Introduction to Abstract Mathematics

UT Knoxville, Fall 2022, MATH 300

Peter Humphries, Conrad Plaut, and Alex Zhang

January 26, 2023

Contents

Preface

This text attempts to give a concise overview of the **Introduction to Abstract Mathematics** course at the University of Tennessee. The contents of this text are a compilation of things from Dr. Conrad Plaut's textbook, *Introduction to Abstract Mathematics*, as well as Dr. Peter Humphries' lecture notes.

Our goal is to create a logically sound model of mathematics that covers most arithmetic and algebraic properties we've been familiar with since grade school. Our general approach will be to assume as little possible, then prove things based on our assumptions.

Although we will focus on aspects of formal math such as proofs and proof writing, we will still take naive approaches to defining fundamental objects such as numbers as sets. That is, we will define many things informally using natural language and prior knowledge.

1 Logic and Set Theory

In this chapter, we will discuss fundamental definitions and concepts that form the basis of abstract mathematics.

Overview

- Logical statements and laws
- Basic proofs and proof techniques
- Naive set theory and functions

1.1 Logic

Logic is the study of formal reasoning. The most basic element of logic is a statement. While statements in spoken language can be ambiguous in meaning, we will only work with statements that are strictly either true or false.

Definition 1.1.1 ▸ Statement

A **statement** is a claim that is either true or false.

Definition 1.1.2 ▸ Truth Value

A statement's **truth value** indicates whether the statement is true or false.

An **axiom** is a statement that is simply assumed to be true, while a **theorem** is a statement that can be proven to be true.

Mathematics is based on the **axiomatic method**. We use defined terms alongside axioms assumed to be true in order to prove certain theorems. Different combinations of axioms can lead to different mathematical structures.

In English, we can combine statements into compound statements using conjunctions like "and" or "or". The same idea can be used to combine logical statements. Throughout this chapter, we will let P and Q denote any arbitrary statement.

Definition 1.1.3 ▸ Logical Connective

Logical connectives combine statements to form compound statements.

Conjunction	"P and Q"	$P \wedge Q$
Disjunction	"P or Q"	$P \vee Q$

We will use **truth tables** to reveal the logic of complex statements. These tables include every combination of possible input truth values and show the resulting truth values of the complex statement.

Example 1.1.1 ▸ Truth Table for Logical Connectives

P	Q	$P \wedge Q$	$P \vee Q$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	F

As we can see, the $\wedge$ and $\vee$ connectives follow our intuition of "and" and "or". Specifically, $P \wedge Q$ is true if P is true **and** Q is true. $P \vee Q$ is true if P is true or Q is true.

Definition 1.1.4 ▸ Negation

The **negation** of a statement gives a statement with **opposite** truth values.

$$\neg P$$

Example 1.1.2 ▸ Truth Table for Negation

P	$\neg P$
T	F
F	T

Definition 1.1.5 ▸ Conditional Statement

A **conditional statement** combines two statements using implication.

$$P \implies Q$$

Some important things to note:

- We can read this as "P implies Q" or "if P, then Q".
- P is called the **hypothesis**; Q is called the **conclusion**.
- A false hypothesis can imply any conclusion, making the implication **vacuously true** (i.e a false statement can imply **any** statement, true or false)
- The implication is false only when P is true and Q is false (i.e. a true statement cannot imply a false one)

Example 1.1.3 ▸ Truth Table for Conditional Statement

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

Definition 1.1.6 ▸ Converse, Contrapositive, and Inverse

Given $P \implies Q$, there are also three closely related conditional statements:

Converse	$Q \implies P$	No inherent equivalence to the original
Contrapositive	$(\neg Q) \implies (\neg P)$	Always equivalent to the original
Inverse	$(\neg P) \implies (\neg Q)$	Always equivalent to the converse

Let's say we want to prove some conditional statement $P \implies Q$. We are only concerned with conditions that would make the implication **false**, namely if P is true and Q is false. That is, we do not have to worry about false hypotheses as the entire implication would then be true, regardless of the conclusion.

