Introduction to Group Theory

R. Philip Grizzard
University of Illinois at Chicago

Presentation for Advanced Mathematics Undergraduates
Westminster College

January 31, 2007

Outline

Definitions

A **group** is a set with an operation.

To be more formal, we say a group is an ordered pair $(G, \star)$, where G is a set and $\star$ is a binary operation on G satisfying the following axioms:

- **Closure:** For all $a, b \in G$, the product $a \star b$ is also in G.

Definitions

A **group** is a set with an operation.
To be more formal, we say a group is an ordered pair $(G, \star)$, where G is a set and $\star$ is a binary operation on G satisfying the following axioms:

- **Closure:** For all $a, b \in G$, the product $a \star b$ is also in G.
- **Associativity:** For all $a, b, c \in G$, $(a \star b) \star c = a \star (b \star c)$.

Definitions

A **group** is a set with an operation.
To be more formal, we say a group is an ordered pair $(G, \star)$, where G is a set and $\star$ is a binary operation on G satisfying the following axioms:

- **Closure:** For all $a, b \in G$, the product $a \star b$ is also in G.
- **Associativity:** For all $a, b, c \in G$, $(a \star b) \star c = a \star (b \star c)$.
- **Identity:** There exists an element $e \in G$, called the *identity* of G, such that for all $a \in G$, $a \star e = e \star a = a$.

Definitions

A **group** is a set with an operation.
To be more formal, we say a group is an ordered pair $(G, \star)$, where G is a set and $\star$ is a binary operation on G satisfying the following axioms:

- **Closure:** For all $a, b \in G$, the product $a \star b$ is also in G.
- **Associativity:** For all $a, b, c \in G$, $(a \star b) \star c = a \star (b \star c)$.
- **Identity:** There exists an element $e \in G$, called the *identity* of G, such that for all $a \in G$, $a \star e = e \star a = a$.
- **Inverses:** For every element $a \in G$, there is an element a^{-1}, called the *inverse* of a, such that $a \star a^{-1} = a^{-1} \star a = e$.

Definitions

A **group** is a set with an operation.
To be more formal, we say a group is an ordered pair $(G, \star)$, where G is a set and $\star$ is a binary operation on G satisfying the following axioms:

- **Closure:** For all $a, b \in G$, the product $a \star b$ is also in G.
- **Associativity:** For all $a, b, c \in G$, $(a \star b) \star c = a \star (b \star c)$.
- **Identity:** There exists an element $e \in G$, called the *identity* of G, such that for all $a \in G$, $a \star e = e \star a = a$.
- **Inverses:** For every element $a \in G$, there is an element a^{-1}, called the *inverse* of a, such that $a \star a^{-1} = a^{-1} \star a = e$.

For a group $(G, \star)$, it is very common to say "G is a group under $\star$."

Definitions

A **group** is a set with an operation.
To be more formal, we say a group is an ordered pair $(G, \star)$, where G is a set and $\star$ is a binary operation on G satisfying the following axioms:

- **Closure:** For all $a, b \in G$, the product $a \star b$ is also in G.
- **Associativity:** For all $a, b, c \in G$, $(a \star b) \star c = a \star (b \star c)$.
- **Identity:** There exists an element $e \in G$, called the *identity* of G, such that for all $a \in G$, $a \star e = e \star a = a$.
- **Inverses:** For every element $a \in G$, there is an element a^{-1}, called the *inverse* of a, such that $a \star a^{-1} = a^{-1} \star a = e$.

For a group $(G, \star)$, it is very common to say "G is a group under $\star$."

Definitions

A **group** is a set with an operation.
To be more formal, we say a group is an ordered pair $(G, \star)$, where G is a set and $\star$ is a binary operation on G satisfying the following axioms:

- **Closure:** For all $a, b \in G$, the product $a \star b$ is also in G.
- **Associativity:** For all $a, b, c \in G$, $(a \star b) \star c = a \star (b \star c)$.
- **Identity:** There exists an element $e \in G$, called the *identity* of G, such that for all $a \in G$, $a \star e = e \star a = a$.
- **Inverses:** For every element $a \in G$, there is an element a^{-1}, called the *inverse* of a, such that $a \star a^{-1} = a^{-1} \star a = e$.

