Warm Up! Group Theory Practice

What operation is the set

$\{e^{ix} | 0 \leq x < 2\pi\}$ *closed under?*

What is the order of each element in

Z_{103}*?*

Let G *be a group. Let* H *and* K *be*

subgroups of G.

Is $H \cap K$ *a subgroup of* G*?*

What cyclic groups Z_n *have all of their*

elements with order $n - 1$*?*

Guided Discussion: Group Theory

Slide Components

Problems

Walter Johnson Math Team

Guided Discussion: Looking at Symmetry

Identity Transformation, I *returns the same value that was used in its argument*

Group Theory *is an area of algebra, which means it's a study of how combining objects can make new ones*

*****Group Theory gets a little looser with it's notation than you're used to. The product sign * is commonly used to denote an operation, not just multiplication. And sometimes, it's another operator denoting it.***

$$T = \{H, V, R, I\}$$

Let's fill it all out!

	I	**H**	**V**	**R**
I	I	H	V	R
H	H	I	R	V
V	V	R	I	H
R	R	V	H	I

$\cong$

	(0, 0)	**(1, 0)**	**(0, 1)**	**(1, 1)**
(0, 0)	(0, 0)	(1, 0)	(0, 1)	(1, 1)
(1, 0)	(1, 0)	(0, 0)	(1, 1)	(0, 1)
(0, 1)	(0, 1)	(1, 1)	(0, 0)	(1, 0)
(1, 1)	(1, 1)	(0, 1)	(1, 0)	(0, 0)

This is isomorphic to an addition table of ordered pairs $\bmod 2$

This special group we call the Klein Group

Guided Discussion: *Defining Groups*

There is a rule that maps every pair of elements from G to G

$$G \times G \rightarrow G$$

Or that "G cross G maps to G"

Known as being "closed" in *

Every element has an inverse, not particularly commutative

*We define a **Group** as a*

- *Set G, together with binary operation $*$*
- *Such that any for any two elements x* and *y* in *G, $x * y \in G$*
- *There is an identity element $e \in G$ such that for any element x in G,*
  $$e * x = x * e = x$$
- *For every element x in G, there is an inverse such that $x * x^{-1} = e$*
- *The operation is associative*
  $$(x * y) * z = x * (y * z)$$

Guided Discussion: *Types of Groups*

*A **Group** is set **G** with binary operation * that satisfies the following **4 axioms***

- ***G** is **Closed** in **
- $\boldsymbol{e} \in G$
- $\forall x \in G, \exists\, x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group,** $\boldsymbol{D_n}$ is a group corresponding to regular n-gon*

*A **Symmetric Group,** $\boldsymbol{S_n}$ are the permutations on $\mathbb{Z}/n\mathbb{Z}$*

*A **Cyclic Group,** $\boldsymbol{Z_n}$ is the group of modular addition* $\mathrm{mod}\ n$

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

There are three main important types of groups:

- *Dihedral Groups, D_n*
  - *Set of symmetries on a regular n-gon with composition as operation*
- *Symmetric Groups, S_n*
  - *Set of permutations on $\mathbb{Z}/n\mathbb{Z}$ with operation of composition*
- *Cyclic Groups*
  - *Set $\mathbb{Z}/n\mathbb{Z}$ itself, with addition as operation*

Guided Discussion:
Dihedral Groups

*A **Group** is set **G** with binary operation * that satisfies the following **4 axioms***

- ***G** is **Closed** in **
- $\boldsymbol{e} \in G$
- $\forall x \in G, \exists\, x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group, $\boldsymbol{D_n}$** is a group corresponding to regular n-gon*

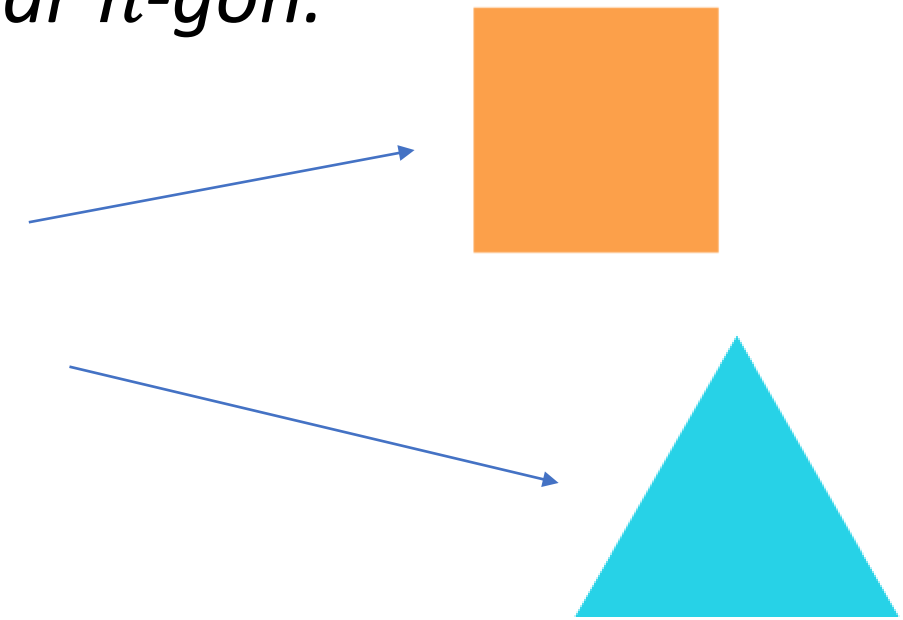
*A **Symmetric Group, $\boldsymbol{S_n}$** are the permutations on $\mathbb{Z}/n\mathbb{Z}$*

*A **Cyclic Group, $\boldsymbol{Z_n}$** is the group of modular addition mod n*

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Dihedral Groups, denoted D_n are the corresponding groups to a regular n-gon.

- D_4
- D_3



What is the size of D_n?

Guided Discussion:
Symmetric Groups

*A **Group** is set **G** with binary operation * that satisfies the following **4 axioms***

- ***G** is **Closed** in **
- $\boldsymbol{e} \in G$
- $\forall x \in G, \exists\, x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group,** $\boldsymbol{D_n}$ is a group corresponding to regular n-gon*

*A **Symmetric Group,** $\boldsymbol{S_n}$ are the permutations on $\mathbb{Z}/n\mathbb{Z}$*

*A **Cyclic Group,** $\boldsymbol{Z_n}$ is the group of modular addition* $\bmod n$

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Symmetric Groups, S_n, is the set of permutations on $\{0,1,2 \cdots n\}$, which is a bijective function from that set to itself. The operation is permutation composition

Consider group S_3 and element ϕ which maps 1 to 2, 2 to 3, and 3 to 1. This permutation, ϕ, is an element of S_3

Where does ϕ^2 map 3?

