MATH301GWAR
REFERENCES AND PROOFS

Marty Martin

March 25, 2024

Contents

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.

□

Different Negations

1. **AND ⇒ OR:** If A and B, then **not** A or **not** B.

   Example: Dr. Beck is 5 ft tall and single ⇒ Dr. Beck is **not** 5 ft tall or is **not** single.

2. **OR ⇒ AND:** If A or B, then **not** A and **not** B.

   Example: Dr. Beck will drink a coffee or it is Wednesday ⇒ Dr. Beck will **not** drink a coffee and it is **not** Wednesday.

3. **If, then ⇒ AND:** If A, then B implies **not** A and **not** B.

   *If it is Monday, then Dr. Beck is on campus ⇒ It is **not** Monday and Dr. Beck is **not** on campus.*

4. **For all ⇒ 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 ⇒ There exists $m \in \mathbb{Z}$, m is **not** even.*

5. **There exists ⇒ For all:** There exists an m, A is true implies for all m, A is **not** true.

   There exists an $m \in \mathbb{Z}$, $m + 1 = 0.5$ ⇒ 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.

□

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 $b = f(a)$.

Theorems

Theorem 2.17 (Principle of Mathematical Induction - First Form):

Let $P(k)$ be a statement depending on a variable $k \in \mathbb{N}$. In order to prove the statement "P(k) is true for all $k \in \mathbb{N}$," it is sufficient to prove:

1. $P(1)$ is true, and
2. For any given $n \in \mathbb{N}$, if $P(n)$ is true, then $P(n+1)$ is true.

Theorem 2.25 (Principle of Mathematical Induction — First Form Revisited):

Let $P(k)$ be a statement, depending on a variable $k \in \mathbb{Z}$, that makes sense for all $k \geq m$, where m is a fixed integer. In order to prove the statement "P(k) is true for all $k \geq m$," it is sufficient to prove:

1. $P(m)$ is true, and
2. For any given $n \geq m$, if $P(n)$ is true then $P(n+1)$ is true.

Theorem 2.32 (Well-Ordering Principle):

Every nonempty subset of $\mathbb{N}$ has a smallest element.

Theorem 4.4:

A legitimate method of describing a sequence $(y_j)_{j=m}^{\infty}$ is:

1. to name y_m, and
2. to state a formula describing y_{n+1} in terms of y_n, for each $n \geq m$.

Theorem 4.19:

Let $k, m \in \mathbb{Z}_{\geq 0}$, where $m \leq k$. Then $m!(k-m)!$ divides $k!$.

Theorem 4.21 (Binomial theorem for integers):

If $a, b \in \mathbb{Z}$ and $k \in \mathbb{Z}_{\geq 0}$ then $(a+b)^k = \displaystyle\sum_{m=0}^{k} \binom{k}{m} a^{k-m} b^m$

Theorem 4.24 (Principle of mathematical induction —second form):

Let $P(k)$ be a statement depending on a variable $k \in \mathbb{N}$. In order to prove the statement "$P(k)$ is true for all $k \in \mathbb{N}$" it is sufficient to prove:

1. $P(1)$ is true and
2. if $P(j)$ is true for all integers j such that $1 \leq j \leq n$, then $P(n+1)$ is true

Theorem 5.15 (De Morgan's laws):

Given two subsets $A, B \subseteq X$,

$$(A \cap B)^c = A^c \cup B^c \quad \text{and} \quad (A \cup B)^c = A^c \cap B^c$$

Collary

Corollary 1.21

$(-1)(-1) = 1$.