For a group $(G, \star)$, it is very common to say "G is a group under $\star$."

Examples

The set of real numbers $\mathbb{R}$ is a group under the operation $+$.

- The identity e is 0.
- For any element $a \in \mathbb{R}$, the corresponding element "a^{-1}" is usually denoted $-a$. This way, we have $a + -a = 0$, the identity.

Examples

The set of real numbers $\mathbb{R}$ is a group under the operation $+$.

- The identity e is 0.
- For any element $a \in \mathbb{R}$, the corresponding element "a^{-1}" is usually denoted $-a$. This way, we have $a + -a = 0$, the identity. So every element in $\mathbb{R}$ has an inverse.

Examples

The set of real numbers $\mathbb{R}$ is a group under the operation $+$.

- The identity e is 0.
- For any element $a \in \mathbb{R}$, the corresponding element "a^{-1}" is usually denoted $-a$. This way, we have $a + -a = 0$, the identity. So every element in $\mathbb{R}$ has an inverse.
- The usual laws of addition give us associativity.

Examples

The set of real numbers $\mathbb{R}$ is a group under the operation $+$.

- The identity e is 0.
- For any element $a \in \mathbb{R}$, the corresponding element "a^{-1}" is usually denoted $-a$. This way, we have $a + -a = 0$, the identity. So every element in $\mathbb{R}$ has an inverse.
- The usual laws of addition give us associativity.
- If we add two real numbers, we certainly get a real number, so we have closure.

Examples

The set of real numbers $\mathbb{R}$ is a group under the operation $+$.

- The identity e is 0.
- For any element $a \in \mathbb{R}$, the corresponding element "a^{-1}" is usually denoted $-a$. This way, we have $a + -a = 0$, the identity. So every element in $\mathbb{R}$ has an inverse.
- The usual laws of addition give us associativity.
- If we add two real numbers, we certainly get a real number, so we have closure.

The integers $\mathbb{Z}$ also form a group with the operation $+$.

Examples

The set of real numbers $\mathbb{R}$ is a group under the operation $+$.

- The identity e is 0.
- For any element $a \in \mathbb{R}$, the corresponding element "a^{-1}" is usually denoted $-a$. This way, we have $a + -a = 0$, the identity. So every element in $\mathbb{R}$ has an inverse.
- The usual laws of addition give us associativity.
- If we add two real numbers, we certainly get a real number, so we have closure.

The integers $\mathbb{Z}$ also form a group with the operation $+$.

Each of these groups are examples of **abelian** (or **commutative**) groups: $a \star b = b \star a$ for all $a, b \in G$.

Examples

The set of real numbers $\mathbb{R}$ is a group under the operation $+$.

- The identity e is 0.
- For any element $a \in \mathbb{R}$, the corresponding element "a^{-1}" is usually denoted $-a$. This way, we have $a + -a = 0$, the identity. So every element in $\mathbb{R}$ has an inverse.
- The usual laws of addition give us associativity.
- If we add two real numbers, we certainly get a real number, so we have closure.

The integers $\mathbb{Z}$ also form a group with the operation $+$.

Each of these groups are examples of **abelian** (or **commutative**) groups: $a \star b = b \star a$ for all $a, b \in G$.

Examples

The set of real numbers $\mathbb{R}$ is a group under the operation $+$.

- The identity e is 0.
- For any element $a \in \mathbb{R}$, the corresponding element "a^{-1}" is usually denoted $-a$. This way, we have $a + -a = 0$, the identity. So every element in $\mathbb{R}$ has an inverse.
- The usual laws of addition give us associativity.
- If we add two real numbers, we certainly get a real number, so we have closure.

The integers $\mathbb{Z}$ also form a group with the operation $+$.

Each of these groups are examples of **abelian** (or **commutative**) groups: $a \star b = b \star a$ for all $a, b \in G$.

Questions

- Is $\mathbb{R}$ a group with the operation multiplication?

Almost, but not quite. What element of $\mathbb{R}$ fails one of the axioms?
Hint: What is the multiplicative inverse of 0?

Questions

- Is $\mathbb{R}$ a group with the operation multiplication?

