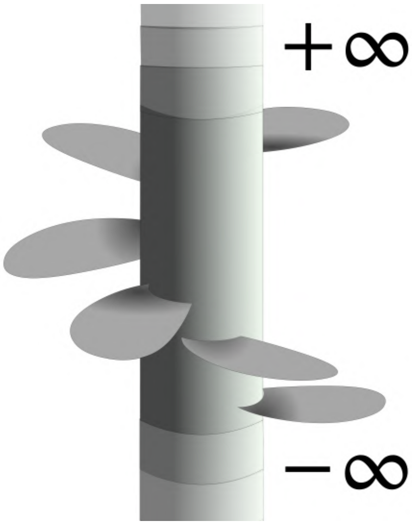
$$\begin{aligned} \varphi : \mathbb{Z} &\to \langle x \rangle \\ k &\mapsto x^k \end{aligned}$$

is well defined and is an isomorphism.

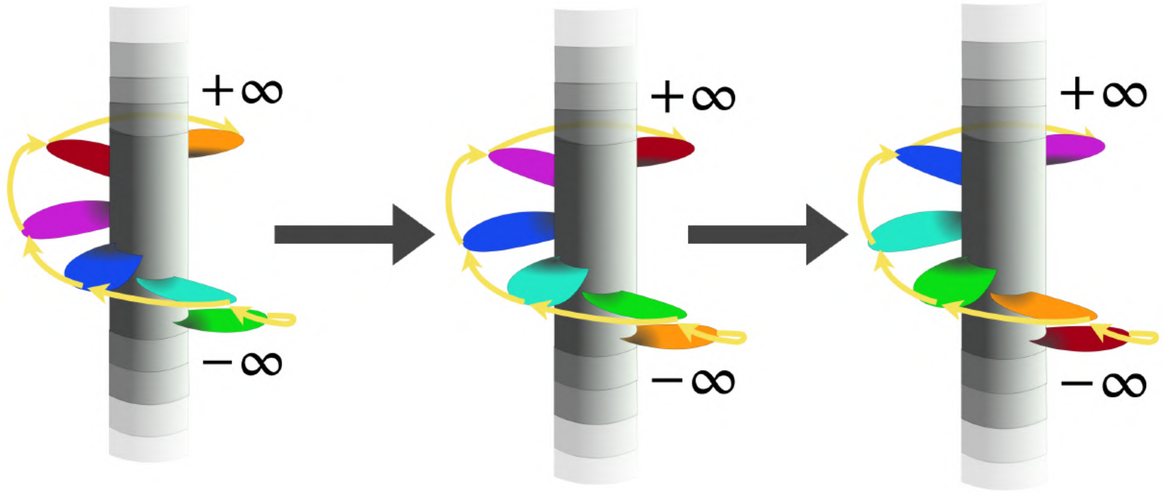
Visualizing Infinite Cyclic Groups



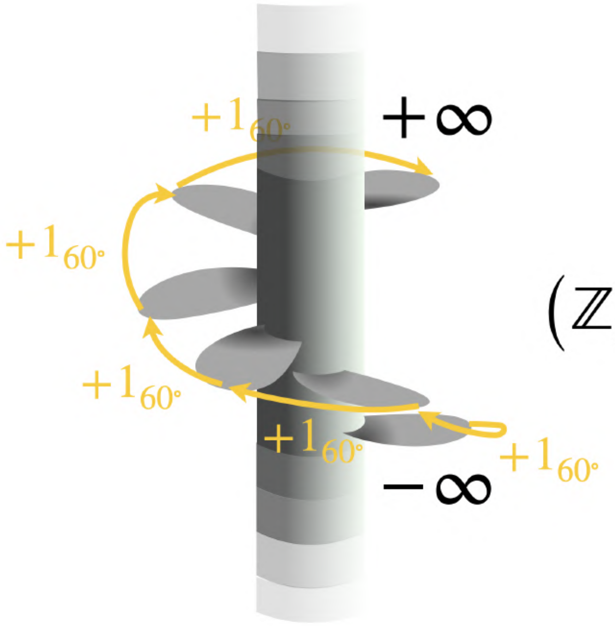
Well, let's take the example of our propeller once again. But this time, we find out that we were actually observing it from the top. And when we add this third dimension to it, we notice that it was a helical propeller all along, such that it extends infinitely upward and downward.