Guided Discussion: *Symmetric Groups*

*A **Group** is set $\boldsymbol{G}$ with binary operation $*$ that satisfies the following **4 axioms***

- *$\boldsymbol{G}$ is **Closed** in $*$*
- *$\boldsymbol{e} \in G$*
- *$\forall x \in G$, $\exists\, x^{-1}$ such that $x^{-1} * x = e$*
- ***Associative** $x * (y * z) = (x * y) * z$*

*A **Dihedral Group, $\boldsymbol{D_n}$** is a group corresponding to regular n-gon*

*A **Symmetric Group, $\boldsymbol{S_n}$** are the permutations on $\mathbb{Z}/n\mathbb{Z}$*

*A **Cyclic Group, $\boldsymbol{Z_n}$** is the group of modular addition $\bmod n$*

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Where does ϕ^2 map 3?

$$3 \to 1, 1 \to 2$$

So it maps $3 \to 2$

*****Note! The Symmetric Group itself does not contain 1,2…n. It instead contains all the possible permutations of that set***

Guided Discussion:
Cyclic Groups

*A **Group** is set **G** with binary operation * that satisfies the following **4 axioms***

- ***G** is **Closed** in **
- $\boldsymbol{e} \in G$
- $\forall x \in G, \exists\, x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group,** $\boldsymbol{D_n}$ is a group corresponding to regular n-gon*

*A **Symmetric Group,** $\boldsymbol{S_n}$ are the permutations on $\mathbb{Z}/n\mathbb{Z}$*

*A **Cyclic Group,** $\boldsymbol{Z_n}$ is the group of modular addition $\mathrm{mod}\ n$*

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Cyclic Groups, Z_n are, put simply, the group of modular addition $\mathrm{mod}\ n$.

The set is $\mathbb{Z}/n\mathbb{Z}$ and the operation is addition modulo n

For Z_4, for example:

$$\{0,1,2,3\}$$

And the operation is addition $\mathrm{mod}\ 4$

Guided Discussion: *Cyclic Groups*

*A **Group** is set $\boldsymbol{G}$ with binary operation $*$ that satisfies the following **4 axioms***

- $\boldsymbol{G}$ is ***Closed*** in $*$
- $\boldsymbol{e} \in G$
- $\forall x \in G, \exists\, x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group, $\boldsymbol{D_n}$** is a group corresponding to regular n-gon*

*A **Symmetric Group, $\boldsymbol{S_n}$** are the permutations on $\mathbb{Z}/n\mathbb{Z}$*

*A **Cyclic Group, $\boldsymbol{Z_n}$** is the group of modular addition $\bmod n$*

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

It's worth noting that Z_n is also the set of rotations of an n-gon

Then what's the difference between Z_n and S_n?

Guided Discussion: *Cyclic Groups*

*A **Group** is set **G** with binary operation * that satisfies the following **4 axioms***

- ***G** is **Closed** in **
- $\boldsymbol{e} \in G$
- $\forall x \in G, \exists\, x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group, $\boldsymbol{D_n}$** is a group corresponding to regular n-gon*

*A **Symmetric Group, $\boldsymbol{S_n}$** are the permutations on $\mathbb{Z}/n\mathbb{Z}$*

*A **Cyclic Group, $\boldsymbol{Z_n}$** is the group of modular addition $\bmod n$*

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

It's worth noting that Z_n is also the set of rotations of an n-gon

Then what's the difference between Z_n and S_n?

*S_n is the set of permutations **on** $\mathbb{Z}/n\mathbb{Z}$, wheras $\mathbb{Z}_n$ is the set itself*

***This really stumped us last week!*

Guided Discussion:
Filling Some Gaps

*A **Group** is set **G** with binary operation * that satisfies the following **4 axioms***

- ***G** is **Closed** in **
- $e \in G$
- $\forall x \in G, \exists\, x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group,** $\boldsymbol{D_n}$ is a group corresponding to regular n-gon*

*A **Symmetric Group,** $\boldsymbol{S_n}$ are the permutations on* $\mathbb{Z}/n\mathbb{Z}$

*A **Cyclic Group,** $\boldsymbol{Z_n}$ is the group of modular addition* $\mathrm{mod}\ n$

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

*Let G be a group. A subset $H \subseteq G$ is a **subgroup** if it forms a group under the same operation already defined in G*

*Not every subset of a group can be a group itself, you need to check and see if there is still **closure** and if every element has an **inverse***

Guided Discussion: Order

*A **Group** is set **G** with binary operation * that satisfies the following **4 axioms***

- ***G** is **Closed** in **
- $e \in G$
- $\forall x \in G, \exists\ x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group,*** $\boldsymbol{D_n}$ *is a group corresponding to regular* n*-gon*

*A **Symmetric Group,*** $\boldsymbol{S_n}$ *are the permutations on* $\mathbb{Z}/n\mathbb{Z}$

*A **Cyclic Group,*** $\boldsymbol{Z_n}$ *is the group of modular addition* $\mathrm{mod}\ n$

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Let G *be a group, and let* $g \in G$*. Suppose there is some positive integer* k *for which*

$$g^k = e$$

Then, there must be an infinite amount of such integers.

Why?

Guided Discussion: Order

*A **Group** is set $\boldsymbol{G}$ with binary operation * that satisfies the following **4 axioms***

- ***$\boldsymbol{G}$ is Closed** in **
- $\boldsymbol{e} \in G$
- $\forall x \in G, \exists\, x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group, $\boldsymbol{D_n}$** is a group corresponding to regular n-gon*

*A **Symmetric Group, $\boldsymbol{S_n}$** are the permutations on $\mathbb{Z}/n\mathbb{Z}$*

*A **Cyclic Group, $\boldsymbol{Z_n}$** is the group of modular addition mod n*

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Let G be a group, and let $g \in G$. Suppose there is some positive integer k for which

$$g^k = e$$

Because

$$g^k g^k = g^{2k} = e$$

And thus all integer multiples of k also satisfy.

We say the order of $\boldsymbol{g}$ is the smallest such integer

Guided Discussion: Order

*A **Group** is set $\boldsymbol{G}$ with binary operation $*$ that satisfies the following **4 axioms***

- ***G is Closed** in $*$*
- $\boldsymbol{e} \in G$
- $\forall x \in G, \exists\, x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group, $\boldsymbol{D_n}$** is a group corresponding to regular n-gon*

*A **Symmetric Group, $\boldsymbol{S_n}$** are the permutations on $\mathbb{Z}/n\mathbb{Z}$*

*A **Cyclic Group, $\boldsymbol{Z_n}$** is the group of modular addition mod n*

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

We say the order of $\boldsymbol{g}$ is the smallest such integer.

What if there is no positive integer k such that $g^k = e$?

Then we say that g has infinite order. Some examples of this are the number 4 and the group defined by $\mathbb{Z}$ and addition. You can keep adding 4 to itself, but you will never get to the identity, 0.

Guided Discussion: *"Trivial Element"*

*A **Group** is set $\boldsymbol{G}$ with binary operation $*$ that satisfies the following **4 axioms***

- ***$\boldsymbol{G}$ is Closed** in $*$*
- $\boldsymbol{e} \in G$
- $\forall x \in G, \exists\, x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group, $\boldsymbol{D_n}$** is a group corresponding to regular n-gon*

*A **Symmetric Group, $\boldsymbol{S_n}$** are the permutations on $\mathbb{Z}/n\mathbb{Z}$*

*A **Cyclic Group, $\boldsymbol{Z_n}$** is the group of modular addition* $\mathrm{mod}\ n$

***Order** of $g \in G$ is smallest such integer such that* $g^k = e$

We may refer to the identity element as the trivial element.

*Much more often, we will refer to elements which aren't the identity element as **nontrivial elements***

Examining the order of nontrivial elements is a big part of isomorphisms.