Almost, but not quite. What element of $\mathbb{R}$ fails one of the axioms?

Hint: What is the multiplicative inverse of 0?

- $\mathbb{R} - \{0\}$ is a group under multiplication.

Questions

- Is $\mathbb{R}$ a group with the operation multiplication?

Almost, but not quite. What element of $\mathbb{R}$ fails one of the axioms?
Hint: What is the multiplicative inverse of 0?

- $\mathbb{R} - \{0\}$ is a group under multiplication.
  - How about $\mathbb{Q}$ under addition?

Questions

- Is $\mathbb{R}$ a group with the operation multiplication?

Almost, but not quite. What element of $\mathbb{R}$ fails one of the axioms?
Hint: What is the multiplicative inverse of 0?

- $\mathbb{R} - \{0\}$ is a group under multiplication.
  - How about $\mathbb{Q}$ under addition?

Yes, similarly as $\mathbb{R}$.

Questions

- Is $\mathbb{R}$ a group with the operation multiplication?

Almost, but not quite. What element of $\mathbb{R}$ fails one of the axioms?
Hint: What is the multiplicative inverse of 0?

- $\mathbb{R} - \{0\}$ is a group under multiplication.
  - How about $\mathbb{Q}$ under addition?

Yes, similarly as $\mathbb{R}$.

  - $\mathbb{Q}$ under multiplication?

Questions

- Is $\mathbb{R}$ a group with the operation multiplication?

Almost, but not quite. What element of $\mathbb{R}$ fails one of the axioms?
Hint: What is the multiplicative inverse of 0?

- $\mathbb{R} - \{0\}$ is a group under multiplication.

- How about $\mathbb{Q}$ under addition?

Yes, similarly as $\mathbb{R}$.

- $\mathbb{Q}$ under multiplication?

$\mathbb{Q} - \{0\}$ is a group under multiplication.

Questions

- Is $\mathbb{R}$ a group with the operation multiplication?

Almost, but not quite. What element of $\mathbb{R}$ fails one of the axioms?
Hint: What is the multiplicative inverse of 0?

- $\mathbb{R} - \{0\}$ is a group under multiplication.

- How about $\mathbb{Q}$ under addition?

Yes, similarly as $\mathbb{R}$.

- $\mathbb{Q}$ under multiplication?

$\mathbb{Q} - \{0\}$ is a group under multiplication.

- Is $\mathbb{Z}$ a group under multiplication?

Questions

- Is $\mathbb{R}$ a group with the operation multiplication?

Almost, but not quite. What element of $\mathbb{R}$ fails one of the axioms?
Hint: What is the multiplicative inverse of 0?

- $\mathbb{R} - \{0\}$ is a group under multiplication.

- How about $\mathbb{Q}$ under addition?

Yes, similarly as $\mathbb{R}$.

- $\mathbb{Q}$ under multiplication?

$\mathbb{Q} - \{0\}$ is a group under multiplication.

- Is $\mathbb{Z}$ a group under multiplication?

No! It's identity is 1, but almost all elements do not have inverses in the set $\mathbb{Z}$.

Questions

- Is $\mathbb{R}$ a group with the operation multiplication?

Almost, but not quite. What element of $\mathbb{R}$ fails one of the axioms?
Hint: What is the multiplicative inverse of 0?

- $\mathbb{R} - \{0\}$ is a group under multiplication.
  - How about $\mathbb{Q}$ under addition?

Yes, similarly as $\mathbb{R}$.

- $\mathbb{Q}$ under multiplication?

$\mathbb{Q} - \{0\}$ is a group under multiplication.

- Is $\mathbb{Z}$ a group under multiplication?

No! It's identity is 1, but almost all elements do not have inverses in the set $\mathbb{Z}$. For example, the multiplicative inverse of 2 would be $\frac{1}{2}$, which is not in $\mathbb{Z}$.

Questions

- Is $\mathbb{R}$ a group with the operation multiplication?

Almost, but not quite. What element of $\mathbb{R}$ fails one of the axioms? Hint: What is the multiplicative inverse of 0?

- $\mathbb{R} - \{0\}$ is a group under multiplication.

- How about $\mathbb{Q}$ under addition?

