

# Abstract Algebra

## Day 1: The $\mathbb{Z}$ Axioms

Nathan Bloomfield

August 23, 2015

# The $\mathbb{Z}$ Axioms

There is a set  $\mathbb{Z}$ , whose elements are called *integers*, which is equipped with two operations  $+$  and  $\cdot$  and a binary relation  $\leq$  which satisfy the following properties.

# The $\mathbb{Z}$ Axioms: Arithmetic

A1.  $a + (b + c) = (a + b) + c$  for all  $a, b, c \in \mathbb{Z}$ .

# The $\mathbb{Z}$ Axioms: Arithmetic

A1.  $a + (b + c) = (a + b) + c$  for all  $a, b, c \in \mathbb{Z}$ .

A2. There is an integer 0 such that  $a + 0 = 0 + a = a$  for all  $a \in \mathbb{Z}$ .

# The $\mathbb{Z}$ Axioms: Arithmetic

- A1.  $a + (b + c) = (a + b) + c$  for all  $a, b, c \in \mathbb{Z}$ .
- A2. There is an integer  $0$  such that  $a + 0 = 0 + a = a$  for all  $a \in \mathbb{Z}$ .
- A3. For every  $a \in \mathbb{Z}$  there is a unique integer, denoted  $-a$ , such that  $a + (-a) = (-a) + a = 0$ .

# The $\mathbb{Z}$ Axioms: Arithmetic

- A1.  $a + (b + c) = (a + b) + c$  for all  $a, b, c \in \mathbb{Z}$ .
- A2. There is an integer  $0$  such that  $a + 0 = 0 + a = a$  for all  $a \in \mathbb{Z}$ .
- A3. For every  $a \in \mathbb{Z}$  there is a unique integer, denoted  $-a$ , such that  $a + (-a) = (-a) + a = 0$ .
- A4.  $a + b = b + a$  for all  $a, b \in \mathbb{Z}$ .

# The $\mathbb{Z}$ Axioms: Arithmetic

- A1.  $a + (b + c) = (a + b) + c$  for all  $a, b, c \in \mathbb{Z}$ .
- A2. There is an integer  $0$  such that  $a + 0 = 0 + a = a$  for all  $a \in \mathbb{Z}$ .
- A3. For every  $a \in \mathbb{Z}$  there is a unique integer, denoted  $-a$ , such that  $a + (-a) = (-a) + a = 0$ .
- A4.  $a + b = b + a$  for all  $a, b \in \mathbb{Z}$ .
- M.  $a(bc) = (ab)c$  for all  $a, b, c \in \mathbb{Z}$ .

# The $\mathbb{Z}$ Axioms: Arithmetic

- A1.  $a + (b + c) = (a + b) + c$  for all  $a, b, c \in \mathbb{Z}$ .
- A2. There is an integer  $0$  such that  $a + 0 = 0 + a = a$  for all  $a \in \mathbb{Z}$ .
- A3. For every  $a \in \mathbb{Z}$  there is a unique integer, denoted  $-a$ , such that  $a + (-a) = (-a) + a = 0$ .
- A4.  $a + b = b + a$  for all  $a, b \in \mathbb{Z}$ .
- M.  $a(bc) = (ab)c$  for all  $a, b, c \in \mathbb{Z}$ .
- D.  $a(b + c) = ab + ac$  and  $(b + c)a = ba + ca$  for all  $a, b, c \in \mathbb{Z}$ .



# The $\mathbb{Z}$ Axioms: Arithmetic

- A1.  $a + (b + c) = (a + b) + c$  for all  $a, b, c \in \mathbb{Z}$ .
- A2. There is an integer  $0$  such that  $a + 0 = 0 + a = a$  for all  $a \in \mathbb{Z}$ .
- A3. For every  $a \in \mathbb{Z}$  there is a unique integer, denoted  $-a$ , such that  $a + (-a) = (-a) + a = 0$ .
- A4.  $a + b = b + a$  for all  $a, b \in \mathbb{Z}$ .
- M.  $a(bc) = (ab)c$  for all  $a, b, c \in \mathbb{Z}$ .
- D.  $a(b + c) = ab + ac$  and  $(b + c)a = ba + ca$  for all  $a, b, c \in \mathbb{Z}$ .
- C.  $ab = ba$  for all  $a, b \in \mathbb{Z}$ .