Technique 1.1.1 ▸ Proving a Conditional Statement

There are three basic methods of proving a conditional statement $P \implies Q$.

1. Direct Proof — Assume P is true. Show that Q would also be true.
2. Contrapositive Proof — Assume Q is false. Show that P would also be false.
3. Proof by Contradiction — Assume the negation of the conditional statement, $P \implies \neg Q$. Show that this assumption leads to an obvious contradiction.

Definition 1.1.7 ▸ Biconditional Statement

A **biconditional statement** is a logical implication that goes both ways.

$$P \iff Q$$

We can read this as "P if and only if Q" or "if P then Q, and vice versa". We can also say P and Q are **logically equivalent** since they share the same truth values.

Example 1.1.4 ▸ Truth Table for Biconditional Statement

P	Q	$P \implies Q$	$Q \implies P$	$P \iff Q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Technique 1.1.2 ▸ Proving a Biconditional Statement

Given a statement $P \iff Q$, we must prove two conditional statements:

1. $P \implies Q$
2. $Q \implies P$

Definition 1.1.8 ▸ Tautology

A **tautology** is a statement that is always true.

Definition 1.1.9 ▸ Contradiction

A **contradiction** is a statement that is always false.

Now that we've defined some basic terms and notation, we can explore some fundamental laws of logic.

Laws of Propositional Logic

Here, let p, q, and r be any statement. Let T be a tautology and F be a contradiction.

Idempotent laws	$p \wedge p \iff p$ $p \vee p \iff p$
Associative Laws	$(p \vee q) \vee r \iff p \vee (q \vee r)$ $(p \wedge q) \wedge r \iff p \wedge (q \wedge r)$
Commutative Laws	$p \vee q \iff q \vee p$ $p \wedge q \iff q \wedge p$
Distributive Laws	$p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r)$
Identity Laws	$p \vee F \iff p$ $p \wedge T \iff p$
Domination Laws	$p \wedge F \iff F$ $p \vee T \iff T$
Double Negation	$\neg\neg p \iff p$
Complement Laws	$p \wedge \neg p \iff F$ $p \vee \neg p \iff T$
De Morgan's Laws	$\neg(p \vee q) \iff \neg p \wedge \neg q$ $\neg(p \vee q) \iff \neg p \vee \neg q$
Absorption Laws	$p \vee (p \wedge q) \iff P$ $p \wedge (p \vee q) \iff p$
Cond. Identities	$(p \implies q) \iff (\neg p \vee q)$ $(p \iff q) \iff [(p \implies q) \wedge (q \implies p)]$
Contrapositive	$(p \implies q) \iff (\neg q \implies \neg p)$

Definition 1.1.10 ▸ Quantifier

A **quantifier** specifies how many elements follow a particular statement.

$\forall$	"for all"	$\forall(x)(P(x))$	$\iff [P(x_0) \land P(x_1) \land P(x_2) \land \ldots]$
$\exists$	"there exists"	$\exists(x)(P(x))$	$\iff [P(x_0) \lor P(x_1) \lor P(x_2) \lor \ldots]$

1.2 Sets

Definition 1.2.1 ▸ Set

A **set** is a collection of distinct objects, none of which is the set itself.

Note that sets do not have to contain just numbers. Anything can be an element of a set—even other sets!

Example 1.2.1 ▸ Common Sets

Commonly used sets are typically denoted by double-struck capital characters.

$\varnothing$	Empty set	$\{\}$
$\mathbb{N}$	Natural numbers	$\{1, 2, 3, \ldots\}$
$\mathbb{Z}$	Integers	$\{\ldots, -1, 0, 1, \ldots\}$
$\mathbb{Q}$	Rationals	$\left\{\ldots, -\frac{1}{2}, \ldots, \frac{1}{2}, \ldots\right\}$
$\mathbb{R}$	Real Numbers	$\{\ldots, 1, \ldots, 2, \ldots, \pi, \ldots\}$

Note: $\{\varnothing\}$ is **not** the empty set, rather the set containing the empty set.