Yes, similarly as $\mathbb{R}$.

- $\mathbb{Q}$ under multiplication?

$\mathbb{Q} - \{0\}$ is a group under multiplication.

- Is $\mathbb{Z}$ a group under multiplication?

No! It's identity is 1, but almost all elements do not have inverses in the set $\mathbb{Z}$. For example, the multiplicative inverse of 2 would be $\frac{1}{2}$, which is not in $\mathbb{Z}$.

Questions

- Is $\mathbb{R}$ a group with the operation multiplication?

Almost, but not quite. What element of $\mathbb{R}$ fails one of the axioms? Hint: What is the multiplicative inverse of 0?

- $\mathbb{R} - \{0\}$ is a group under multiplication.
  - How about $\mathbb{Q}$ under addition?

Yes, similarly as $\mathbb{R}$.

- $\mathbb{Q}$ under multiplication?

$\mathbb{Q} - \{0\}$ is a group under multiplication.

- Is $\mathbb{Z}$ a group under multiplication?

No! It's identity is 1, but almost all elements do not have inverses in the set $\mathbb{Z}$. For example, the multiplicative inverse of 2 would be $\frac{1}{2}$, which is not in $\mathbb{Z}$.

Finite groups

- Is the subset of the integers $S = \{1, 2, 3, 4\}$ a group under addition?

No, there is no identity. Plus none of the elements have inverses in S.

- How about $T = \{-1, 0, 1\}$ under addition?

Finite groups

- Is the subset of the integers $S = \{1, 2, 3, 4\}$ a group under addition?

No, there is no identity. Plus none of the elements have inverses in S.

- How about $T = \{-1, 0, 1\}$ under addition?

No. $1 + 1 = 2 \notin T$, so T is not closed under addition.

Finite groups

- Is the subset of the integers $S = \{1, 2, 3, 4\}$ a group under addition?

No, there is no identity. Plus none of the elements have inverses in S.

- How about $T = \{-1, 0, 1\}$ under addition?

No. $1 + 1 = 2 \notin T$, so T is not closed under addition.

- So how do we make a *finite* group, where G is a finite set?

Finite groups

- Is the subset of the integers $S = \{1, 2, 3, 4\}$ a group under addition?

No, there is no identity. Plus none of the elements have inverses in S.

- How about $T = \{-1, 0, 1\}$ under addition?

No. $1 + 1 = 2 \notin T$, so T is not closed under addition.

- So how do we make a *finite* group, where G is a finite set?

We can't use a subset of the integers under usual addition to make a finite group.

Finite groups

- Is the subset of the integers $S = \{1, 2, 3, 4\}$ a group under addition?

No, there is no identity. Plus none of the elements have inverses in S.

- How about $T = \{-1, 0, 1\}$ under addition?

No. $1 + 1 = 2 \notin T$, so T is not closed under addition.

- So how do we make a *finite* group, where G is a finite set?

We can't use a subset of the integers under usual addition to make a finite group.

Finite groups

- Is the subset of the integers $S = \{1, 2, 3, 4\}$ a group under addition?

No, there is no identity. Plus none of the elements have inverses in S.

- How about $T = \{-1, 0, 1\}$ under addition?

No. $1 + 1 = 2 \notin T$, so T is not closed under addition.

- So how do we make a *finite* group, where G is a finite set?

We can't use a subset of the integers under usual addition to make a finite group.

Constructing a group of order 2

- Let's construct the easiest possible nontrivial group: a group G of 2 elements. We say that G has **order** 2.
- I tell you that e and f are distinct elements of G, so $G = \{e, f\}$. We will denote the operation of G as $\star$. There are only two elements in G, so any other elements we need to fulfill the axioms will turn out to be either e or f.

Constructing a group of order 2

- Let's construct the easiest possible nontrivial group: a group G of 2 elements. We say that G has **order** 2.
- I tell you that e and f are distinct elements of G, so $G = \{e, f\}$. We will denote the operation of G as $\star$.
  There are only two elements in G, so any other elements we need to fulfill the axioms will turn out to be either e or f.
- Since we have to follow the axioms, we can explicitly describe all the possible operations for this group.