# The $\mathbb{Z}$ Axioms: Arithmetic

- A1.  $a + (b + c) = (a + b) + c$  for all  $a, b, c \in \mathbb{Z}$ .
- A2. There is an integer 0 such that  $a + 0 = 0 + a = a$  for all  $a \in \mathbb{Z}$ .
- A3. For every  $a \in \mathbb{Z}$  there is a unique integer, denoted  $-a$ , such that  $a + (-a) = (-a) + a = 0$ .
- A4.  $a + b = b + a$  for all  $a, b \in \mathbb{Z}$ .
- M.  $a(bc) = (ab)c$  for all  $a, b, c \in \mathbb{Z}$ .
- D.  $a(b + c) = ab + ac$  and  $(b + c)a = ba + ca$  for all  $a, b, c \in \mathbb{Z}$ .
- C.  $ab = ba$  for all  $a, b \in \mathbb{Z}$ .
- U. There is an integer 1 such that  $a \cdot 1 = 1 \cdot a = a$  for all  $a \in \mathbb{Z}$ .

# The $\mathbb{Z}$ Axioms: Arithmetic

- A1.  $a + (b + c) = (a + b) + c$  for all  $a, b, c \in \mathbb{Z}$ .
- A2. There is an integer 0 such that  $a + 0 = 0 + a = a$  for all  $a \in \mathbb{Z}$ .
- A3. For every  $a \in \mathbb{Z}$  there is a unique integer, denoted  $-a$ , such that  $a + (-a) = (-a) + a = 0$ .
- A4.  $a + b = b + a$  for all  $a, b \in \mathbb{Z}$ .
- M.  $a(bc) = (ab)c$  for all  $a, b, c \in \mathbb{Z}$ .
- D.  $a(b + c) = ab + ac$  and  $(b + c)a = ba + ca$  for all  $a, b, c \in \mathbb{Z}$ .
- C.  $ab = ba$  for all  $a, b \in \mathbb{Z}$ .
- U. There is an integer 1 such that  $a \cdot 1 = 1 \cdot a = a$  for all  $a \in \mathbb{Z}$ .
- Z. If  $ab = 0$ , then either  $a = 0$  or  $b = 0$  for all  $a, b \in \mathbb{Z}$ .

# The $\mathbb{Z}$ Axioms: Order

P1.  $a \leq a$  for all  $a \in \mathbb{Z}$ .

# The $\mathbb{Z}$ Axioms: Order

P1.  $a \leq a$  for all  $a \in \mathbb{Z}$ .

P2. If  $a \leq b$  and  $b \leq a$  then  $a = b$  for all  $a, b \in \mathbb{Z}$ .

# The $\mathbb{Z}$ Axioms: Order

P1.  $a \leq a$  for all  $a \in \mathbb{Z}$ .

P2. If  $a \leq b$  and  $b \leq a$  then  $a = b$  for all  $a, b \in \mathbb{Z}$ .

P3. If  $a \leq b$  and  $b \leq c$  then  $a \leq c$  for all  $a, b, c \in \mathbb{Z}$ .

# The $\mathbb{Z}$ Axioms: Order

- P1.  $a \leq a$  for all  $a \in \mathbb{Z}$ .
- P2. If  $a \leq b$  and  $b \leq a$  then  $a = b$  for all  $a, b \in \mathbb{Z}$ .
- P3. If  $a \leq b$  and  $b \leq c$  then  $a \leq c$  for all  $a, b, c \in \mathbb{Z}$ .
- P4. Either  $a \leq b$  or  $b \leq a$  for all  $a, b \in \mathbb{Z}$ .

# The $\mathbb{Z}$ Axioms: Order

- P1.  $a \leq a$  for all  $a \in \mathbb{Z}$ .
- P2. If  $a \leq b$  and  $b \leq a$  then  $a = b$  for all  $a, b \in \mathbb{Z}$ .
- P3. If  $a \leq b$  and  $b \leq c$  then  $a \leq c$  for all  $a, b, c \in \mathbb{Z}$ .
- P4. Either  $a \leq b$  or  $b \leq a$  for all  $a, b \in \mathbb{Z}$ .
- O1. If  $a \leq b$  then  $a + c \leq b + c$  for all  $a, b, c \in \mathbb{Z}$ .



# The $\mathbb{Z}$ Axioms: Order

- P1.  $a \leq a$  for all  $a \in \mathbb{Z}$ .
- P2. If  $a \leq b$  and  $b \leq a$  then  $a = b$  for all  $a, b \in \mathbb{Z}$ .
- P3. If  $a \leq b$  and  $b \leq c$  then  $a \leq c$  for all  $a, b, c \in \mathbb{Z}$ .
- P4. Either  $a \leq b$  or  $b \leq a$  for all  $a, b \in \mathbb{Z}$ .
- O1. If  $a \leq b$  then  $a + c \leq b + c$  for all  $a, b, c \in \mathbb{Z}$ .
- O2. If  $0 \leq a$  and  $0 \leq b$  then  $0 \leq ab$  for all  $a, b \in \mathbb{Z}$ .