Proof.

$$\begin{aligned}(-1)(-1) &= 1 \cdot 1 && \text{(Proposition 1.20 with } m = n = 1\text{)} \\ &= 1 && \text{(Axiom 1.3)}\end{aligned}$$

□

Corollary 4.20:

For $1 \leq m \leq k$, $\binom{k+1}{m} = \binom{k}{m-1} + \binom{k}{m}$

Corollary 4.22:

For $k \in \mathbb{Z}_{\geq 0}$, $\displaystyle\sum_{m=0}^{k} \binom{k}{m} = 2^k$

Axioms

Axiom 1.1: Properties of Integers

If m, n, and p are integers, then:

(i) $m + n = n + m$ (**commutativity of addition**)

(ii) $(m + n) + p = m + (n + p)$ (**associativity of addition**)

(iii) $m \cdot (n + m) = m \cdot n + m \cdot p$ (**distributivity**)

(iv) $m \cdot n = n \cdot m$ (**commutativity of multiplication**)

(v) $(m \cdot n) \cdot p = m \cdot (n \cdot p)$ (**associativity of multiplication**)

Axiom 1.2: Identity Element for Addition

There exists an integer 0 such that whenever $m \in \mathbb{Z}$, $m + 0 = m$ (**identity element for addition**).

Axiom 1.3: Identity Element for Multiplication

There exists an integer 1 such that $1 \neq 0$ and whenever $m \in \mathbb{Z}$, $m \cdot 1 = m$ (**identity element for multiplication**).

Axiom 1.4: Additive Inverse

For each $m \in \mathbb{Z}$, there exists an integer, denoted by $-m$, such that $m + (-m) = 0$ (**additive inverse**).

Axiom 1.5: Cancellation

Let m, n, and p be integers. If $m \cdot n = m \cdot p$ and $m \neq 0$, then $n = p$ (**cancellation**).

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. □

Axiom 2.1:

There exists a subset $\mathbb{N} \subseteq \mathbb{Z}$ with the following properties:

(i) If $m, n \in \mathbb{N}$ then $m + n \in \mathbb{N}$.

(ii) If $m, n \in \mathbb{N}$ then $mn \in \mathbb{N}$.

(iii) $0 \notin \mathbb{N}$.

(iv) For every $m \in \mathbb{Z}$, we have $m \in \mathbb{N}$ or $m = 0$ or $-m \in \mathbb{N}$.

Propositions

Chapter 1: Propositions

Proposition 1.6

If m, n, and p are integers, then $(m+n)\cdot p = mp + np$.

Proof. Let m, n, and p be arbitrary integers.

$$\begin{aligned}(m+n)\cdot p &= m\cdot p + n\cdot p && \text{(Axiom 1.1(iii))}\\ &= mp + np\end{aligned}$$

Therefore, $(m+n)\cdot p = mp + np$ for all integers m, n, and p. □

Proposition 1.7

If m is an integer, then $0 + m = m$ and $1\cdot m = m$.

Proof. Let m be an arbitrary integer.

$$0 + m = m \qquad \text{(Axiom 1.2)}$$

$$1\cdot m = m \qquad \text{(Axiom 1.3)}$$

Therefore, for any integer m, $0 + m = m$ and $1\cdot m = m$. □

Proposition 1.8

If m is an integer, then $(-m) + m = 0$.

Proof. Let m be an arbitrary integer.

$$(-m) + m = 0 \qquad \text{(Axiom 1.4)}$$

Therefore, for any integer m, $(-m) + m = 0$. □

Proposition 1.9

Let m, n, and p be integers. If $m + n = m + p$, then $n = p$.

Proof. Let m, n, and p be arbitrary integers, and suppose $m + n = m + p$.

$$\begin{aligned}m + n &= m + p && \text{(given)}\\ (-m) + (m+n) &= (-m) + (m+p) && \text{(Axiom 1.1(i))}\\ ((-m)+m) + n &= ((-m)+m) + p && \text{(Axiom 1.1(ii))}\\ 0 + n &= 0 + p && \text{(Axiom 1.4)}\\ n &= p && \text{(Axiom 1.2)}\end{aligned}$$

Therefore, if $m + n = m + p$ for integers m, n, and p, then $n = p$. □

Proposition 1.10

Let m, x_1, $x_2 \in \mathbb{Z}$. If m, x_1, x_2 satisfy the equation $m + x_1 = 0$ and $m + x_2 = 0$, then $x_1 = x_2$.