Constructing a group of order 2

- Let's construct the easiest possible nontrivial group: a group G of 2 elements. We say that G has **order** 2.
- I tell you that e and f are distinct elements of G, so $G = \{e, f\}$. We will denote the operation of G as $\star$. There are only two elements in G, so any other elements we need to fulfill the axioms will turn out to be either e or f.
- Since we have to follow the axioms, we can explicitly describe all the possible operations for this group.

Constructing a group of order 2

- Let's construct the easiest possible nontrivial group: a group G of 2 elements. We say that G has **order** 2.
- I tell you that e and f are distinct elements of G, so $G = \{e, f\}$. We will denote the operation of G as $\star$. There are only two elements in G, so any other elements we need to fulfill the axioms will turn out to be either e or f.
- Since we have to follow the axioms, we can explicitly describe all the possible operations for this group.

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$.

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$.

(Therefore $e^{-1} =$

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$.

(Therefore $e^{-1} = e$).

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$. (Therefore $e^{-1} = e$).
- Also $e \star f =$

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$. (Therefore $e^{-1} = e$).
- Also $e \star f = f$

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$. (Therefore $e^{-1} = e$).
- Also $e \star f = f$, and $f \star e =$

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$. (Therefore $e^{-1} = e$).
- Also $e \star f = f$, and $f \star e = f$.

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$. (Therefore $e^{-1} = e$).
- Also $e \star f = f$, and $f \star e = f$.

What does $f \star f$ have to be?

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$. (Therefore $e^{-1} = e$).
- Also $e \star f = f$, and $f \star e = f$.

What does $f \star f$ have to be?

- f has to have an inverse f^{-1} such that $f \star f^{-1} = f^{-1} \star f = e$.

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$. (Therefore $e^{-1} = e$).
- Also $e \star f = f$, and $f \star e = f$.

What does $f \star f$ have to be?

- f has to have an inverse f^{-1} such that $f \star f^{-1} = f^{-1} \star f = e$.
- Since G has only 2 elements, we have only 2 choices: $f^{-1} = e$ or $f^{-1} = f$.

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$. (Therefore $e^{-1} = e$).
- Also $e \star f = f$, and $f \star e = f$.

What does $f \star f$ have to be?

- f has to have an inverse f^{-1} such that $f \star f^{-1} = f^{-1} \star f = e$.
- Since G has only 2 elements, we have only 2 choices: $f^{-1} = e$ or $f^{-1} = f$.
- If $f^{-1} = e$, then $f \star \mathbf{f}^{-1} = f \star \mathbf{e} =$

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$. (Therefore $e^{-1} = e$).
- Also $e \star f = f$, and $f \star e = f$.

What does $f \star f$ have to be?

- f has to have an inverse f^{-1} such that $f \star f^{-1} = f^{-1} \star f = e$.
- Since G has only 2 elements, we have only 2 choices: $f^{-1} = e$ or $f^{-1} = f$.
- If $f^{-1} = e$, then $f \star \mathbf{f}^{-1} = f \star \mathbf{e} = f$.

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$. (Therefore $e^{-1} = e$).
- Also $e \star f = f$, and $f \star e = f$.

What does $f \star f$ have to be?

- f has to have an inverse f^{-1} such that $f \star f^{-1} = f^{-1} \star f = e$.
- Since G has only 2 elements, we have only 2 choices: $f^{-1} = e$ or $f^{-1} = f$.
- If $f^{-1} = e$, then $f \star \mathbf{f^{-1}} = f \star \mathbf{e} = f$. But by the definition of inverse, we need $f \star f^{-1} =$

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$. (Therefore $e^{-1} = e$).
- Also $e \star f = f$, and $f \star e = f$.

What does $f \star f$ have to be?

- f has to have an inverse f^{-1} such that $f \star f^{-1} = f^{-1} \star f = e$.
- Since G has only 2 elements, we have only 2 choices: $f^{-1} = e$ or $f^{-1} = f$.
- If $f^{-1} = e$, then $f \star \mathbf{f^{-1}} = f \star \mathbf{e} = f$. But by the definition of inverse, we need $f \star f^{-1} = e$.

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$. (Therefore $e^{-1} = e$).
- Also $e \star f = f$, and $f \star e = f$.