Definition 1.2.2 ▸ Set Relations

Symbol	Description	Example
$x \in A$	Element x is in set A	$1 \in \mathbb{N}$
$x \notin A$	Element x is **not** in set A	$0 \notin \mathbb{N}$
$A = B$	Sets A and B are equal	$\{1,2,3\} = \{2,1,3\}$
$A \subseteq B$	A is a subset of B	$\{1,2,3\} \subseteq \{1,2,3\}$
$A \subsetneq B$	A is a **proper** subset of B	$\{1,2\} \subsetneq \{1,2,3\}$

There is no consistent rule regarding the usage of the generic subset symbol $\subset$. Among different texts, it can denote either "subset or equal to" or "proper subset". To avoid ambiguity, we will only use $\subseteq$ and $\subsetneq$.

Definition 1.2.3 ▸ Set Operations

Set operations take two input sets and creates a new set.

Name	Definition
Intersection	$A \cap B \coloneqq \{x : (x \in A) \land (x \in B)\}$
Union	$A \cup B \coloneqq \{x : (x \in A) \lor (x \in B)\}$
Set Difference	$A \setminus B \coloneqq \{x : (x \in A) \land (x \notin B)\}$
Symmetric Difference	$A \triangle B \coloneqq \{x : (x \in A) \oplus (x \in B)\}$

Technique 1.2.1 ▸ Proving Set Equality

Imagine we had two sets, A and B, and had to prove $A = B$. The usual approach is to show $A \subseteq B$ and $B \subseteq A$.

Example 1.2.2 ▸ Simple Set Equality Proof

Prove that if A and B are disjoint, then $A \setminus B = A$

Proof. We will prove the two subset relations.

1. Let $x \in A \setminus B$. Then $x \in A$ and $X \notin B$, so $x \in A$. Thus, $A \setminus B \subseteq A$.
2. Let $x \in A$. Suppos for contradiction $x \in B$. Then $x \in A \cup B$. But $A \cup B = \varnothing$ because A and B are disjoint. Hence, $x \notin B$, so $x \in A \setminus B$. Thus, $A \subseteq A \setminus B$

Because $A \setminus B \subseteq A$ and $A \subseteq A \setminus B$, we therefore have $A \setminus B = A$. ▢

Theorem 1.2.1 ▸ Disjoint Union

If A and B are sets, then:

$$A \cup B = (A \setminus B) \cup (A \cap B) \cup (B \setminus A)$$

where $A \setminus B, A \cap B, B \setminus A$ are all disjiont from one another.

Proof. Let $x \in A \cup B$ be arbitrary. TODO: FINISH PROOF ▢

Definition 1.2.4 ▸ Tuple

A **tuple** is a collection of objects where order matters, denoted as $(a, b, c, \ldots)$.

$$a \neq b \iff (a, b) \neq (b, a)$$

A tuple of two elements is typically called an **ordered pair**.

Definition 1.2.5 ▸ Cartesian Product

The **cartesian product** between two sets A and B is the set with every possible ordered pair of elements from A and B.

$$A \times B = \{(a, b) : a \in A \ \wedge b \in B\}$$

A Cartesian Product can also be expressed as a set raised to a power.

$$A^n = \{(a_0, \ldots, a_n) : a_0, \ldots, a_n \in A\} = A \times \cdots \times A$$

1.3 Functions

Consider the function $f(x) = x^2$ for the natural numbers $(1, 2, 3, \ldots)$. f maps values as such:

$$1 \mapsto 1$$
$$2 \mapsto 4$$
$$3 \mapsto 9$$
$$\vdots$$

The function f is actually a set of ordered pairs $\{(1, 1), (2, 4), (3, 9), \ldots\}$ where we assign every natural number to its corresponding square.