The generator of this new group is still 1_{60°, but this time each blade, after this action, never returns to the same initial position. It's still a cyclic group, though, because every element of the group can be reached by repeatedly applying the generator $+1_{60^\circ}$ (or its inverse -1_{60°).

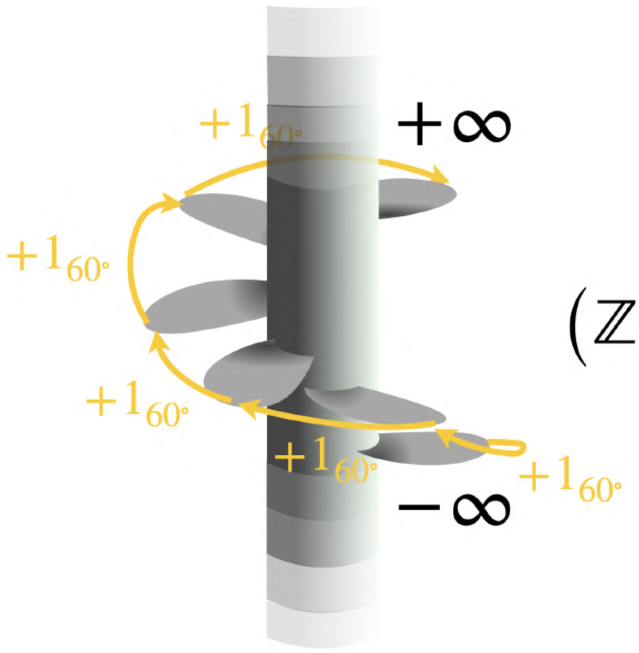


But now, its order (i.e. the number of elements in the group) is infinite:



$$(\mathbb{Z}_n, +) \rightsquigarrow \cancel{(\mathbb{Z}_\infty, +)}$$

We don't write it this way, though. This is, actually, just the set of integers $\mathbb{Z}$ with the addition operation.