What does $f \star f$ have to be?

- f has to have an inverse f^{-1} such that $f \star f^{-1} = f^{-1} \star f = e$.
- Since G has only 2 elements, we have only 2 choices: $f^{-1} = e$ or $f^{-1} = f$.
- If $f^{-1} = e$, then $f \star \mathbf{f^{-1}} = f \star \mathbf{e} = f$. But by the definition of inverse, we need $f \star f^{-1} = e$. So we can't have $f^{-1} = e$.

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$. (Therefore $e^{-1} = e$).
- Also $e \star f = f$, and $f \star e = f$.

What does $f \star f$ have to be?

- f has to have an inverse f^{-1} such that $f \star f^{-1} = f^{-1} \star f = e$.
- Since G has only 2 elements, we have only 2 choices: $f^{-1} = e$ or $f^{-1} = f$.
- If $f^{-1} = e$, then $f \star \mathbf{f^{-1}} = f \star \mathbf{e} = f$. But by the definition of inverse, we need $f \star f^{-1} = e$. So we can't have $f^{-1} = e$.
- Thus we must have $f^{-1} = f$.

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$. (Therefore $e^{-1} = e$).
- Also $e \star f = f$, and $f \star e = f$.

What does $f \star f$ have to be?

- f has to have an inverse f^{-1} such that $f \star f^{-1} = f^{-1} \star f = e$.
- Since G has only 2 elements, we have only 2 choices: $f^{-1} = e$ or $f^{-1} = f$.
- If $f^{-1} = e$, then $f \star \mathbf{f^{-1}} = f \star \mathbf{e} = f$. But by the definition of inverse, we need $f \star f^{-1} = e$. So we can't have $f^{-1} = e$.
- Thus we must have $f^{-1} = f$.

So $f \star f = e$.

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$. (Therefore $e^{-1} = e$).
- Also $e \star f = f$, and $f \star e = f$.

What does $f \star f$ have to be?

- f has to have an inverse f^{-1} such that $f \star f^{-1} = f^{-1} \star f = e$.
- Since G has only 2 elements, we have only 2 choices: $f^{-1} = e$ or $f^{-1} = f$.
- If $f^{-1} = e$, then $f \star \mathbf{f^{-1}} = f \star \mathbf{e} = f$. But by the definition of inverse, we need $f \star f^{-1} = e$. So we can't have $f^{-1} = e$.
- Thus we must have $f^{-1} = f$.

So $f \star f = e$. It is straightforward to check closure and associativity, so G is indeed a group.

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$. (Therefore $e^{-1} = e$).
- Also $e \star f = f$, and $f \star e = f$.

What does $f \star f$ have to be?

- f has to have an inverse f^{-1} such that $f \star f^{-1} = f^{-1} \star f = e$.
- Since G has only 2 elements, we have only 2 choices: $f^{-1} = e$ or $f^{-1} = f$.
- If $f^{-1} = e$, then $f \star \mathbf{f^{-1}} = f \star \mathbf{e} = f$. But by the definition of inverse, we need $f \star f^{-1} = e$. So we can't have $f^{-1} = e$.
- Thus we must have $f^{-1} = f$.

So $f \star f = e$. It is straightforward to check closure and associativity, so G is indeed a group.

$G = \{e, f\}$

- Since G must have an identity, either e or f has to be the identity. Let's call the identity e.
- The identity property tells us that $e \star e = e$. (Therefore $e^{-1} = e$).
- Also $e \star f = f$, and $f \star e = f$.

What does $f \star f$ have to be?

- f has to have an inverse f^{-1} such that $f \star f^{-1} = f^{-1} \star f = e$.
- Since G has only 2 elements, we have only 2 choices: $f^{-1} = e$ or $f^{-1} = f$.
- If $f^{-1} = e$, then $f \star \mathbf{f^{-1}} = f \star \mathbf{e} = f$. But by the definition of inverse, we need $f \star f^{-1} = e$. So we can't have $f^{-1} = e$.
- Thus we must have $f^{-1} = f$.

So $f \star f = e$. It is straightforward to check closure and associativity, so G is indeed a group.