Proof. Let $m, x_1, x_2 \in \mathbb{Z}$. Suppose $m + x_1 = 0$ and $m + x_2 = 0$.

$$\begin{aligned} m + x_1 &= 0 && \text{(given)} \\ (-m) + (m + x_1) &= (-m) + 0 && \text{(Axiom 1.1(i))} \\ ((-m) + m) + x_1 &= (-m) + 0 && \text{(Axiom 1.1(ii))} \\ 0 + x_1 &= -m && \text{(Axiom 1.4)} \\ x_1 &= -m && \text{(Axiom 1.2)} \end{aligned}$$

Similarly, from $m + x_2 = 0$, we can derive $x_2 = -m$.

$$\begin{aligned} & x_1 = -m && \text{(derived)} \\ & x_2 = -m && \text{(derived)} \\ & x_1 = x_2 && \text{(transitive property of equality)} \end{aligned}$$

Therefore, if $m, x_1, x_2 \in \mathbb{Z}$ such that $m + x_1 = 0$ and $m + x_2 = 0$, then $x_1 = x_2$. □

Proposition 1.11

If m, n, p, and q are integers, then:

(i) $(m + n)(p + q) = (mp + np) + (mq + nq)$.

(ii) $m + (n + (p + q)) = (m + n) + (p + q) = ((m + n) + p) + q$.

(iii) $m + (n + p) = (p + m) + n$.

(iv) $m(np) = p(mn)$.

(v) $m(n + (p + q)) = (mn + mp) + mq$.

(vi) $(m(n + p))q = (mn)q + m(pq)$.

Proof. Let m, n, p, and q be arbitrary integers.

(i) $(m + n)(p + q) = (mp + np) + (mq + nq)$

$$\begin{aligned} (m + n)(p + q) &= mp + mq + np + nq && \text{(Axiom 1.1(iii))} \\ &= (mp + np) + (mq + nq) && \text{(Axiom 1.1(ii))} \end{aligned}$$

(ii) $m + (n + (p + q)) = (m + n) + (p + q) = ((m + n) + p) + q$

$$\begin{aligned} m + (n + (p + q)) &= (m + n) + (p + q) && \text{(Axiom 1.1(ii))} \\ &= ((m + n) + p) + q && \text{(Axiom 1.1(ii))} \end{aligned}$$

(iii) $m + (n + p) = (p + m) + n$

$$\begin{aligned} m + (n + p) &= (m + n) + p && \text{(Axiom 1.1(ii))} \\ &= (n + m) + p && \text{(Axiom 1.1(i))} \\ &= (p + m) + n && \text{(Axiom 1.1(i))} \end{aligned}$$

(iv) $m(np) = p(mn)$

$$\begin{aligned} m(np) &= (mn)p && \text{(Axiom 1.1(v))} \\ &= (nm)p && \text{(Axiom 1.1(iv))} \\ &= p(mn) && \text{(Axiom 1.1(v))} \end{aligned}$$

(v) $m(n+(p+q)) = (mn+mp)+mq$

$$\begin{aligned} m(n+(p+q)) &= mn+m(p+q) && \text{(Axiom 1.1(iii))} \\ &= mn+(mp+mq) && \text{(Axiom 1.1(iii))} \\ &= (mn+mp)+mq && \text{(Axiom 1.1(ii))} \end{aligned}$$

(vi) $(m(n+p))q = (mn)q+m(pq)$

$$\begin{aligned} (m(n+p))q &= m((n+p)q) && \text{(Axiom 1.1(v))} \\ &= m(nq+pq) && \text{(Axiom 1.1(iii))} \\ &= (mnq)+(mpq) && \text{(Axiom 1.1(iii))} \\ &= (mn)q+m(pq) && \text{(Axiom 1.1(v))} \end{aligned}$$

□

Proposition 1.12

Let $x \in \mathbb{Z}$. If x has the property that for each integer m, $m+x=m$, then $x=0$.

Proof. Let $x \in \mathbb{Z}$. Suppose for each integer m, $m+x=m$.

$$\begin{aligned} 0+x &= 0 && \text{(substituting } m=0\text{)} \\ x &= 0 && \text{(Axiom 1.2)} \end{aligned}$$

Therefore, if $x \in \mathbb{Z}$ has the property that for each integer m, $m+x=m$, then $x=0$. □

Proposition 1.13

Let $x \in \mathbb{Z}$. If x has the property that there exists an integer m such that $m+x=m$, then $x=0$.