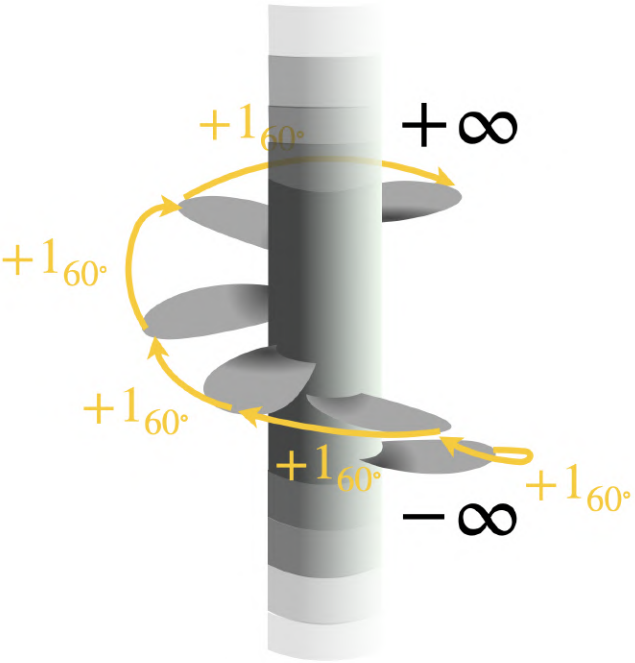


$$(\mathbb{Z}_n,+) \rightsquigarrow (\mathbb{Z},+)$$

✓

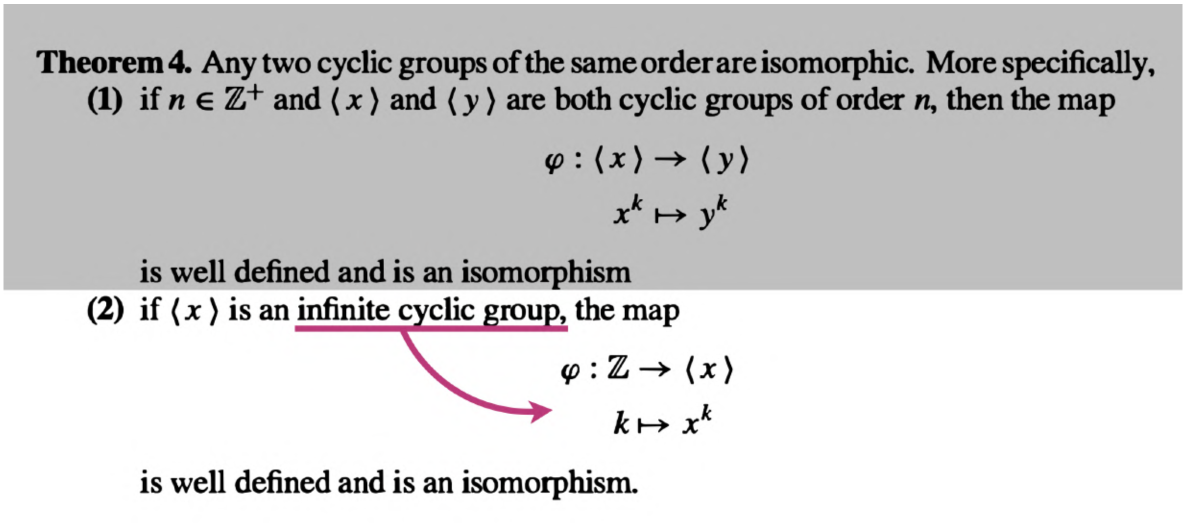
And therefore, this is the infinite cyclic group of integers under addition:

$$\langle 1_{60^\circ} \rangle = \mathbb{Z}$$



That’s what part 2 of the theorem says:

Every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$



Theorem 4. Any two cyclic groups of the same order are isomorphic. More specifically,

(1) if $n \in \mathbb{Z}^+$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n, then the map

$$\begin{aligned} \varphi : \langle x \rangle &\to \langle y \rangle \\ x^k &\mapsto y^k \end{aligned}$$

is well defined and is an isomorphism

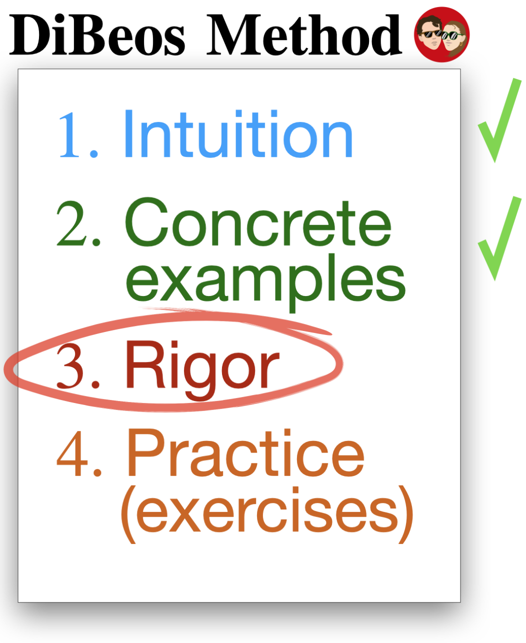
(2) if $\langle x \rangle$ is an infinite cyclic group, the map

$$\begin{aligned} \varphi : \mathbb{Z} &\to \langle x \rangle \\ k &\mapsto x^k \end{aligned}$$

is well defined and is an isomorphism.

Context & Proof of Homomorphism

Following our method to learn anything in advanced math and physics, we see that we already covered the intuition and concrete examples part of it:



DiBeos Method

1. Intuition ✓
2. Concrete examples ✓
3. Rigor
4. Practice (exercises)

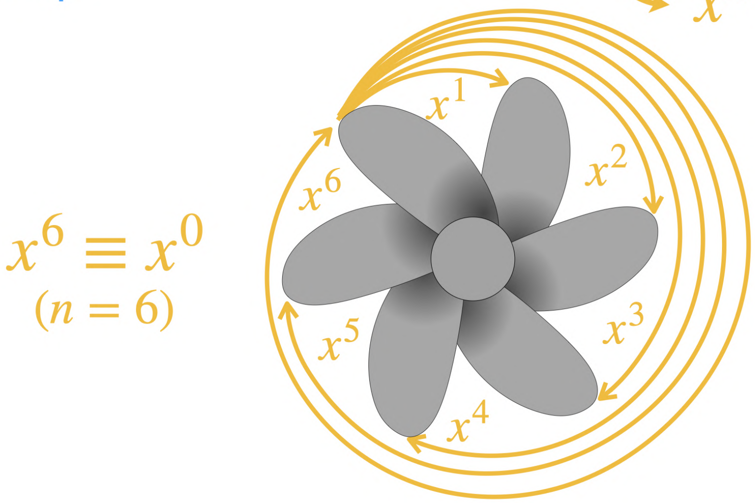
Now it is time to revisit the theorem, and study how to rigorously prove it.

Proof:

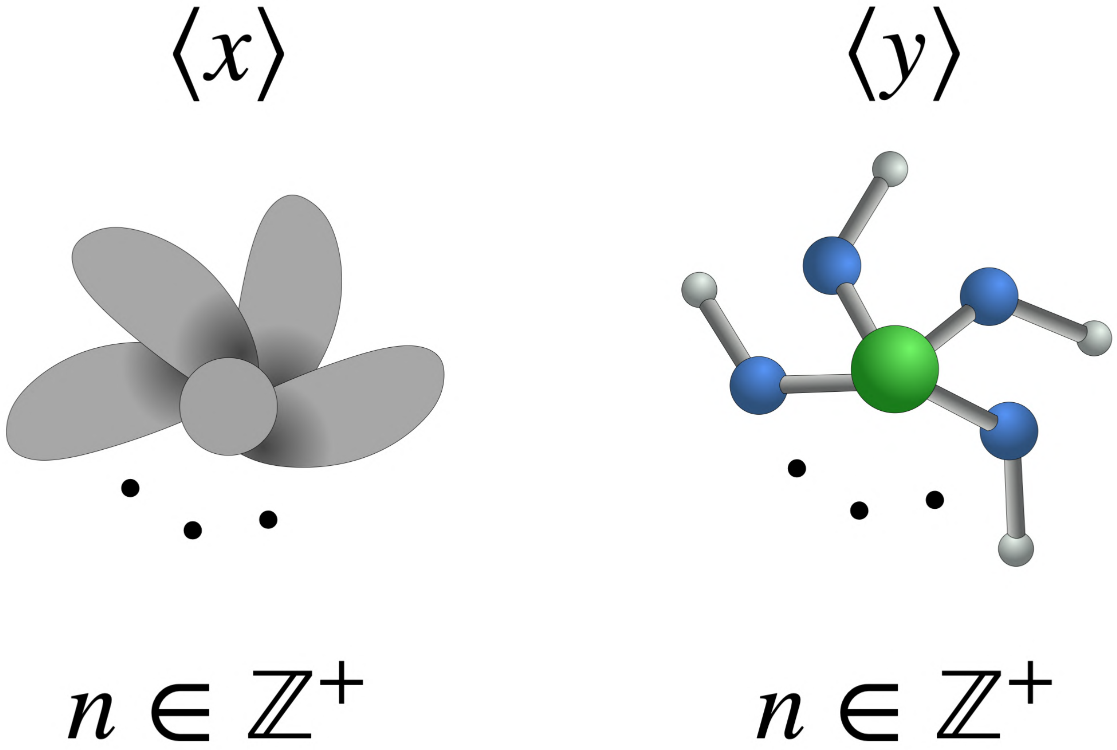
Let's start by recalling that $\langle\, x \,\rangle$ means that x is the generator of the group, and therefore that all other elements in the group can be reached by successively multiplying x as many times as necessary, say k times for example, with k being an integer (i.e. $x\,x\,x \ldots\, x = x^k$).

$$\overset{\text{generator}}{\underbrace{\langle x\rangle}_{\text{group}}} = \{x^0, x^1,\ \ldots\ \underbrace{x^k}, \ldots, x^{n-1}\}$$