Guided Discussion: Isomorphisms

*A **Group** is set $\boldsymbol{G}$ with binary operation $*$ that satisfies the following **4 axioms***

- ***$\boldsymbol{G}$** is **Closed** in $*$*
- $\boldsymbol{e} \in G$
- $\forall x \in G, \exists\, x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group, $\boldsymbol{D_n}$** is a group corresponding to regular n-gon*

*A **Symmetric Group, $\boldsymbol{S_n}$** are the permutations on $\mathbb{Z}/n\mathbb{Z}$*

*A **Cyclic Group, $\boldsymbol{Z_n}$** is the group of modular addition $mod\ n$*

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

An Isomorphism between two groups is a bijective map preserving group operations.

Essentially, the groups are the same.

Guided Discussion: Isomorphisms

*A **Group** is set $\boldsymbol{G}$ with binary operation $*$ that satisfies the following **4 axioms***

- ***$\boldsymbol{G}$ is Closed** in $*$*
- *$\boldsymbol{e} \in G$*
- *$\forall x \in G, \exists\, x^{-1}$ such that $x^{-1} * x = e$*
- ***Associative** $x * (y * z) = (x * y) * z$*

*A **Dihedral Group, $\boldsymbol{D_n}$** is a group corresponding to regular n-gon*

*A **Symmetric Group, $\boldsymbol{S_n}$** are the permutations on $\mathbb{Z}/n\mathbb{Z}$*

*A **Cyclic Group, $\boldsymbol{Z_n}$** is the group of modular addition $\mathrm{mod}\ n$*

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

We can determine if two groups are isomorphic by looking at if there elements behave the same way, if there are the same number of elements, if the elements have the same order as those in the other group, and seeing if there is a bijection.

Guided Discussion: Isomorphisms

*A **Group** is set $\boldsymbol{G}$ with binary operation $*$ that satisfies the following **4 axioms***

- ***G is Closed** in $*$*
- $\boldsymbol{e} \in G$
- $\forall x \in G, \exists\, x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group, $\boldsymbol{D_n}$** is a group corresponding to regular n-gon*

*A **Symmetric Group, $\boldsymbol{S_n}$** are the permutations on $\mathbb{Z}/n\mathbb{Z}$*

*A **Cyclic Group, $\boldsymbol{Z_n}$** is the group of modular addition $\mathrm{mod}\ n$*

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Looking back, we saw that the group of symmetries on the letter I is isomorphic to the group of pairs of integers $\mathrm{mod}\ 2$ and the operation addition.

This underlying structure between these two is called the Klein Group. Both groups previously examined are isomorphic to the Klein Group.

Guided Discussion: *Cartesian Product*

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- ***G** is **Closed** in ******
- $\boldsymbol{e} \in G$
- $\forall x \in G, \exists\, x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group, $\boldsymbol{D_n}$** is a group corresponding to regular n-gon*

*A **Symmetric Group, $\boldsymbol{S_n}$** are the permutations on $\mathbb{Z}/n\mathbb{Z}$*

*A **Cyclic Group, $\boldsymbol{Z_n}$** is the group of modular addition* $\mathrm{mod}\ n$

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Order** of group **G** is the amount of elements in **G

The cartesian product of two sets

$$S_1 \times S_2$$

Is the set of ordered pairs where the first element comes from S_1 and the second comes from S_2

Guided Discussion: Cartesian Product

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- ***G** is **Closed** in ******
- $\boldsymbol{e} \in G$
- $\forall x \in G, \exists\, x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group, $\boldsymbol{D_n}$** is a group corresponding to regular n-gon*

*A **Symmetric Group, $\boldsymbol{S_n}$** are the permutations on $\mathbb{Z}/n\mathbb{Z}$*

*A **Cyclic Group, $\boldsymbol{Z_n}$** is the group of modular addition $\mathrm{mod}\ n$*

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Order** of group **G** is the amount of elements in **G

$$S_1 \times S_2 = \{(x, y) | x \in S_1, y \in S_2\}$$

We also see the cardinality of the set is

$$|S_1 \times S_2| = |S_1| \times |S_2|$$

Guided Discussion:
Cartesian Power

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- ***G** is **Closed** in ******
- $\boldsymbol{e} \in G$
- $\forall x \in G, \exists\, x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group,** $\boldsymbol{D_n}$ is a group corresponding to regular n-gon*

*A **Symmetric Group,** $\boldsymbol{S_n}$ are the permutations on $\mathbb{Z}/n\mathbb{Z}$*

*A **Cyclic Group,** $\boldsymbol{Z_n}$ is the group of modular addition* $\mathrm{mod}\ n$

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Order** of group **G** is the amount of elements in **G

The cartesian product of a set and itself, n times, is

$$\underbrace{S \times S \cdots \times S}_{n\ times} = S^n$$

Where we have the set S^n being ordered n-tuples of elements in S

$$|S^n| = |S|^n$$

Guided Discussion: More Subgroups

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- ***G** is **Closed** in ******
- $\boldsymbol{e} \in G$
- $\forall x \in G, \exists\, x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group, $\boldsymbol{D_n}$** is a group corresponding to regular n-gon*

*A **Symmetric Group, $\boldsymbol{S_n}$** are the permutations on $\mathbb{Z}/n\mathbb{Z}$*

*A **Cyclic Group, $\boldsymbol{Z_n}$** is the group of modular addition $\mathrm{mod}\ n$*

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Order** of group **G** is the amount of elements in **G

Let G be a group.

There are two subgroups of G which will always exist for any group G

These two groups are

- *The set G itself with operation $*$*
- *The "trivial group" with just identity element $\{e\}$ and $*$*

Guided Discussion:
More Subgroups

*A **Group** is set **G** with binary operation ******
*that satisfies the following **4 axioms***

- ***G** is **Closed** in ******
- $\boldsymbol{e} \in G$
- $\forall x \in G, \exists\, x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group,** $\boldsymbol{D_n}$ is a group corresponding to regular n-gon*

*A **Symmetric Group,** $\boldsymbol{S_n}$ are the permutations on* $\mathbb{Z}/n\mathbb{Z}$

*A **Cyclic Group,** $\boldsymbol{Z_n}$ is the group of modular addition* $\mathrm{mod}\ n$

***Order** of $g \in G$ is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

How do we know the trivial group will always be a subgroup?

- *Is it closed?*
- *Does every element have an inverse?*

Guided Discussion:
More Subgroups

*A **Group** is set **G** with binary operation ******
*that satisfies the following **4 axioms***

- ***G** is **Closed** in ******
- $\boldsymbol{e} \in G$
- $\forall x \in G, \exists\, x^{-1}$ *such that* $x^{-1} * x = e$
- ***Associative*** $x * (y * z) = (x * y) * z$

*A **Dihedral Group,** $\boldsymbol{D_n}$ is a group corresponding to regular* n*-gon*

*A **Symmetric Group,** $\boldsymbol{S_n}$ are the permutations on* $\mathbb{Z}/n\mathbb{Z}$

*A **Cyclic Group,** $\boldsymbol{Z_n}$ is the group of modular addition* $\bmod n$

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

How do we know the trivial group will always be a subgroup?

- *Is it closed?*
- *Does every element have an inverse?*

Yes, as the only element, e, maps back to itself when operated on by $*$ *and the inverse of e is e*

Guided Discussion: Generators

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G is ***Closed*** in *****, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\ \boldsymbol{x^{-1}}$ such that $x^{-1} * x = e$, ***Associative*** $x * (y * z) = (x * y) * z$

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

A Generating Set of a group is a subset from which all the other elements of the group can be created from finitely many operations on the initial elements of the subgroup.