Multiplication Table of $G = \{e, f\}$

We can describe G with a multiplication table:

$\star$	e	f
e	e	f
f	f	e

We have constructed the only possible order 2 group, usually called $\mathbb{Z}_2$: the set $\{0, 1\}$ with operation *addition mod 2*:

Multiplication Table of $G = \{e, f\}$

We can describe G with a multiplication table:

$\star$	e	f
e	e	f
f	f	e

We have constructed the only possible order 2 group, usually called $\mathbb{Z}_2$: the set $\{0, 1\}$ with operation *addition mod 2*:

$+_2$	0	1
0	0	1
1	1	0

Multiplication Table of $G = \{e, f\}$

We can describe G with a multiplication table:

$\star$	e	f
e	e	f
f	f	e

We have constructed the only possible order 2 group, usually called $\mathbb{Z}_2$: the set $\{0, 1\}$ with operation *addition mod 2*:

$+_2$	0	1
0	0	1
1	1	0

You can see that G is really the "same thing" as $\mathbb{Z}_2$.

Multiplication Table of $G = \{e, f\}$

We can describe G with a multiplication table:

$\star$	e	f
e	e	f
f	f	e

We have constructed the only possible order 2 group, usually called $\mathbb{Z}_2$: the set $\{0, 1\}$ with operation *addition mod 2*:

$+_2$	0	1
0	0	1
1	1	0

You can see that G is really the "same thing" as $\mathbb{Z}_2$.
We say that G is **isomorphic** to $\mathbb{Z}_2$ and write $G \cong \mathbb{Z}_2$.

Multiplication Table of $G = \{e, f\}$

We can describe G with a multiplication table:

$\star$	e	f
e	e	f
f	f	e

We have constructed the only possible order 2 group, usually called $\mathbb{Z}_2$: the set $\{0, 1\}$ with operation *addition mod 2*:

$+_2$	0	1
0	0	1
1	1	0

You can see that G is really the "same thing" as $\mathbb{Z}_2$.

We say that G is **isomorphic** to $\mathbb{Z}_2$ and write $G \cong \mathbb{Z}_2$.

Multiplication Table of $G = \{e, f\}$

We can describe G with a multiplication table:

$\star$	e	f
e	e	f
f	f	e

We have constructed the only possible order 2 group, usually called $\mathbb{Z}_2$: the set $\{0, 1\}$ with operation *addition mod 2*:

$+_2$	0	1
0	0	1
1	1	0

You can see that G is really the "same thing" as $\mathbb{Z}_2$.
We say that G is **isomorphic** to $\mathbb{Z}_2$ and write $G \cong \mathbb{Z}_2$.

Construct a group of order 3

- With a group, construct the multiplication table for a group of order 3. There is only one possible group (up to isomorphism).

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

We call this group $\mathbb{Z}_3$.

Construct a group of order 3

- With a group, construct the multiplication table for a group of order 3. There is only one possible group (up to isomorphism).

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

We call this group $\mathbb{Z}_3$.

- We have only just begun this concept. If you're interested, play around with constructing a group of order 4. In this case, there are two *different* (non-isomorphic) groups.

Construct a group of order 3

- With a group, construct the multiplication table for a group of order 3. There is only one possible group (up to isomorphism).

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

We call this group $\mathbb{Z}_3$.

- We have only just begun this concept. If you're interested, play around with constructing a group of order 4. In this case, there are two *different* (non-isomorphic) groups.
- And if you haven't already, be sure to sign up for MAT 422 this fall!

Construct a group of order 3

- With a group, construct the multiplication table for a group of order 3. There is only one possible group (up to isomorphism).

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

We call this group $\mathbb{Z}_3$.

- We have only just begun this concept. If you're interested, play around with constructing a group of order 4. In this case, there are two *different* (non-isomorphic) groups.
- And if you haven't already, be sure to sign up for MAT 422 this fall!

Construct a group of order 3

- With a group, construct the multiplication table for a group of order 3. There is only one possible group (up to isomorphism).

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

We call this group $\mathbb{Z}_3$.

- We have only just begun this concept. If you're interested, play around with constructing a group of order 4. In this case, there are two *different* (non-isomorphic) groups.
- And if you haven't already, be sure to sign up for MAT 422 this fall!