Your Document Title

Your Name

March 23, 2024

Contents

Proof Methods **2**

If then statements 2

If then types 2

Induction Proof 2

Proof by contradiction 3

Definitions **4**

Equality $=$ 4

Inequality $\neq$ 4

In the set of $\in$ 4

Not in the set of $\notin$ 4

Divisibility 4

2 and other integers 4

Even Integers 4

Subtraction 4

Power 4

Sum 5

Product 5

Non-negative integer ($\mathbb{Z}_{\geq 0}$) 5

Factorial 5

Subset ($\subseteq$) 5

The Empty Set ($\emptyset$) 5

Equal Sets ($=$) 5

Functions 5

Proof Methods

If then statements

Format:

Proof. **If A, then B:**

1. **Assume A.**
2. **Show that assuming A leads to B.**
3. **Therefore, B is concluded from A.**

□

Example:

Proof. **If $m = 1$, then $m + 0 = 1$.**

1. **Assume $m = 1$.**
2. **Considering $m = 1$, we have $1 + 0 = 1$.**
3. **This simplifies to $1 = 1$, which is true.**

□

If then types

Different types of implications and their meaning:

- $A \Rightarrow B$: "If it is Wednesday, Dr. Beck will get a cup of coffee from the student union."
- $B \Rightarrow A$ (Converse): "If Dr. Beck got a cup of coffee from the student union, then it is Wednesday."
- $A \Leftrightarrow B$ (Bi-conditional): "It is Wednesday if and only if Dr. Beck got a cup of coffee from the student union."
- $\neg B \Rightarrow \neg A$ (Contrapositive): "If Dr. Beck did not get a cup of coffee from the student union, then it is not Wednesday."

Induction Proof

Format:

Proof. **Prove that $F(x)$ is true for all $x \in A$:**

1. **Base case:** Show $F(a)$ is true, where a is the smallest element in set A.
2. **Induction step:** Assume $F(k)$ is true for an arbitrary $k \in A$. Show that $F(k) \Rightarrow F(k+1)$.
3. **Therefore, $F(x+1)$ is true for all $x \in A$.**

□

Example:

Proof. **For all $n \in \mathbb{N}$, $n = n$:**

1. **Base case ($n = 1$):** $1 = 1$ is true.
2. **Induction step:** Assume $n = n$ is true for an arbitrary natural number n. Show that this implies $n + 1 = n + 1$.
3. By the induction hypothesis, $n = n$. Adding 1 to both sides, $n + 1 = n + 1$, which holds true.

□

Proof by contradiction

Format:

Proof. **Prove that A is true by contradiction:**

1. Assume **not** A.
2. Show that this assumption leads to a contradiction (something that we know is false).
3. Therefore, A must be true.

$\square$

Different Negations

1. **AND $\Rightarrow$ OR:** If A and B, then **not** A or **not** B.

   Example: Dr. Beck is 5 ft tall and single $\Rightarrow$ Dr. Beck is **not** 5 ft tall or is **not** single.
2. **OR $\Rightarrow$ AND:** If A or B, then **not** A and **not** B.

   Example: Dr. Beck will drink a coffee or it is Wednesday $\Rightarrow$ Dr. Beck will **not** drink a coffee and it is **not** Wednesday.
3. **If, then $\Rightarrow$ AND:** If A, then B implies **not** A and **not** B.

   *If it is Monday, then Dr. Beck is on campus $\Rightarrow$ It is **not** Monday and Dr. Beck is **not** on campus.*
4. **For all $\Rightarrow$ There exists:** For all m, A is true implies there exists an m, A is **not** true.

   *For all $m \in \mathbb{Z}$, m is even $\Rightarrow$ There exists $m \in \mathbb{Z}$, m is **not** even.*
5. **There exists $\Rightarrow$ For all:** There exists an m, A is true implies for all m, A is **not** true.

   There exists an $m \in \mathbb{Z}$, $m + 1 = 0.5 \Rightarrow$ For all $m \in \mathbb{Z}$, $m + 1 \neq 0$.

Example:

Proof. **There is no $x \in \mathbb{N}$ that satisfies the equation $1 - x = 0 \cdot x$.**

1. Assume by way of contradiction that such an x exists in $\mathbb{N}$.
2. Since $x \neq 0$ for any $x \in \mathbb{N}$, cancelling x from both sides of the equation $1 - x = 0 \cdot x$ leads to $0 = 1$.
3. Since $0 \neq 1$ is a true mathematical contradiction, the initial statement is proven to be true by contradiction.

$\square$

Definitions

Equality =

The symbol = means **equals**. To say $m = n$ means that m and n are the same number. Some properties are:

i. $m = m$ (**reflexivity**)

ii. If $m = n$ then $n = m$ (**symmetry**)

iii. If $m = n$ and $n = p$ then $m = p$ (**transitivity**)

iv. If $m = n$, then n can be substituted for m in any statement without changing the meaning (**replacement**)

Inequality $\neq$

The symbol $\neq$ means **is not equal to**. To say $m \neq n$ means that m and n are different numbers. Note that $\neq$ satisfies **symmetry**, but not **transitivity** and **reflexivity**.

In the set of $\in$

The symbol $\in$ means **is an element of**. For example, $0 \in \mathbb{Z}$ means "0 is an element of the set $\mathbb{Z}$."