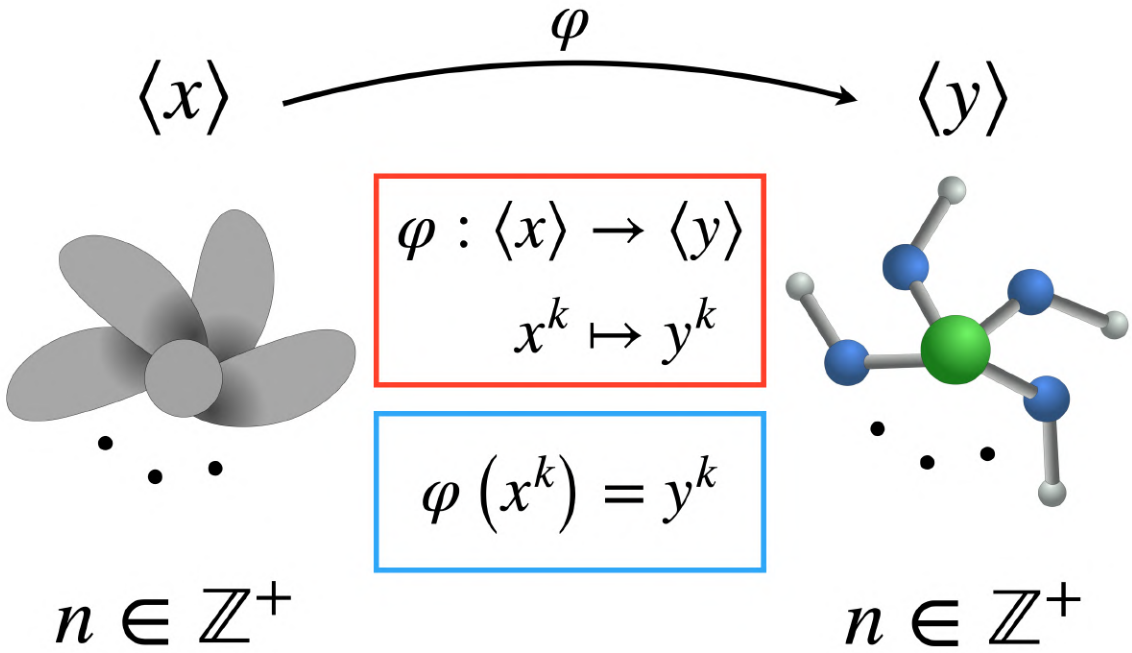
$$x^k = \underbrace{x \cdot x \cdot \ldots \cdot x}_{\text{k times}}$$



The order of both cyclic groups we're dealing with here is $n \in \mathbb{Z}^+$, which means that there are n unique elements in each group. Think of a propeller with n blades, or a molecule with n branches.