Proof. Let $x \in \mathbb{Z}$. Suppose there exists an integer m such that $m+x=m$.

$$\begin{aligned} m+x &= m && \text{(given)} \\ (-m)+(m+x) &= (-m)+m && \text{(Axiom 1.1(i))} \\ ((-m)+m)+x &= (-m)+m && \text{(Axiom 1.1(ii))} \\ 0+x &= 0 && \text{(Axiom 1.4)} \\ x &= 0 && \text{(Axiom 1.2)} \end{aligned}$$

Therefore, if $x \in \mathbb{Z}$ has the property that there exists an integer m such that $m+x=m$, then $x=0$. □

Proposition 1.14

For all $m \in \mathbb{Z}$, $m \cdot 0 = 0 = 0 \cdot m$.

Proof. Let $m \in \mathbb{Z}$.

$$\begin{aligned} m \cdot 0 &= \underbrace{m+m+\cdots+m}_{0\text{ times}} && \text{(definition of multiplication)} \\ &= 0 && \text{(additive identity)} \end{aligned}$$

Similarly,

$$\begin{aligned} 0 \cdot m &= \underbrace{0+0+\cdots+0}_{m\text{ times}} && \text{(definition of multiplication)} \\ &= 0 && \text{(additive identity)} \end{aligned}$$

Therefore, for all $m \in \mathbb{Z}$, $m \cdot 0 = 0 = 0 \cdot m$. □

Proposition 1.16

If m and n are even integers, then so are $m+n$ and mn.

Proof. Let m and n be even integers. Then, by the definition of even integers, $2 \mid m$ and $2 \mid n$.

$$\begin{aligned} m &= 2j && \text{(definition of divisibility, for some } j \in \mathbb{Z}\text{)} \\ n &= 2k && \text{(definition of divisibility, for some } k \in \mathbb{Z}\text{)} \end{aligned}$$

Part 1: $m+n$ is even.

$$\begin{aligned} m+n &= 2j+2k && \text{(substitution)} \\ &= 2(j+k) && \text{(Axiom 1.1(iii))} \end{aligned}$$

Since $j+k \in \mathbb{Z}$, we have $2 \mid (m+n)$, so $m+n$ is even.

Part 2: mn is even.

$$\begin{aligned} mn &= (2j)(2k) && \text{(substitution)} \\ &= 2(2jk) && \text{(Axiom 1.1(v))} \end{aligned}$$

Since $2jk \in \mathbb{Z}$, we have $2 \mid mn$, so mn is even.

Therefore, if m and n are even integers, then $m+n$ and mn are also even. □

Proposition 1.17

(i) 0 is divisible by every integer.

(ii) If m is an integer not equal to 0, then m is not divisible by 0.

Proof. (i) Let m be an arbitrary integer.

$$m \cdot 0 = 0 \qquad \text{(Proposition 1.14)}$$

Thus, by the definition of divisibility, $m \mid 0$ for all $m \in \mathbb{Z}$.

(ii) Let m be a non-zero integer.

$$\begin{aligned} m \cdot 0 &= 0 && \text{(Proposition 1.14)} \\ m \cdot 0 &\neq m && \text{(since } m \neq 0\text{)} \end{aligned}$$

Therefore, by the definition of divisibility, $0 \nmid m$ for all non-zero integers m. □

Proposition 1.18

Let $x \in \mathbb{Z}$. If x has the property that for all $m \in \mathbb{Z}$, $mx = m$, then $x = 1$.

Proof. Let $x \in \mathbb{Z}$. Suppose for all $m \in \mathbb{Z}$, $mx = m$.

$$\begin{aligned} 1 \cdot x &= 1 && \text{(substituting } m = 1\text{)} \\ x &= 1 && \text{(Axiom 1.3)} \end{aligned}$$

Thus, if $x \in \mathbb{Z}$ has the property that for all $m \in \mathbb{Z}$, $mx = m$, then $x = 1$. □

Proposition 1.19

Let $x \in \mathbb{Z}$. If x has the property that for some nonzero $m \in \mathbb{Z}$, $mx = m$, then $x = 1$.