# The $\mathbb{Z}$ Axioms: Order

- P1.  $a \leq a$  for all  $a \in \mathbb{Z}$ .
- P2. If  $a \leq b$  and  $b \leq a$  then  $a = b$  for all  $a, b \in \mathbb{Z}$ .
- P3. If  $a \leq b$  and  $b \leq c$  then  $a \leq c$  for all  $a, b, c \in \mathbb{Z}$ .
- P4. Either  $a \leq b$  or  $b \leq a$  for all  $a, b \in \mathbb{Z}$ .
- O1. If  $a \leq b$  then  $a + c \leq b + c$  for all  $a, b, c \in \mathbb{Z}$ .
- O2. If  $0 \leq a$  and  $0 \leq b$  then  $0 \leq ab$  for all  $a, b \in \mathbb{Z}$ .
- O3.  $0 < 1$ .

# The $\mathbb{Z}$ Axioms: Well-Ordering Property

We call

$$\mathbb{N} = \{a \in \mathbb{Z} \mid 0 \leq a\}$$

the set of *natural numbers*.

# The $\mathbb{Z}$ Axioms: Well-Ordering Property

We call

$$\mathbb{N} = \{a \in \mathbb{Z} \mid 0 \leq a\}$$

the set of *natural numbers*.

**WOP.** Every nonempty subset of  $\mathbb{N}$  has a  $\leq$ -least element.

# The $\mathbb{Z}$ Axioms: Well-Ordering Property

We call

$$\mathbb{N} = \{a \in \mathbb{Z} \mid 0 \leq a\}$$

the set of *natural numbers*.

**WOP.** Every nonempty subset of  $\mathbb{N}$  has a  $\leq$ -least element.

That is, if  $S \subseteq \mathbb{N}$  is not empty, there is a natural number  $m \in S$  such that  $m \leq s$  for all  $s \in S$ .

# Consequences

These 17 axioms uniquely characterize the “integers” we know and love; any other provably true statement about  $\mathbb{Z}$  can be derived from them. For example:

# Consequences

These 17 axioms uniquely characterize the “integers” we know and love; any other provably true statement about  $\mathbb{Z}$  can be derived from them. For example:

- $a \cdot 0 = 0 \cdot a = 0$  for all  $a \in \mathbb{Z}$ .

# Consequences

These 17 axioms uniquely characterize the “integers” we know and love; any other provably true statement about  $\mathbb{Z}$  can be derived from them. For example:

- $a \cdot 0 = 0 \cdot a = 0$  for all  $a \in \mathbb{Z}$ . (Use D)



# Consequences

These 17 axioms uniquely characterize the “integers” we know and love; any other provably true statement about  $\mathbb{Z}$  can be derived from them. For example:

- $a \cdot 0 = 0 \cdot a = 0$  for all  $a \in \mathbb{Z}$ . (Use D)
- $(-1) \cdot a = -a$  for all  $a \in \mathbb{Z}$ .

# Consequences

These 17 axioms uniquely characterize the “integers” we know and love; any other provably true statement about  $\mathbb{Z}$  can be derived from them. For example:

- $a \cdot 0 = 0 \cdot a = 0$  for all  $a \in \mathbb{Z}$ . (Use D)
- $(-1) \cdot a = -a$  for all  $a \in \mathbb{Z}$ .
- If  $a \leq b$  and  $0 \leq c$ , then  $ac \leq bc$ .

# Consequences

These 17 axioms uniquely characterize the “integers” we know and love; any other provably true statement about  $\mathbb{Z}$  can be derived from them. For example:

- $a \cdot 0 = 0 \cdot a = 0$  for all  $a \in \mathbb{Z}$ . (Use D)
- $(-1) \cdot a = -a$  for all  $a \in \mathbb{Z}$ .
- If  $a \leq b$  and  $0 \leq c$ , then  $ac \leq bc$ . (Use D)

# Consequences

These 17 axioms uniquely characterize the “integers” we know and love; any other provably true statement about  $\mathbb{Z}$  can be derived from them. For example:

- $a \cdot 0 = 0 \cdot a = 0$  for all  $a \in \mathbb{Z}$ . (Use D)
- $(-1) \cdot a = -a$  for all  $a \in \mathbb{Z}$ .
- If  $a \leq b$  and  $0 \leq c$ , then  $ac \leq bc$ . (Use D)
- There is no integer  $t$  such that  $0 < t < 1$ .