This sounds confusing! Understood!

But it really isn't once you get an understanding for it.

Guided Discussion: Generators

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in* $*$, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative*** $x * (y * z) = (x * y) * z$

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

We're going to look at a few examples.

- *What are the generators of* Z_6*?*
- *What are the generators of* Z_5*?*
- *What are the generators of* Z_n*?*
- *What are the generators of* Z_p*?*

Guided Discussion: Generators

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in* $*$, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative*** $x * (y * z) = (x * y) * z$

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

- *What are the generators of* Z_6*?*
  - $\{1\}$
  - $\{5\}$
  - ***The only single-element generators are those elements relatively prime to 6!!*
- *What are the generators of* Z_5*?*
  - $\{1\}$
  - $\{2\}$
  - $\{3\}$
  - $\{4\}$

Guided Discussion: Generators

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in* ***, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative*** $x * (y * z) = (x * y) * z$

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

- *What are the generators of* Z_n*?*
  - *The only guaranteed generators of* Z_n *are the sets of individual numbers relatively prime to* n *or sets of factors of* n
- *What are the generators of* Z_p*?*
  - *We see that any element of* Z_p *can generate* Z_p*! Try it yourself!*
  - *We see that this is because any element of* Z_p *is relatively prime to* p

Guided Discussion: Generators

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in *,* $\boldsymbol{e \in G}$*,* $\forall x \in G$*,* $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$*, **Associative*** $x * (y * z) = (x * y) * z$

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

We're going to try generating Z_5 *with a random element of* Z_5

Take $\{3\}$.

$$3 = 3$$
$$3 + 3 = 1$$
$$3 + 3 + 3 = 4$$
$$3 + 3 + 3 + 3 = 2$$
$$3 + 3 + 3 + 3 + 3 = 0$$

And we've generated all the elements of Z_5 *from* $\{3\}$*! (we could do this for any number less than a prime* p*)*

Guided Discussion:
Lagrange's Theorem

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in* *, $\boldsymbol{e \in G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative*** $x * (y * z) = (x * y) * z$

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$

Lagrange's Theorem states that for a group G *and subgroup* H*, that*

$$|H| \text{ divides } |G|$$

Where $|G|$ *denotes the cardinality or "order" of* G

Which is more complicated to prove, but we take it as a lemma

Guided Discussion:
Lagrange's Theorem

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in* *, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\ \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative*** $x * (y * z) = (x * y) * z$

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$, *that* $|H|$ *divides* $|G|$

Lagrange's Theorem states that for a group G *and subgroup* H, *that*

$$|H| \text{ divides } |G|$$

Where $|G|$ *denotes the cardinality or "order" of* G

Which is more complicated to prove, but we take it as a lemma

Guided Discussion: Lagrange's Theorem

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G is **Closed** in *, $\boldsymbol{e \in G}$, $\forall x \in G$, $\exists\ \boldsymbol{x^{-1}}$ such that $x^{-1} * x = e$, **Associative** $x * (y * z) = (x * y) * z$

*A **Cyclic Group, $\boldsymbol{Z_n}$** is the group of modular addition $\mathrm{mod}\ n$*

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for G and $H \subset G$, that $|H|$ divides $|G|$*

How many subgroups does Z_6 have?

Guided Discussion: Lagrange's Theorem

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G is **Closed** in *, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\ \boldsymbol{x^{-1}}$ such that $x^{-1} * x = e$, **Associative** $x * (y * z) = (x * y) * z$

*A **Cyclic Group, $\boldsymbol{Z_n}$** is the group of modular addition $\bmod n$*

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for G and $H \subset G$, that $|H|$ divides $|G|$*

How many subgroups does Z_6 have?

- $\{0\}$
- $\{0,3\}$
- $\{0,2,4\}$
- Z_6

It has 4 subgroups.

Guided Discussion:
Lagrange's Theorem

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in *,* $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative*** $x * (y * z) = (x * y) * z$

*A **Cyclic Group,*** $\boldsymbol{Z_n}$ *is the group of modular addition* $\bmod n$

Order *of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order *of group **G** is the amount of elements in **G***

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

Lagrange's Theorem *states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$

$$|Z_6| = 6$$

- $|\{0\}| = 1$
- $|\{0,3\}| = 2$
- $|\{0,2,4\}| = 3$
- $|Z_6| = 6$

We see that the order of the subgroups divides the order of the group itself, complying by Lagrange's

Guided Discussion: Lagrange's Theorem

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G is **Closed** in *, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\ \boldsymbol{x^{-1}}$ such that $x^{-1} * x = e$, ***Associative*** $x * (y * z) = (x * y) * z$

*A **Cyclic Group, $\boldsymbol{Z_n}$** is the group of modular addition $\mathrm{mod}\ n$*

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for G and $H \subset G$, that $|H|$ divides $|G|$*

How many subgroups does Z_p have for p a prime?

Guided Discussion:
Lagrange's Theorem

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in* *, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative*** $x * (y * z) = (x * y) * z$

*A **Cyclic Group,*** $\boldsymbol{Z_n}$ *is the group of modular addition* $\mathrm{mod}\ n$

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$

How many subgroups does Z_p *have for* p *a prime?*

Only 2*, as only two subgroups can exist, one with order* 1 *and one with order* p*, as these are the only two which can divide* p*. These two are*

- $\{0\}$
- Z_p

Guided Discussion: Abelian Groups

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in *,* $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$, *that* $|H|$ *divides* $|G|$

An Abelian Group is one for which the operation $*$ *commutes for any two elements of* G.

$$xy = yx \text{ for all } x, y \in G$$

One example of this are the cyclic groups Z_n

We think of these cyclic groups as building blocks, building up with direct products

Guided Discussion: *Abelian Groups*

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in *,* $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$, *that* $|H|$ *divides* $|G|$

We're going to play around with direct product groups a little bit.

Which of the following are isomorphic?

- Z_4
- $Z_2 \times Z_3$
- $Z_2 \times Z_2$
- Z_6

Guided Discussion: Abelian Groups

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in *,* $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\ \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$

Which of the following are isomorphic?

- Z_4
- $Z_2 \times Z_3$
- $Z_2 \times Z_2$
- Z_6

Only $Z_2 \times Z_3$ *and* Z_6*! None others.*

Guided Discussion:
Abelian Groups

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G is **Closed** in *, $\boldsymbol{e \in G}$, $\forall x \in G$, $\exists\ \boldsymbol{x^{-1}}$ such that $x^{-1} * x = e$, ***Associative***

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for G and $H \subset G$, that $|H|$ divides $|G|$*

- Z_4
- $Z_2 \times Z_3$
- $Z_2 \times Z_2$
- Z_6

Only $Z_2 \times Z_3$ and Z_6 because Z_4 has an element of order 4 while $Z_2 \times Z_2$ does not. But Z_6 has a generating element of order 6, as well as $Z_2 \times Z_3$. We can further examine that Z_6 is isomorphic to $Z_2 \times Z_3$

Guided Discussion:
Abelian Groups

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- *G is **Closed** in *, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ such that $x^{-1} * x = e$, **Associative***

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for G and $H \subset G$, that $|H|$ divides $|G|$*

A key fact about abelian groups is that

$$Z_a \times Z_b \text{ is isomorphic to } Z_{ab}$$

If both a and b are relatively prime.