Proof. Let $x \in \mathbb{Z}$. Suppose there exists a nonzero $m \in \mathbb{Z}$ such that $mx = m$.

$$\begin{aligned} mx &= m && \text{(given)} \\ m^{-1}(mx) &= m^{-1}m && \text{(multiplying both sides by } m^{-1}\text{)} \\ (m^{-1}m)x &= m^{-1}m && \text{(Axiom 1.1(v))} \\ 1 \cdot x &= 1 && \text{(multiplicative inverse)} \\ x &= 1 && \text{(Axiom 1.3)} \end{aligned}$$

Therefore, if $x \in \mathbb{Z}$ has the property that there exists a nonzero $m \in \mathbb{Z}$ such that $mx = m$, then $x = 1$. □

Proposition 1.20

For all $m, n \in \mathbb{Z}$, $(-m)(-n) = mn$.

Proof. Let $m, n \in \mathbb{Z}$.

$$\begin{aligned} (-m)(-n) &= ((-1) \cdot m)((-1) \cdot n) && \text{(definition of negation)} \\ &= ((-1) \cdot (-1))(m \cdot n) && \text{(Axiom 1.1(iv))} \\ &= (-1) \cdot ((-1) \cdot (m \cdot n)) && \text{(Axiom 1.1(v))} \\ &= (-1) \cdot ((-1) \cdot m) \cdot n && \text{(Axiom 1.1(v))} \\ &= (-1) \cdot (-m) \cdot n && \text{(definition of negation)} \\ &= m \cdot n && \text{(definition of negation)} \\ &= mn && \text{(simplification of notation)} \end{aligned}$$

Thus, for all $m, n \in \mathbb{Z}$, $(-m)(-n) = mn$. □

Proposition 1.22

(i) For all $m \in \mathbb{Z}$, $-(m) = m$.

(ii) $-0 = 0$.

Proof. (i) Let $m \in \mathbb{Z}$.

$$\begin{aligned} -(m) &= (-1)(-m) && \text{(Proposition 1.25(ii))} \\ &= (-1)(-1)m && \text{(Proposition 1.25(iii))} \\ &= 1 \cdot m && \text{(Corollary 1.21)} \\ &= m && \text{(Axiom 1.3)} \end{aligned}$$

(ii) $-0 = 0$.

$$\begin{aligned} -0 &= (-1) \cdot 0 && \text{(Proposition 1.25(ii))} \\ &= 0 && \text{(Proposition 1.14)} \end{aligned}$$

□

Proposition 1.23

Given $m, n \in \mathbb{Z}$, there exists one and only one $x \in \mathbb{Z}$ such that $m + x = n$.

Proof. Let $m, n \in \mathbb{Z}$. Consider the integer $x = n + (-m)$.

$$\begin{aligned}
m + x &= m + (n + (-m)) && \text{(substitution)} \\
&= (m + n) + (-m) && \text{(Axiom 1.1(ii))} \\
&= (n + m) + (-m) && \text{(Axiom 1.1(i))} \\
&= n + (m + (-m)) && \text{(Axiom 1.1(ii))} \\
&= n + 0 && \text{(Axiom 1.4)} \\
&= n && \text{(Axiom 1.2)}
\end{aligned}$$

Thus, there exists an integer x such that $m + x = n$.

To prove uniqueness, suppose there exist $x_1, x_2 \in \mathbb{Z}$ such that $m + x_1 = n$ and $m + x_2 = n$.

$$\begin{aligned}
m + x_1 &= n && \text{(given)} \\
m + x_2 &= n && \text{(given)} \\
m + x_1 &= m + x_2 && \text{(transitive property of equality)} \\
x_1 &= x_2 && \text{(Proposition 1.9)}
\end{aligned}$$

Therefore, the integer x such that $m + x = n$ is unique. □

Proposition 1.24

Let $x \in \mathbb{Z}$. If $x \cdot x = x$ then $x = 0$ or 1.