Not in the set of $\notin$

The symbol $\notin$ means **is not an element of**. For example, $0.5 \notin \mathbb{Z}$ means "0.5 is not an element of the set $\mathbb{Z}$."

Divisibility

When m and n are integers, we say m is divisible by n (or alternatively, n divides m) if there exists $j \in \mathbb{Z}$ such that $m = jn$. We use the notation $n|m$.

2 and other integers

2 is defined as $2 = 1 + 1$ and **3** is $2 + 1$ and so on.

Even Integers

Even integers are defined to be those integers that are divisible by 2. That is, $x = 2j$, where $j \in \mathbb{Z}$.

Subtraction

Subtraction is defined as $m - n$ is defined to be $m + (-n)$.

Number Theory

Power

Let b be a fixed integer. We define b^k for all integers $k \geq 0$ by:

1. $\boldsymbol{b^0 := 1}$
2. Assuming b^n is defined, let $\boldsymbol{b^{n+1} := b^n \cdot b}$

Sum

Let $(x_j)_{j=1}^{\infty}$ be a sequence of integers. $(x_j)_{j=1}^{3} = \{1, 2, 3\}$. For each $k \in \mathbb{N}$, we want to define an integer called $\Sigma_{j=1}^{k} x_j$:

1. Define $\mathbf{\Sigma_{j=1}^{1} x_j}$ to be x_1
2. Assuming $\Sigma_{j=1}^{n} x_j$ is already defined, we define $\mathbf{\Sigma_{j=1}^{n+1} x_j}$ to be $\Sigma_{j=1}^{n} x_j + x_{n+1}$

Product

Let $(x_j)_{j=1}^{\infty}$ be a sequence of integers. $(x_j)_{j=1}^{3} = \{1, 2, 3\}$. For each $k \in \mathbb{N}$, we want to define an integer called $\Pi_{j=1}^{k} x_j$:

1. Define $\mathbf{\Pi_{j=1}^{1} x_j}$ to be x_1
2. Assuming $\Pi_{j=1}^{n} x_j$ is already defined, we define $\mathbf{\Pi_{j=1}^{n+1} x_j}$ to be $\Pi_{j=1}^{n} x_j \cdot x_{n+1}$

Non-negative integer ($\mathbb{Z}_{\geq 0}$)

$\mathbb{Z}_{\geq 0} := \{m \in \mathbb{Z} : m \geq 0\}$

Factorial

We define $k!$ ("k factorial") for all integers $k \geq 0$ by:

1. Define $\mathbf{0}! := \mathbf{1}$
2. Assuming $n!$ is defined (where $n \in \mathbb{Z}_{\geq 0}$), define $(\mathbf{n}+\mathbf{1})! := (\mathbf{n}!) \cdot (\mathbf{n}+\mathbf{1})$

Subset ($\subseteq$)

$A \subseteq B$ means that if $x \in A$, then $x \in B$

The Empty Set ($\emptyset$)

The empty set is defined as a set that contains no elements.

Equal Sets ($=$)

The set A is equal to B means that $A \subseteq B$ and $B \subseteq A$. In order to prove two sets are equal, you have to complete two proofs.

Functions

Informal Definition

A function consists of:

- a set A called the **domain** of the function
- a set B called the **codomain** of the function
- a rule f that assigns to each $a \in A$ an element $f(a) \in B$. Shorthand for this is $f : A \to B$

Abstract Definition

A function with domain A and codomain B is a subset of Γ of $A \times B$ such that for each $a \in A$, there is one and only one element of Γ whose first entry is a. If $(a, b) \in \Gamma$, we write $b = f(a)$.

Axioms

Axioms of Integers

The axioms of integers describe the basic properties that define the structure of the set of integers ($\mathbb{Z}$).

Axiom 1.1 (Commutativity and Associativity)

- For any integers m, n, the operation of addition is commutative: $m + n = n + m$.
- For any integers m, n, p, the operation of addition is associative: $(m + n) + p = m + (n + p)$.
- For any integers m, n, p, the distributive property connects the operations of multiplication and addition: $m \cdot (n + p) = m \cdot n + m \cdot p$.
- For any integers m, n, the operation of multiplication is commutative: $m \cdot n = n \cdot m$.
- For any integers m, n, p, the operation of multiplication is associative: $(m \cdot n) \cdot p = m \cdot (n \cdot p)$.

Axiom 1.2 (Identity Elements)

- There exists an integer 0 such that for any integer m, adding 0 to m leaves it unchanged: $m + 0 = m$.
- There exists an integer 1 ($1 \neq 0$) such that for any integer m, multiplying m by 1 leaves it unchanged: $m \cdot 1 = m$.

Axiom 1.3 (Additive Inverse)

For each integer m, there exists an integer denoted by $-m$ such that their sum is 0: $m + (-m) = 0$.

Axiom 1.4 (Cancellation Law)

For any integers m, n, p, if $m \neq 0$ and $m \cdot n = m \cdot p$, then $n = p$.

Proof Example

Proof. If m is an integer and $m \cdot 0 = 0$, then $m = m$.

- Consider an integer m.
- Multiplying by 0 gives $m \cdot 0 = 0$.
- Since $m \cdot 0 = 0$, by the property of zero in multiplication, we have $m = m$.
- Thus, the statement is proven. $\square$