Definition 1.3.1 ▸ Function

Let X and Y be sets. A **function** from X to Y is a relation $f \subseteq X \times Y$ such that:

1. for all $x \in X$, there exists some $y \in Y$ such that $(x, y) \in f$, and
2. for all $x \in X$ and $y_1, y_2 \in Y$, if $(x, y_1) \in f$ and $(x, y_2) \in f$, then $y_1 = y_2$.

The standard notation to define a function is $f : X \to Y$ where X is the **domain** and Y is the **codomain** of the function. We also write $f(x) = y$ instead of $(x, y) \in f$.

Definition 1.3.2 ▸ Image

Let $f : X \to Y$ be a function, and let $A \subseteq X$. The **image** of A is the set of all possible output values A can produce.

$$f[A] \coloneqq \{y \in Y : \exists (x \in A)\,[y = f(x)]\}$$

In a function $f : X \to Y$, taking the image of X (i.e. $f[X]$) gives us the **range** of the function. It's a subset of the codomain, which is not necessarily equal to the codomain.

Definition 1.3.3 ▸ Inverse Image

Let $f : X \to Y$ be a function, and let $B \subseteq Y$. The **inverse image** of B is the set of all values of X that map to something in B.

$$f^{-1}[B] \coloneqq \{x \in X : f(x) \in B\}$$

Definition 1.3.4 ▸ Open/Closed Interval

An **interval** is a set that contains a range of elements.

- Open Interval $(a, b) = \{n : a < n < b\}$
- Closed Interval $[a, b] = \{n : a \leq n \leq b\}$

Example 1.3.1 ▸ Image and Inverse Image

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. We have:

- $f[\{1, -1\}] = \{1\}$
- $f^{-1}[(0, 1)] = (-1, 0) \cup (0, 1)$
- $f[f^{-1}[\{-1\}]] = f[\varnothing] = \varnothing$
- $f^{-1}[f[\{-1\}]] = f^{-1}[\{1\}] = \{-1, 1\}$

2 Real Numbers

We are all familiar with the properties of real numbers. It is less obvious how we can define the set of real numbers. The goal of this chapter is to present an axiomatic basis for defining the set real numbers. We can characterize the real numbers as a **complete ordered field**, and we take as axiomatic that there is only one complete ordered field.[1]

Overview

- Definition of field, field axioms, and consequences of field axioms
- Order axioms and their consequences
- Infimum, supremum, completeness, and the Approximation Property
- Absolute value, triangle inequality, and approximating polynomials

2.1 Field Axioms

Definition 2.1.1 ▸ Field

A **field** is a set with two closed operations, addition and multiplication, that satisfy the following axioms for all $a, b, c \in \mathbb{F}$:

Axiom	Addition	Multiplication
Associativity	$(a+b)+c = a+(b+c)$	$(ab)c = a(bc)$
Commutativity	$a+b = b+a$	$ab = ba$
Distributivity	$a(b+c) = ab+ac$	$(a+b)c = ac+bc$
Identities	$\exists(0 \in \mathbb{F})(a+0=a)$	$\exists(1 \in \mathbb{F})(1 \neq 0 \wedge 1a = a)$
Inverses	$\exists(-a \in \mathbb{F})(a+(-a)=0)$	$(a \neq 0) \iff \exists(a^{-1} \in \mathbb{F})(aa^{-1}=1)$

"Closed operation" just means that we can add or multiply any two things in the field and still get a thing in the field. "Field" is a pretty broad term and encompasses a lot more than just the real numbers.

[1] More formally: if $\mathbb{R}$ and S are both complete ordered fields, then there exists a unique isomorphism from $\mathbb{R}$ to S. This can actually be proven, but it won't be a topic for these notes.

Example 2.1.1 ▸ Common Fields

Fields	**Not Fields**	
$\mathbb{R}$: Real numbers	$\mathbb{Z}$: Integers	(no multiplicative inverse beside ± 1)
$\mathbb{Q}$: Rational numbers	$\mathbb{N}$: Natural numbers	(no additive identity)
$\mathbb{C}$: Complex numbers	$M_n(\mathbb{R})$: $n \times n$ matrices	(multiplication is not commutative)

We may be tempted to start using familiar properties, like how multiplying by zero yields zero or how $x^{-1^{-1}} = x$. However, at this stage, we only know of the five field axioms. We will have to prove most of the properties we've been familiar with, no matter how trivial they may seem.