Proof. Let $x \in \mathbb{Z}$ and suppose $x \cdot x = x$.

$$\begin{aligned}
x \cdot x &= x && \text{(given)} \\
x \cdot x - x &= x - x && \text{(subtracting } x \text{ from both sides)} \\
x(x - 1) &= 0 && \text{(Axiom 1.1(iii))} \\
\text{Case 1: } x &= 0 && \\
\text{Case 2: } x - 1 &= 0 && \\
x &= 1 && \text{(adding 1 to both sides)}
\end{aligned}$$

Therefore, if $x \in \mathbb{Z}$ satisfies $x \cdot x = x$, then $x = 0$ or 1. □

Proposition 1.25

(i) $-(m + n) = (-m) + (-n)$.

(ii) $-m = (-1)m$.

(iii) $(-m)n = m(-n) = -(mn)$.

Proof. Let $m, n \in \mathbb{Z}$.

(i)

$$\begin{aligned}
-(m + n) &= (-1) \cdot (m + n) && \text{(definition of negation)} \\
&= (-1) \cdot m + (-1) \cdot n && \text{(Axiom 1.1(iii))} \\
&= (-m) + (-n) && \text{(definition of negation)}
\end{aligned}$$

(ii)

$$-m = (-1) \cdot m \qquad \text{(definition of negation)}$$

(iii)

$$\begin{aligned}
(-m)n &= ((-1)\cdot m)n && \text{(definition of negation)}\\
&= (-1)\cdot(mn) && \text{(Axiom 1.1(v))}\\
&= -(mn) && \text{(definition of negation)}
\end{aligned}$$

Similarly,

$$\begin{aligned}
m(-n) &= m((-1)\cdot n) && \text{(definition of negation)}\\
&= (m\cdot(-1))n && \text{(Axiom 1.1(iv))}\\
&= (-1)\cdot(mn) && \text{(Axiom 1.1(v))}\\
&= -(mn) && \text{(definition of negation)}
\end{aligned}$$

□

Proposition 1.26

Let $m, n \in \mathbb{Z}$. If $mn = 0$, then $m = 0$ or $n = 0$.

Proof. Let $m, n \in \mathbb{Z}$ and suppose $mn = 0$. **Case 1:** $m = 0$ If $m = 0$, then $m \cdot n = 0$ for any integer n by Proposition 1.14, so the statement holds.

Case 2: $m \neq 0$

$$\begin{aligned}
mn &= 0 && \text{(given)}\\
m^{-1}(mn) &= m^{-1}\cdot 0 && \text{(multiplying both sides by } m^{-1}\text{)}\\
(m^{-1}m)n &= 0 && \text{(Axiom 1.1(v))}\\
1\cdot n &= 0 && \text{(multiplicative inverse)}\\
n &= 0 && \text{(Axiom 1.3)}
\end{aligned}$$

Thus, if $m \neq 0$, then $n = 0$.

Therefore, if $mn = 0$, then $m = 0$ or $n = 0$. □

Proposition 1.27

(i) $(m-n)+(p-q) = (m+p)-(n+q)$.

(ii) $(m-n)-(p-q) = (m+q)-(n+p)$.

(iii) $(m-n)(p-q) = (mp+nq)-(mq+np)$.

(iv) $m-n = p-q$ if and only if $m+q = n+p$.

(v) $(m-n)p = mp-np$.

Chapter 2: Propositions

Proposition 2.2:

For every $m \in \mathbb{Z}$, one and only one of the following is true: $m \in \mathbb{N}$, $-m \in \mathbb{N}$, or $m = 0$.

Proposition 2.3:

$1 \in \mathbb{N}$.

Proposition 2.4:

Let $m, n, p \in \mathbb{Z}$. If $m < n$ and $n < p$, then $m < p$.

Proposition 2.5:

For each $n \in \mathbb{N}$, there exists $m \in \mathbb{N}$ such that $m > n$.

Proposition 2.6:

Let $m, n \in \mathbb{Z}$. If $m \leq n \leq m$, then $m = n$.

Proposition 2.7:

(i) If $m < n$, then $m + p < n + p$.

(ii) If $m < n$ and $p < q$, then $m + p < n + q$.

(iii) If $0 < m < n$ and $0 < p \leq q$, then $mp < nq$.