We can see one deduction from this is that $(1,1)$ is a generator of $Z_a \times Z_b$ with the same order as 1 in Z_{ab}

Guided Discussion:
Abelian Groups

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in *,* $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$

Further, we can say that every finite abelian group is isomorphic to a product of cyclic groups whose orders are prime powers.

$$Z_{p^m} \times Z_{q^n} \times \cdots Z_{l^k}$$

Where p, q *and* l *are primes*

Guided Discussion: Abelian Groups

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in* *****, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$, *that* $|H|$ *divides* $|G|$

***Abelian Groups** are those whose operation commutes with all elements in **G**. Finite Abelian Groups are the direct product of cyclic groups of prime powers.*

How many abelian groups have order 20?

Guided Discussion:
Abelian Groups

*A **Group** is set **G** with binary operation ******
*that satisfies the following **4 axioms***

- G is ***Closed*** in ***, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\ \boldsymbol{x^{-1}}$ such that $x^{-1} * x = e$, ***Associative***

Order *of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order *of group* $\boldsymbol{G}$ *is the amount of elements in* $\boldsymbol{G}$

*A **Generating Set** is a **subset** of all elements in group* $\boldsymbol{G}$ *for which all the other elements of* $\boldsymbol{G}$ *can be created from.*

Lagrange's Theorem *states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$

How many abelian groups have order 20?

Only 2

- $Z_5 \times Z_4$
- $Z_5 \times Z_2 \times Z_2$

Why aren't these two Isomorphic?

Why isn't Z_{20} *in here?*

Guided Discussion:

Abelian Groups

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in *,* $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\ \boldsymbol{x}^{-1}$ *such that* $x^{-1} * x = e$, ***Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$

- $Z_5 \times Z_4$
- $Z_5 \times Z_2 \times Z_2$

Why aren't these two Isomorphic?

- *Because* Z_4 *and* $Z_2 \times Z_2$ *aren't isomorphic*

Why isn't Z_{20} *in here?*

- *Because that is isomorphic to* $Z_5 \times Z_4$

Guided Discussion:
Cyclic Groups

*A **Group** is set **G** with binary operation ******
*that satisfies the following **4 axioms***

- G *is **Closed** in* *, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$, *that* $|H|$ *divides* $|G|$

We've been calling Z_n *the cyclic groups, but a group is really just cyclic if it is isomorphic to* Z_n *for some* n*.*

This means a group is cyclic if it is generated by a single element.

This also means that there is some element whose order equals the order of the group.

What is an element that can generate Z_6*? What about* Z_9*? What about* Z_{103}*?*

Guided Discussion: Cyclic Groups

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in* $*$, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$

Is $Z_2 \times Z_4$ *cyclic? (with operation of componentwise addition)*

Guided Discussion: Cyclic Groups

*A **Group** is set **G** with binary operation ******
*that satisfies the following **4 axioms***

- G *is **Closed** in *,* $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\ \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$, *that* $|H|$ *divides* $|G|$

Is $Z_2 \times Z_4$ *cyclic? (with operation of componentwise addition)*

No, because all of the elements of this set have order 1, 2, or 4, but the set has order 8. Let's look at one of the elements:

$$(1,3), (1,3)^2 = (0,2), (1,3)^3 = (1,1), (1,3)^4 = (0,0)$$

We see that $(1,3)$ *has order 4. We can check all elements and find that none of them generate the group.*

Guided Discussion:
Cyclic Groups

*A **Group** is set **G** with binary operation ******
*that satisfies the following **4 axioms***

- G *is **Closed** in* *, $\boldsymbol{e \in G}$, $\forall x \in G$, $\exists\ \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$

Let's look at a new type of group.
Let's define

$$Z_n^*$$

To be the set of elements of Z_n *which are relatively prime to* n*, for which the operation is multiplication* $\mathrm{mod}\ n$ *instead of addition* $\mathrm{mod}\ n$

What is the order of Z_n^**?*

Guided Discussion:
Cyclic Groups

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in *****,* $\boldsymbol{e \in G}$, $\forall x \in G$, $\exists\ \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$*, **Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$

Let's look at a new type of group. Let's define

$$Z_n^*$$

To be the set of elements of Z_n *which are relatively prime to* n*, for which the operation is multiplication* $\mathrm{mod}\ n$ *instead of addition* $\mathrm{mod}\ n$

What is the order of Z_n^**?*

$$|Z_n^*| = \phi(n)$$

Guided Discussion: Cyclic Groups

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in *,* $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\ \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$

Which group is Z_8^* *isomorphic to?*

- Z_4
- Z_7
- Z_8
- $Z_2 \times Z_2$

Guided Discussion: Cyclic Groups

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in *,* $\boldsymbol{e \in G}$, $\forall x \in G$, $\exists\ \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$*, **Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$

Which group is Z_8^* isomorphic to?

- $Z_2 \times Z_2$

For both of these groups, the nontrivial elements have order 2.

$$3^2 = 5^2 = 7^2 = 1$$

Guided Discussion: Cyclic Groups

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in* *, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$

Which group is Z_{10}^* *isomorphic to?*

- Z_4
- Z_5
- Z_8
- $Z_2 \times Z_5$

Guided Discussion: Cyclic Groups

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G is ***Closed*** *in *,* $\boldsymbol{e \in G}$, $\forall x \in G$, $\exists\ \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$*, **Associative***

Order *of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order *of group **G** is the amount of elements in **G***

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

Lagrange's Theorem *states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$

Which group is Z_{10}^* *isomorphic to?*

- Z_4

For both groups, there are 4 elements and 1 generator. In Z_{10}^*, 3 *is the generator*

$$3^2 = 9$$
$$3^3 = 7$$
$$3^4 = 1$$

Guided Discussion: *Number Theory*

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in* *, $\boldsymbol{e \in G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$

We're going to show that the set

$$\{1,2,3 \ldots p\}$$

Is the same as the set

$$\{a, 2a, 3a \ldots pa\}$$

With group theory (remember this from Fermat's little theorem?

Guided Discussion:
Number Theory

*A **Group** is set **G** with binary operation ******
*that satisfies the following **4 axioms***

- G *is **Closed** in **, $\boldsymbol{e \in G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$

Take Z_p *to be a group with* p *a prime.*

Now let's take the subgroup G *generated by* $a \neq 1$ *,*$a \in Z_p$

What is the order of Z_p*?*

What is the order of G*?*

Guided Discussion:
Number Theory

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in *,* $\boldsymbol{e \in G}$, $\forall x \in G$, $\exists\ \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$, *that* $|H|$ *divides* $|G|$

Now let's take the subgroup G *generated by* $a \neq 1$, $a \in Z_p$

What is the order of Z_p^**?*

- *We know this is* $\phi(p) = p - 1$

What is the order of G*?*

- *We know that the order of* G *must divide the order of* Z_p *by Lagrange's. This means the order of* G *is* $p - 1$

Guided Discussion:

Number Theory

*A **Group** is set **G** with binary operation ******
*that satisfies the following **4 axioms***

- G *is **Closed** in ******, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\ \boldsymbol{x}^{-1}$ *such that* $x^{-1} * x = e$, ***Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$, *that* $|H|$ *divides* $|G|$

Because the order of G *is* $p - 1$ *and* G *is generated entirely from* a, *we know that* G *is just the set*

$$\{a, 2a, 3a \dots pa\}$$

But this is just a rearrangement of Z_p *because it is a subgroup of* Z_p *and has the same elements.*

Guided Discussion: Number Theory

*A **Group** is set **G** with binary operation * that satisfies the following **4 axioms***

- *G is **Closed** in *, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ such that $x^{-1} * x = e$, **Associative***

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for G and $H \subset G$, that $|H|$ divides $|G|$*

Now we know that

$$\{1,2,3 \ldots (p-1)\}$$

$$\{a, 2a, 3a \ldots (p-1)a\}$$

Are the same sets $\mathrm{mod}\ p$. (we just took out the 0 element.