Theorem 2.1.1 ▸ Uniqueness of Addition in a Field

For any field $\mathbb{F}$ and all $a, b \in \mathbb{F}$, the equation $a + x = b$ has a unique solution.

Proof. Let $\mathbb{F}$ be a field, and let $a, b \in \mathbb{F}$. We need to show both of the following:

1. **Existence:** $a + x = b$ has a solution $x \in \mathbb{F}$.
2. **Uniqueness:** if x_1 and x_2 are solutions to $a + x = b$, then $x_1 = x_2$.

Let $x_1 \coloneqq (-a) + b$. Since $-a, b \in \mathbb{F}$ and $\mathbb{F}$ is closed under addition, then $x_1 \in \mathbb{F}$.

$$\begin{aligned} a + x_1 &= a + ((-a) + b) && x_1 = (-a) + b \\ &= (a + (-a)) + b && \text{Additive Associativity} \\ &= 0 + b && \text{Additive Inverse} \\ &= b && \text{Additive Identity} \end{aligned}$$

Thus, x_1 is a solution to $a + x = b$.

Suppose that there exists some $x_2 \in \mathbb{F}$ that is also a solution to $a+x = b$. Then $a+x_1 = b$ and $a + x_2 = b$.

$$\begin{aligned} a + x_1 &= a + x_2 \\ (-a) + (a + x_1) &= (-a) + (a + x_2) && \text{Add } -a \text{ to both sides} \\ ((-a) + a) + x_1 &= ((-a) + a) + x_2 && \text{Additive Associativity} \\ 0 + x_1 &= 0 + x_2 && \text{Additive Inverse} \\ x_1 &= x_2 && \text{Additive Identity} \end{aligned}$$

Therefore, $a + x = b$ has only one solution. ▢

A similar proof can be done for multiplication where $a \neq 0$.

Technique 2.1.1 ▸ Proving Equality in a Field

Imagine we had elements $a, b \in \mathbb{F}$ and had to prove they were equal. We can use the idea of uniqueness to prove that $a = b$.

1. Create some equation in the form of $x + y = z$ or $x \cdot y = z$ with y and z being fixed constants.
2. Show that $x = a$ and $x = b$ are both valid solutions to the equation.

We can then use the fact that addition/multiplication is unique to conclude that $a = b$.

Note: When using uniqueness of multiplication, we cannot let $y = 0$ since anything times zero is zero.

The following theorem demonstrates the above technique.

Theorem 2.1.2 ▸ Multiplication by Zero

For any field $\mathbb{F}$ and all $a \in \mathbb{F}$, $0 \cdot a = 0$

Proof. Let $\mathbb{F}$ be a field, and let $a \in \mathbb{F}$. Consider the following equation:

$$a + x = a$$

1. Let $x = 0$. Then, by definition of the additive identity, $a + x = a + 0 = a$. Thus, $x = 0$ is a valid solution.
2. Let $x = 0 \cdot a$. Then:

$$\begin{aligned} a + x &= a + (0 \cdot a) && x = 0 \cdot a \\ &= (1 \cdot a) + (0 \cdot a) && \text{Multiplicative Identity} \\ &= a(1 + 0) && \text{Distributivity} \\ &= a \cdot 1 && \text{Additive Identity} \\ &= 1 \cdot a && \text{Commutative Property} \\ &= a && \text{Multiplicative Identity} \end{aligned}$$

Thus, $x = a \cdot 0$ is also a valid solution.

By Uniqueness of Addition in a Field, it must follow that $0 = a \cdot 0$. ▢

Theorem 2.1.3 ▸ Zero Product Property

For any field $\mathbb{F}$ and all $a, b \in \mathbb{F}$, if $ab = 0$, then $a = 0$ or $b = 0$.