(iv) If $m < n$ and $p < 0$, then $np < mp$.

Proposition 2.8:

Let $m, n \in \mathbb{Z}$. Exactly one of the following is true: $m < n$, $m = n$, $m > n$.

Proposition 2.9:

Let $m \in \mathbb{Z}$. If $m \neq 0$ then $m^2 \in \mathbb{N}$.

Proposition 2.10:

The equation $x^2 = -1$ has no solution in $\mathbb{Z}$.

Proposition 2.11:

Let $m \in \mathbb{N}$ and $n \in \mathbb{Z}$. If $mn \in \mathbb{N}$, then $n \in \mathbb{N}$.

Proposition 2.12:

For all $m, n, p \in \mathbb{Z}$:

(i) $-m < -n$ if and only if $m > n$.

(ii) If $p > 0$ and $mp < np$ then $m < n$.

(iii) If $p < 0$ and $mp < np$ then $n < m$.

(iv) If $m \leq m$ and $0 \leq p$ then $mp \leq np$.

Proposition 2.13:

$\mathbb{N} = \{n \in \mathbb{Z} : n > 0\}$.

Proposition 2.14:

(i) $1 \in \mathbb{N}$.

(ii) If $n \in \mathbb{N}$, then $n + 1 \in \mathbb{N}$.

Axiom 2.15 (Induction Axiom):

If a subset $A \subseteq \mathbb{Z}$ satisfies:

1. $1 \in A$, and
2. If $n \in A$, then $n + 1 \in A$,

then $\mathbb{N} \subseteq A$.

Proposition 2.16:

Let $B \subseteq \mathbb{Z}$ be such that:

1. $1 \in B$, and
2. If $n \in B$, then $n + 1 \in B$,

then $B = \mathbb{N}$.

Proposition 2.18:

(i) For all $k \in \mathbb{N}$, $k^3 + 2k$ is divisible by 3.

(ii) For all $k \in \mathbb{N}$, $k^4 - 6k^3 + 11k^2 - 6k$ is divisible by 4.

(iii) For all $k \in \mathbb{N}$, $k^3 + 5k$ is divisible by 6.

Proposition 2.20:

For all $k \in \mathbb{N}$, $k \geq 1$.

Proposition 2.21:

There exists no integer x such that $0 < x < 1$.

Corollary 2.22:

Let $n \in \mathbb{Z}$. There exists no integer x such that $n < x < n + 1$.

Proposition 2.23:

Let $m, n \in \mathbb{N}$. If n is divisible by m, then $m \leq n$.

Proposition 2.24:

For all $k \in \mathbb{N}$, $k^2 + 1 > k$.

Proposition 2.26:

For all integers $k \geq -3$, $3k^2 + 21k + 37 \geq 0$.

Proposition 2.27:

For all integers $k \geq 2$, $k^2 < k^3$.

Proposition 2.33:

Let A be a nonempty subset of $\mathbb{Z}$ and $b \in \mathbb{Z}$, such that for each $a \in A$, $b \leq a$. Then A has a smallest element.

Proposition 2.34:

If m and n are integers that are not both 0, then

$$S = \{k \in \mathbb{N} : k = mx + ny \text{ for some } x, y \in \mathbb{Z}\}$$

Quizzes

Set Definition and Inclusion

(a) Let A and B be sets. Carefully define $A \subseteq B$.

A set A is a subset of a set B, denoted $A \subseteq B$, means that if an element x is in A, then that element x must also be in B.

(b) Carefully define $A = B$.

Two sets A and B are equal, denoted $A = B$, means that every element x in A is also in B and vice versa.

Definition of Division (m|n)

(a) Let $m, n \in \mathbb{Z}$. Carefully define what it means that m divides n.

We say that m divides n, denoted as $m|n$, if there exists an integer j such that $n = jm$.

(b) Carefully define what it means for n to be even.

An integer n is even if there exists an integer j such that $n = 2j$, where 2 is defined as the sum $1 + 1$ and 1 is established as the multiplicative identity.

Empty Set Definition and Subset Property

(a) Carefully define the empty set $\emptyset$.