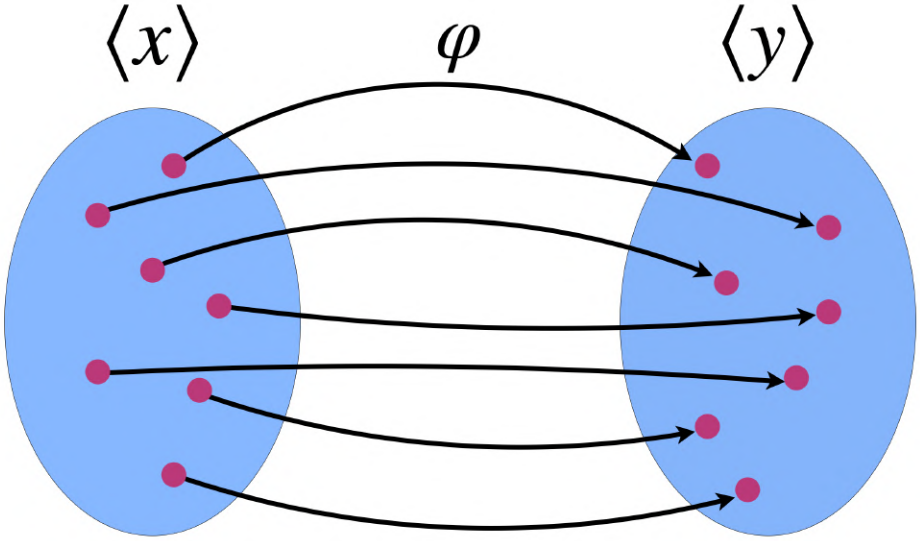


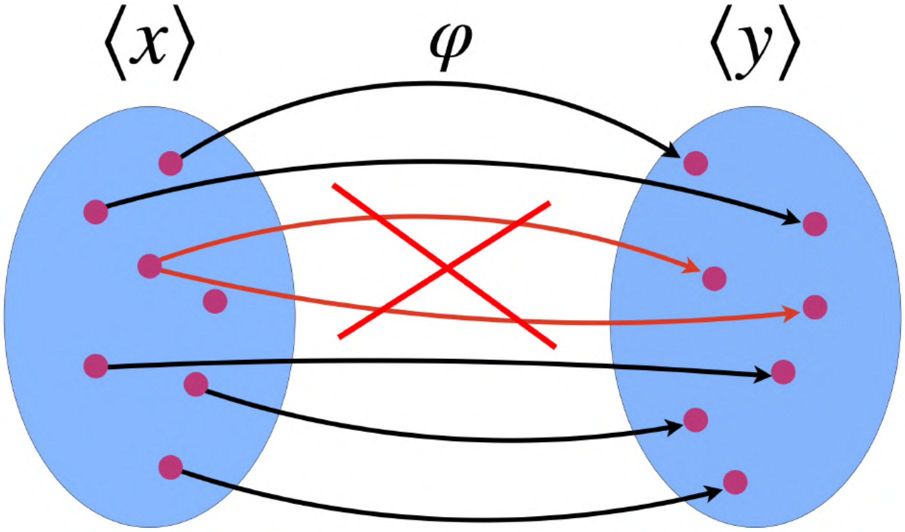
The map φ has an input x^k and an output y^k:



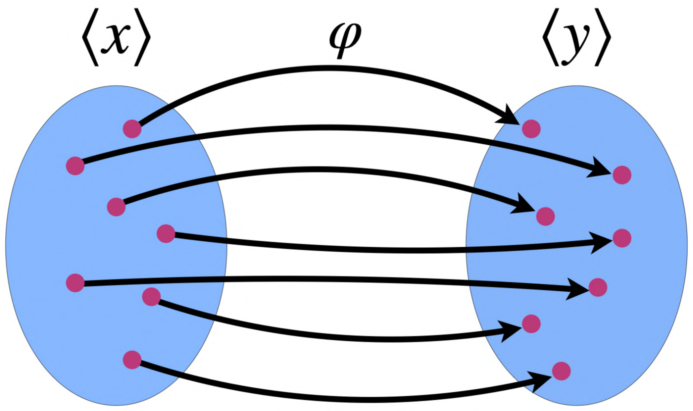
Our first goal is to prove that this mapping is **well defined**.

Now, this expression, *"well defined"* in mathematics, can be problematic sometimes, because it means different things for different contexts. In our case in particular, the map φ is well defined if it doesn't send the same element to two different elements.





Rigorously speaking, if $x^r = x^s$ (for some integers r and s), then $\varphi(x^r) = \varphi(x^s)$.



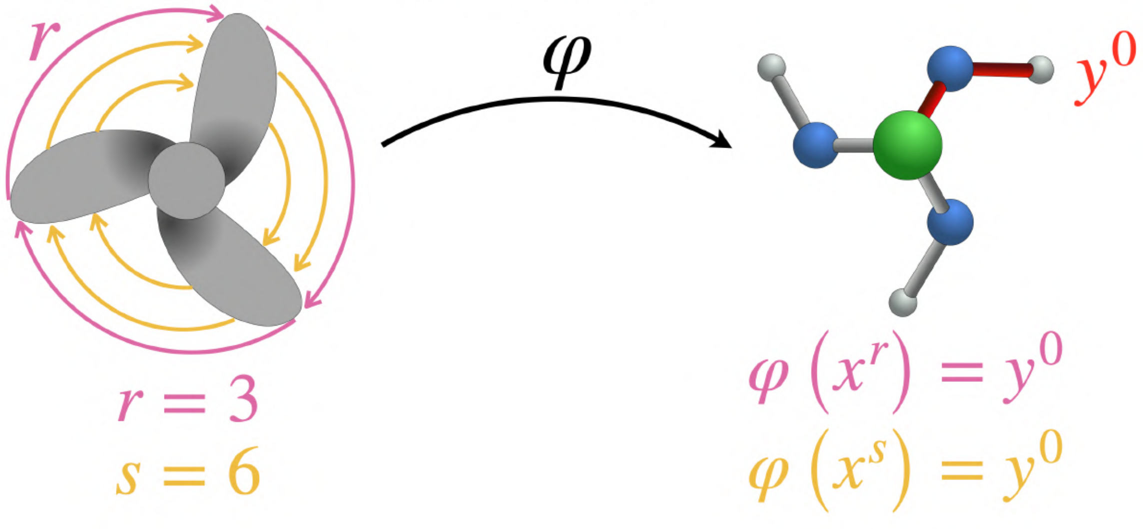
$$\boxed{\text{if } \; x^r = x^s, \;\; \text{then } \; \varphi\left(x^r\right) = \varphi\left(x^s\right)}$$