That means the product of every element in the first set equals the product of every element in the second set $\mathrm{mod}\ p$

Guided Discussion:
Number Theory

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in *****,* $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$, ***Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$, *that* $|H|$ *divides* $|G|$

$$\{1,2,3 \ldots (p-1)\}$$
$$\{a, 2a, 3a \ldots (p-1)a\}$$

So now we take

$$(p-1)! = a^{p-1}(p-1)!$$

We see this is

$$1 \equiv a^{p-1} \bmod p$$

Guided Discussion:
Number Theory

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- *G is **Closed** in *, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x}^{-1}$ such that $x^{-1} * x = e$, **Associative***

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for G and $H \subset G$, that $|H|$ divides $|G|$*

With group theory, we show this as any subset G of Z_p^* generated by element $a \in Z_p^*$ has order $p - 1$ by Lagrange's Theorem. This means the order of a is $p - 1$ since it generated G. This also means that

$$a^p \equiv a$$

Which is (after multiplying by a^{-1})

$$a^p * a^{-1} = a^{p-1} = 1 = a^{-1} * a$$

Guided Discussion:
Number Theory

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G *is **Closed** in *,* $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$*, **Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$

Practice!

What does $(p-1)!$ *equal* $\bmod p$*?*

Hint: consider this as multiplying all the elements in Z_p^**, and that* Z_p^* *is an abelian group, and think about our group axioms!*

Guided Discussion: Applications

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

- G is **Closed** in *, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ such that $x^{-1} * x = e$, ***Associative***

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

Order** of group **G** is the amount of elements in **G

*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for G and $H \subset G$, that $|H|$ divides $|G|$*

We're going to do this.

Actually try to understand an application behind this crazy "group theory".

Guided Discussion:

Peg-Solitaire

*A **Group** is set **G** with binary operation ******
*that satisfies the following **4 axioms***

- G *is **Closed** in *,* $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\ \boldsymbol{x}^{-1}$ *such that* $x^{-1} * x = e$, ***Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

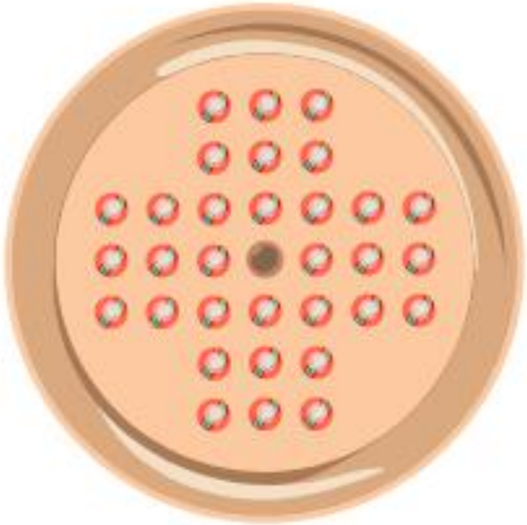
*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$, *that* $|H|$ *divides* $|G|$

Most of the time we can describe permutations of puzzle objects.

Consider Peg-Solitaire.

We have a board filled with pegs and one blank square. The main move is jumping, like checkers but only horizontally and vertically.



Guided Discussion:
Peg-Solitaire

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

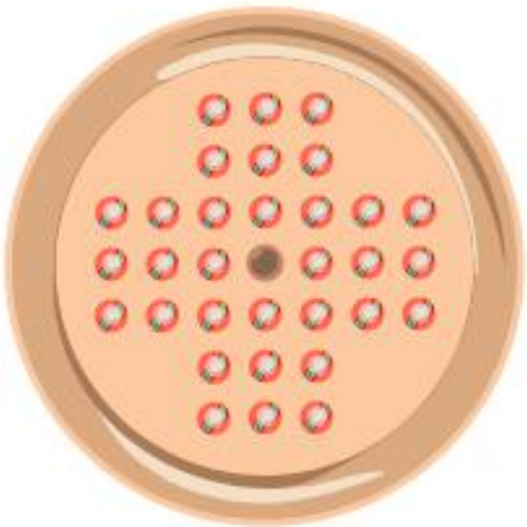
- G *is **Closed** in *,* $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\ \boldsymbol{x}^{-1}$ *such that* $x^{-1} * x = e$*, **Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

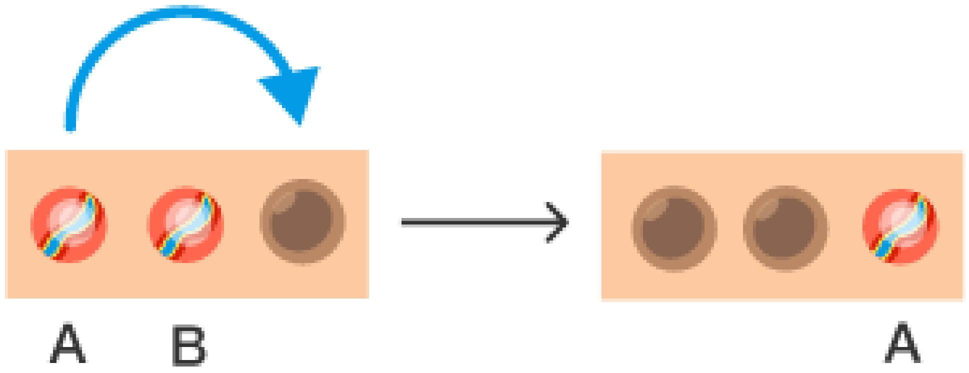
*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$



Most of the time we can describe permutations of puzzle objects.

The goal is to only get one peg left. We can do this by jumping pegs.



Guided Discussion:
Peg-Solitaire

*A **Group** is set **G** with binary operation ***** that satisfies the following **4 axioms***

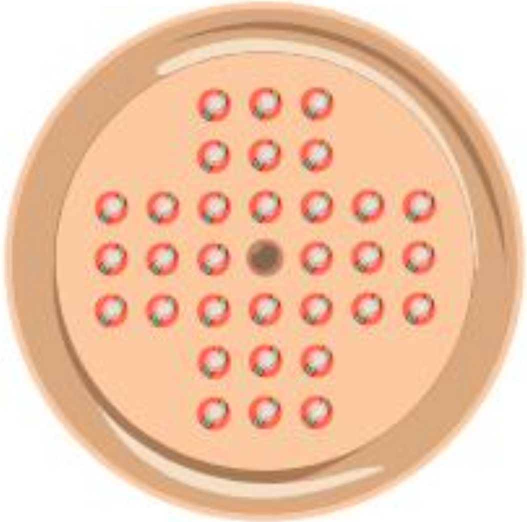
- G *is **Closed** in *,* $\boldsymbol{e \in G}$*,* $\forall x \in G$*,* $\exists\, \boldsymbol{x^{-1}}$ *such that* $x^{-1} * x = e$*, **Associative***