# Consequences

These 17 axioms uniquely characterize the “integers” we know and love; any other provably true statement about  $\mathbb{Z}$  can be derived from them. For example:

- $a \cdot 0 = 0 \cdot a = 0$  for all  $a \in \mathbb{Z}$ . (Use D)
- $(-1) \cdot a = -a$  for all  $a \in \mathbb{Z}$ .
- If  $a \leq b$  and  $0 \leq c$ , then  $ac \leq bc$ . (Use D)
- There is no integer  $t$  such that  $0 < t < 1$ . (Use WOP;  $t^2 < t$ )

# Consequences

These 17 axioms uniquely characterize the “integers” we know and love; any other provably true statement about  $\mathbb{Z}$  can be derived from them. For example:

- $a \cdot 0 = 0 \cdot a = 0$  for all  $a \in \mathbb{Z}$ . (Use D)
- $(-1) \cdot a = -a$  for all  $a \in \mathbb{Z}$ .
- If  $a \leq b$  and  $0 \leq c$ , then  $ac \leq bc$ . (Use D)
- There is no integer  $t$  such that  $0 < t < 1$ . (Use WOP;  $t^2 < t$ )
- If  $a < b$  then  $a + 1 \leq b$

# Consequences

These 17 axioms uniquely characterize the “integers” we know and love; any other provably true statement about  $\mathbb{Z}$  can be derived from them. For example:

- $a \cdot 0 = 0 \cdot a = 0$  for all  $a \in \mathbb{Z}$ . (Use D)
- $(-1) \cdot a = -a$  for all  $a \in \mathbb{Z}$ .
- If  $a \leq b$  and  $0 \leq c$ , then  $ac \leq bc$ . (Use D)
- There is no integer  $t$  such that  $0 < t < 1$ . (Use WOP;  $t^2 < t$ )
- If  $a < b$  then  $a + 1 \leq b$
- Exactly one of  $a < 0$ ,  $a = 0$ , and  $a > 0$  is true.

# Consequences

These 17 axioms uniquely characterize the “integers” we know and love; any other provably true statement about  $\mathbb{Z}$  can be derived from them. For example:

- $a \cdot 0 = 0 \cdot a = 0$  for all  $a \in \mathbb{Z}$ . (Use D)
- $(-1) \cdot a = -a$  for all  $a \in \mathbb{Z}$ .
- If  $a \leq b$  and  $0 \leq c$ , then  $ac \leq bc$ . (Use D)
- There is no integer  $t$  such that  $0 < t < 1$ . (Use WOP;  $t^2 < t$ )
- If  $a < b$  then  $a + 1 \leq b$
- Exactly one of  $a < 0$ ,  $a = 0$ , and  $a > 0$  is true.
- Every element of  $\mathbb{N}$  is either 0 or of the form  $n + 1$  where  $n \in \mathbb{N}$ .



# Consequences

These 17 axioms uniquely characterize the “integers” we know and love; any other provably true statement about  $\mathbb{Z}$  can be derived from them. For example:

- $a \cdot 0 = 0 \cdot a = 0$  for all  $a \in \mathbb{Z}$ . (Use D)
- $(-1) \cdot a = -a$  for all  $a \in \mathbb{Z}$ .
- If  $a \leq b$  and  $0 \leq c$ , then  $ac \leq bc$ . (Use D)
- There is no integer  $t$  such that  $0 < t < 1$ . (Use WOP;  $t^2 < t$ )
- If  $a < b$  then  $a + 1 \leq b$
- Exactly one of  $a < 0$ ,  $a = 0$ , and  $a > 0$  is true.
- Every element of  $\mathbb{N}$  is either 0 or of the form  $n + 1$  where  $n \in \mathbb{N}$ .
- ... etc.

# Principle of Mathematical Induction

## Theorem (Induction)

*Suppose  $B \subseteq \mathbb{N}$  is a subset such that*

- $0 \in B$  (the Base Case) and
- If  $n \in B$ , then  $n + 1 \in B$  (the Inductive Step).

*Then  $B = \mathbb{N}$ .*

## Theorem (Strong Induction)

*Suppose  $B \subseteq \mathbb{N}$  is a subset such that*

- $0 \in B$  and
- If  $k \in B$  for all  $0 \leq k \leq n$ , then  $n + 1 \in B$ .

*Then  $B = \mathbb{N}$ .*

Proof: Use WOP. These two statements are equivalent in power, but sometimes Strong Induction is convenient.

# Principle of Mathematical Induction: Examples

## Proposition

*For all natural numbers  $n$ , we have*

$$\sum_{i=1}^n i = \frac{n(n+1)}{2}.$$

# Principle of Mathematical Induction: Examples

## Proposition

*For all natural numbers  $n$ , we have*

$$\sum_{i=1}^n i = \frac{n(n+1)}{2}.$$

## Proposition

*For all natural numbers  $n$ , we have*

$$\sum_{i=1}^n \frac{1}{i(i+1)} = \frac{n}{n+1}$$

*(Hint: Use two base cases, 0 and 1.)*