(well defined)

For example, if $r = 3$ here, and $s = 6$, then the mapping φ will translate both of them into the **“do nothing action”**, i.e y^0. The propeller spins and returns to the same initial position for 3 and for 6, which is equivalent to doing nothing with the boric acid molecule.

$$\boxed{\text{if } \; x^r = x^s, \;\; \text{then } \; \varphi\left(x^r\right) = \varphi\left(x^s\right)}$$

(well defined)


r
φ
y^0
$r = 3$
$s = 6$
$\varphi\left(x^r\right) = y^0$
$\varphi\left(x^s\right) = y^0$

So, let's prove it:

First write $x^r = x^s \implies x^r\, x^{-s} = 1 \implies \boxed{x^{r-s} \equiv 1}$ mod n, since n is the order (or size) of the group.

$$\boxed{\text{if } \ x^r = x^s, \ \text{ then } \ \varphi\left(x^r\right) = \varphi\left(x^s\right)}$$

(well defined)

$$x^r = x^s \implies x^r\, x^{-s} = 1 \implies \underset{\text{mod } n}{\boxed{x^{r-s} = 1}}$$

order (or size) of the group

If you know some modular arithmetic, you'll notice that this means that the exponent $r - s$ is divisible by n, or (which is equivalent), n divides $r - s$:

$$\boxed{\text{if } \ x^r = x^s, \ \text{ then } \ \varphi\left(x^r\right) = \varphi\left(x^s\right)} \quad \text{(well defined)}$$

$$\underset{\text{mod } n}{\boxed{x^{r-s} = 1}} \implies \frac{r-s}{n} \in \mathbb{Z} \implies n \mid r - s$$

"divides"

This implies that we can write $r - s$ as a multiple of n (for some $t \in \mathbb{Z}$):

$$\boxed{\text{if } \; x^r = x^s, \; \text{ then } \; \varphi\left(x^r\right) = \varphi\left(x^s\right)} \quad \text{(well defined)}$$

$$\underset{\text{mod } n}{\boxed{x^{r-s} = 1}} \Longrightarrow \frac{r-s}{n} \in \mathbb{Z} \Longrightarrow n \,\big|\, r-s \Longrightarrow$$

$$\Longrightarrow r - s = \underset{t \in \mathbb{Z}}{t}n \Longrightarrow r = tn + s$$

Finally, all we have to do is check what is after the **"then"** in our expression:

$$\boxed{\text{if } \; x^r = x^s, \; \text{ then } \; \underline{\varphi\left(x^r\right) = \varphi\left(x^s\right)}} \quad \text{(well defined)}$$

$$r = tn + s$$

$$\varphi\left(x^k\right) \overset{\text{def}}{=} y^k$$

$$\begin{aligned}
\varphi\left(x^r\right) &= \varphi\left(x^{tn+s}\right) \\
&= y^{tn+s} \\
&= y^{tn}\, y^s \\
&= \left(y^n\right)^t \, y^s \\
&= (1)^t \, y^t \\
&= 1 y^s \\
&= y^s \\
&= \varphi\left(x^s\right)
\end{aligned}$$

Therefore, the map φ is well defined.

But is it an isomorphism? Well, let's see:

CLICK HERE TO CONTINUE READING