***Order** of* $g \in G$ *is smallest such integer such that* $g^k = e$

Order** of group **G** is the amount of elements in **G

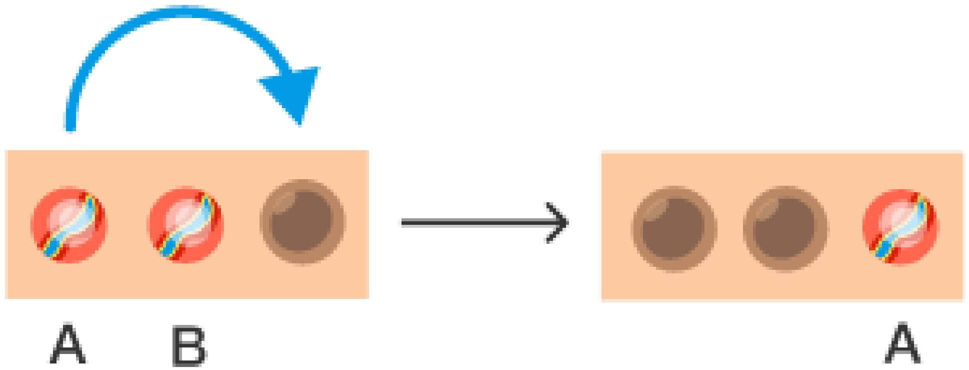
*A **Generating Set** is a **subset** of all elements in group **G** for which all the other elements of **G** can be created from.*

***Lagrange's Theorem** states that for* G *and* $H \subset G$*, that* $|H|$ *divides* $|G|$



Most of the time we can describe permutations of puzzle objects.

The goal is to only get one peg left. We can do this by jumping pegs.



Guided Discussion:

Peg-Solitaire

*A **Group** is set $\boldsymbol{G}$ with binary operation $*$ that satisfies the following **4 axioms***

- *G is **Closed** in $*$, $\boldsymbol{e} \in \boldsymbol{G}$, $\forall x \in G$, $\exists\, \boldsymbol{x^{-1}}$ such that $x^{-1} * x = e$, **Associative***

***Order** of $g \in G$ is smallest such integer such that $g^k = e$*

***Order** of group $\boldsymbol{G}$ is the amount of elements in $\boldsymbol{G}$*

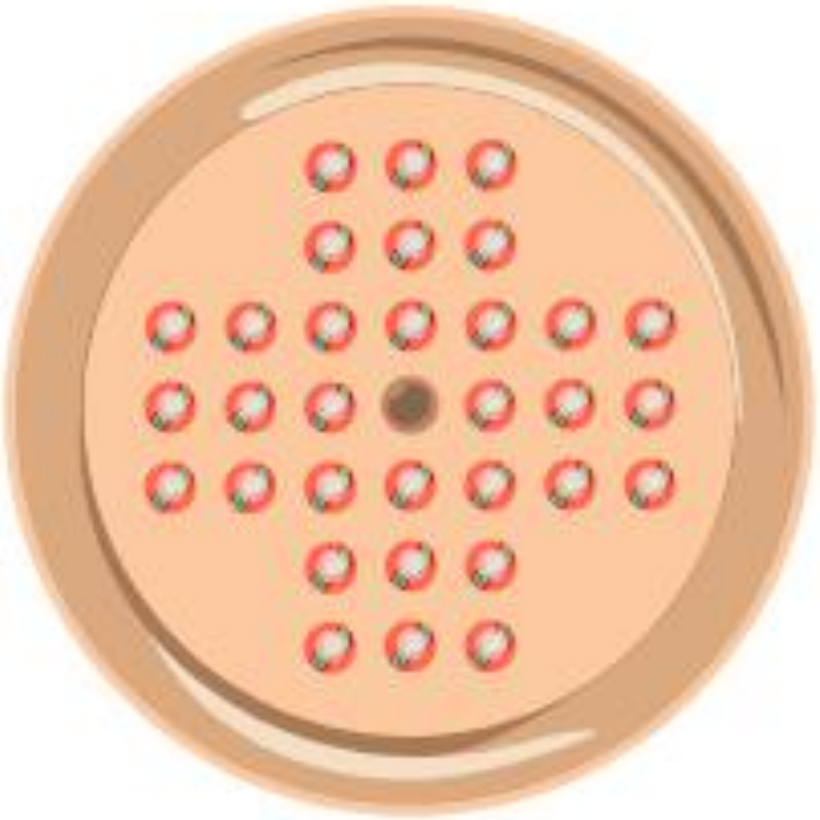
*A **Generating Set** is a **subset** of all elements in group $\boldsymbol{G}$ for which all the other elements of $\boldsymbol{G}$ can be created from.*

***Lagrange's Theorem** states that for G and $H \subset G$, that $|H|$ divides $|G|$*

*In this context, an **Invariant** is a quantity which stays the same after each move of the game.*

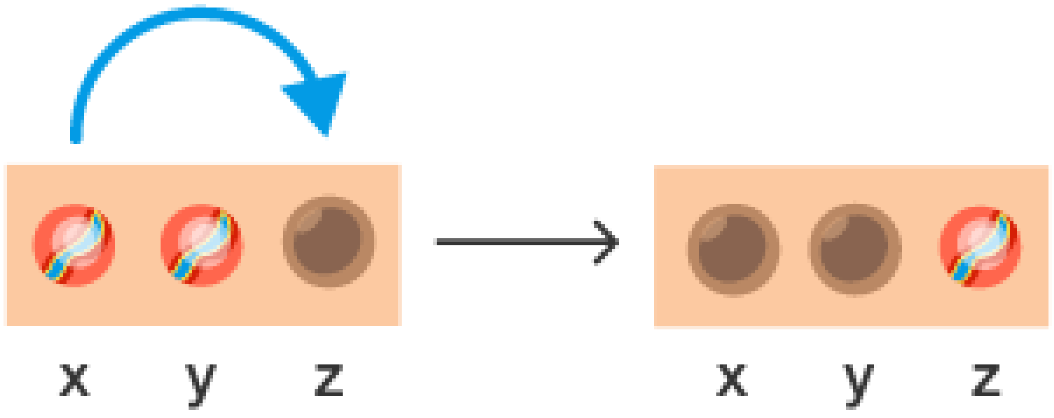
*We will use **invariants** to determine which configurations of the board are impossible.*