The empty set $\emptyset$ is the unique set that contains no elements.

(b) Explain why $\emptyset \subseteq S$ for any set S.

The statement $\emptyset \subseteq S$ holds true for any set S because the condition "if x is in $\emptyset$, then x is in S" is vacuously true due to the absence of any elements in $\emptyset$.

Union and Intersection Definitions

(a) Let A and B be sets. Carefully define $A \cup B$.

The union $A \cup B$ is defined as the set of elements that are in either A, B, or in both.

(b) Carefully define $A \cap B$.

The intersection $A \cap B$ is the set of elements that are in both A and B.

Equivalence Relation Definition

Let $\sim$ be a relation on a set A. Carefully define what it means for $\sim$ to be an equivalence relation.

An equivalence relation $\sim$ on a set A satisfies three conditions:

1. Reflexivity: *For all $a \in A$, $a \sim a$.*
2. Symmetry: *For all $a, b \in A$, if $a \sim b$, then $b \sim a$.*
3. Transitivity: *For all $a, b, c \in A$, if $a \sim b$ and $b \sim c$, then $a \sim c$.*

Birthday Statement and Subtraction Definition

(a) Decide whether or not the statement ”today is Wednesday or it’s my birthday” is true.

This statement is true because in mathematics, the logical ”or” is inclusive. If either condition is met, the entire statement holds true.

(b) Let $m, n \in \mathbb{Z}$. Carefully define $m - n$.

The subtraction of n from m, denoted $m - n$, is defined as the addition of m to the additive inverse of n: $m + (-n)$.

Further Explanation on the Empty Set

(a) Carefully define the empty set $\emptyset$:

The empty set $\emptyset$ is a set that contains no elements whatsoever.

(b) Explain why $\emptyset \subseteq S$ for any set S.

The statement $\emptyset \subseteq S$ is true for any set S because the premise ”if x is in $\emptyset$” is never true, and therefore, the conditional statement ”if x is in $\emptyset$, then x is in S” is vacuously true.

Union and Intersection Definitions

(a) Let A and B be sets. Carefully define $A \cup B$.

The union of two sets A and B, denoted by $A \cup B$, is the set that includes all the elements that are either in A, in B, or in both.

(b) Carefully define $A \cap B$.

The intersection of two sets A and B, denoted by $A \cap B$, is the set consisting of all elements that are both in A and B.

Equivalence Relation Definition

Let $\sim$ be a relation on a set A. Carefully define what it means for $\sim$ to be an equivalence relation.

An equivalence relation on a set A, denoted by $\sim$, must satisfy the following conditions:

1. **Reflexivity:** Every element is related to itself; that is, $a \sim a$ for all $a \in A$.
2. **Symmetry:** If one element is related to another, then the second element is related to the first; in other words, if $a \sim b$, then $b \sim a$ for all $a, b \in A$.
3. **Transitivity:** If an element is related to a second element, which is in turn related to a third, then the first element is related to the third; that is, if $a \sim b$ and $b \sim c$, then $a \sim c$ for all $a, b, c \in A$.

Logical Statements and Subtraction Definition

(a) Decide whether or not the statement ”today is Wednesday or it’s my birthday” is true.

This statement can be considered true if today is indeed Wednesday, as the ’or’ in the statement is inclusive. Therefore, even if it is not the speaker’s birthday, the statement is still true if today is Wednesday.

(b) Let $m, n \in \mathbb{Z}$. Carefully define $m - n$.

Subtraction in the context of integers is defined by the operation $m - n = m + (-n)$, where $-n$ represents the additive inverse of n, such that $n + (-n) = 0$.

Further Discussion on the Empty Set

(a) Carefully define the empty set $\emptyset$:

The empty set $\emptyset$ is the set with no elements. It is the unique set for which the statement ”there exists an x such that x is in $\emptyset$” is always false.

(b) Explain why $\emptyset \subseteq S$ for any set S.

For any set S, the empty set $\emptyset$ is a subset because there are no elements in $\emptyset$ to contradict the statement ”if x is in $\emptyset$, then x is in S.” Hence, the statement $\emptyset \subseteq S$ is always true.