Guided Discussion: *Peg-Solitaire*

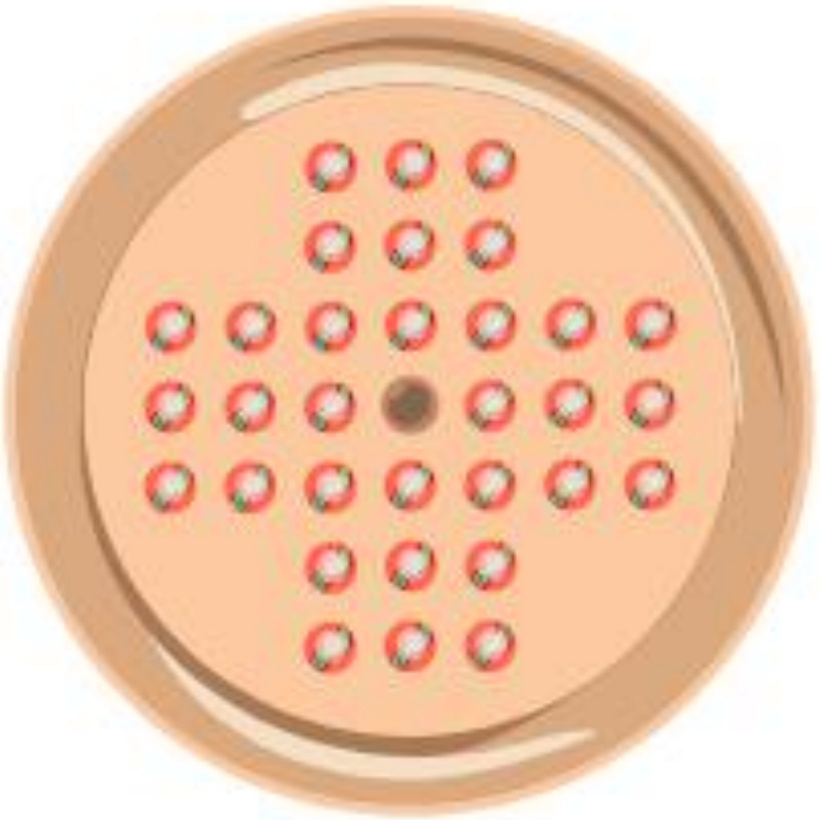


Suppose we label the holes of this board with the elements of the Klein Group $\{e, x, y, z\}$ *such that* $x^2 = y^2 = z^2 = e$ *and* $xy = yx = z$, $xz = zx = y$, *and* $zy = yz = x$.

Suppose we label our board with members of this group.

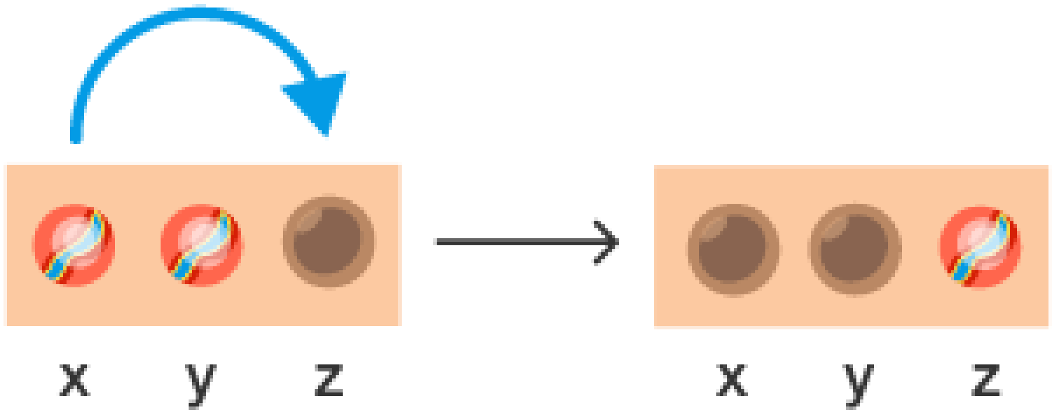


Guided Discussion:
Peg-Solitaire



We see that if we calculate the product of the elements labeling occupied holes, then perform the jump and do the same calculation, this product stays the same.

$$xy = z$$
$$z = z$$



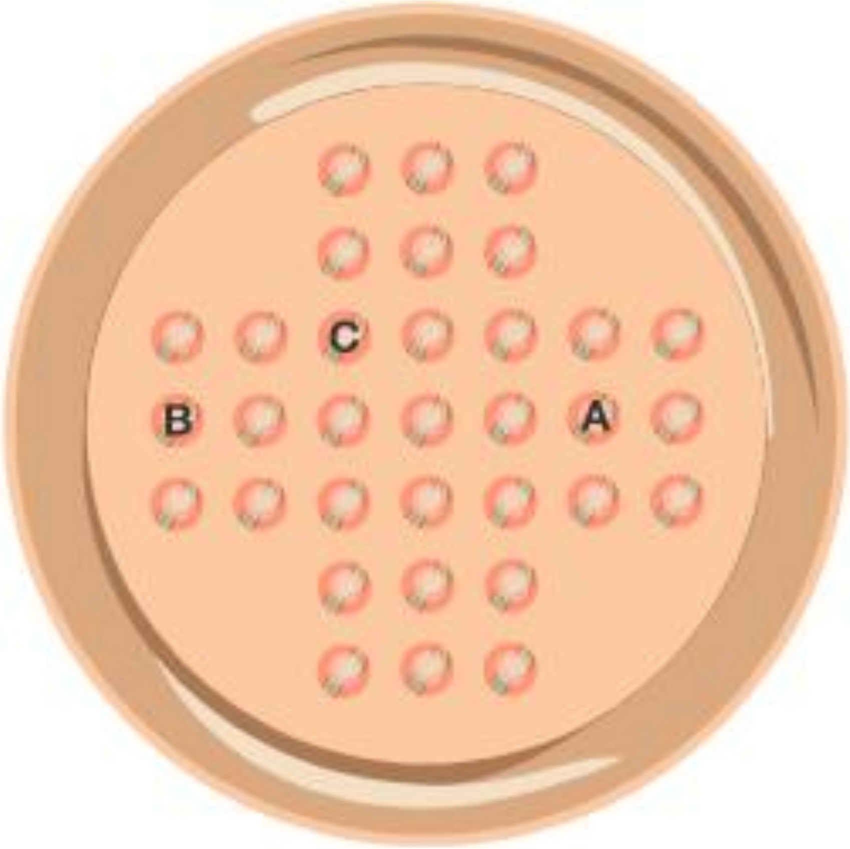
Guided Discussion:
Peg-Solitaire

Now we label our hole board to accompany this.

Every 3 consecutive spots contain x, y and z in some order.

The product of group elements taken over all occupied squares is an ***invariant*** *no matter what moves you do.*

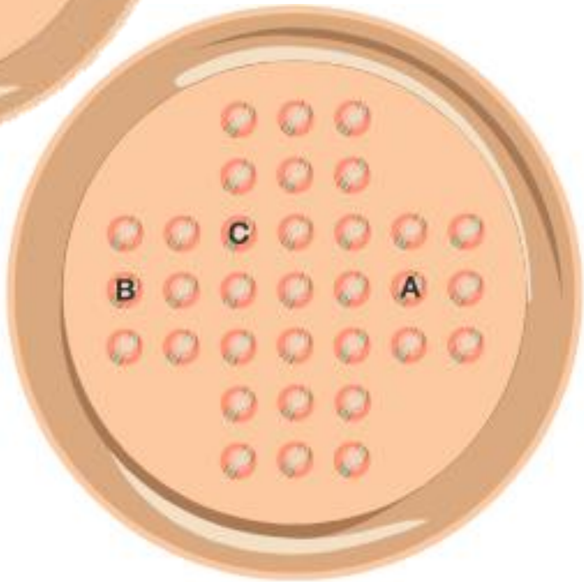
Guided Discussion:
Peg-Solitaire



Which of these possible pebbles is a possible location for our last marble to be?

Guided Discussion:

Peg-Solitaire



First we have to calculate the invariant for the initial position. But we quickly see that if we can group our board into 3s, we see that this is just y.

Now we find which of A, B and C are also labeled y. We see this is B