Proof. Let $\mathbb{F}$ be a field, and let $a, b \in \mathbb{F}$ where $ab = 0$.

- If $a = 0$, we're done.
- If $a \neq 0$, then $a^{-1} \in \mathbb{F}$. Thus:

$$\begin{aligned} ab = 0 &\implies aba^{-1} = 0a^{-1} && \text{Multiply both sides by } a^{-1} \\ &\implies aa^{-1}b = 0a^{-1} && \text{Multiplicative Commutativity} \\ &\implies 1b = 0a^{-1} && \text{Multiplicative Inverse} \\ &\implies b = 0a^{-1} && \text{Multiplicative Identity} \\ &\implies b = 0 && \text{Multiplication by Zero} \end{aligned}$$

In either case, $a = 0$ or $b = 0$. ▢

Theorem 2.1.4 ▸ Double Additive Inverse

For any field $\mathbb{F}$ and all $a \in \mathbb{F}$, $a = -(-a)$.

Proof. Let $\mathbb{F}$ be a field, and let $a \in \mathbb{F}$. Consider the equation $x + (-a) = 0$.

1. Let $x = a$. Then $a + (-a) = 0$ by definition of Additive Inverse.
2. Let $x = -(-a)$. Then $-(-a) + (-a) = (-a) + -(-a) = 0$ by definition of Additive Inverse.

By Uniqueness of Addition in a Field, it must follow that $a = -(-a)$. ▢

Theorem 2.1.5 ▸ Double Multiplicative Inverse

For any field $\mathbb{F}$ and all $a \in \mathbb{F}$ where $a \neq 0$, $a = (a^{-1})^{-1}$.

Proof. Let $\mathbb{F}$ be a field, and let $a \in \mathbb{F}$ where $a \neq 0$. Consider the equation $xa^{-1} = 1$.

1. Let $x = a$. Then $aa^{-1} = 1$ by definition of the Multiplicative Inverse.
2. Let $x = (a^{-1})^{-1}$. Then $(a^{-1})^{-1}a^{-1} = a^{-1}(a^{-1})^{-1} = 1$ by definition of the Multiplicative Inverse.

By Uniqueness of Addition in a Field, it must follow that $a = (a^{-1})^{-1}$. □

We can define subtraction and division as shorthand notation as adding/multiplying by the respective inverse.

Definition 2.1.2 ▸ Subtraction

$$a - b \coloneqq a + (-b)$$

Definition 2.1.3 ▸ Division

$$\frac{a}{b} \coloneqq ab^{-1}$$

2.2 Order Axioms

Definition 2.2.1 ▸ Ordered Field

A field $\mathbb{F}$ is **ordered** if and only if there exists a relation $<$ on $\mathbb{F}$ such that all $a, b, c \in \mathbb{F}$ satisfy the following axioms:

Axiom	Description
Transitivity	If $a < b$ and $b < c$, then $a < c$
Trichotomy	Only **one** is true: $a < b$ **or** $a = b$ **or** $b < a$
Additive Property	If $a < b$, then $a + c < b + c$
Multiplicative Property	If $a < b$ and $0 < c$, then $ac < bc$

This leaves us with the real numbers ($\mathbb{R}$) and rational numbers ($\mathbb{Q}$). The complex numbers ($\mathbb{C}$)

have no order between the elements (is $1 + 2i < 2 + 1i$, or $2 + 1i < 1 + 2i$).

Order Notation and Terminology

- $a < b$ is equivalent to $b > a$
- $a \leq b$ is equivalent to $a < b$ or $a = b$
- $a \in \mathbb{F}$ is **positive** if $a > 0$
- $a \in \mathbb{F}$ is **negative** if $a < 0$

From now on, we will use basic algebra in proofs without explaining each individual step.

Be careful when negating inequalities!

- The negation of $a < b$ is $a \geq b$, not $a > b$.
- $a < b < c$ means $a < b$ **and** $b < c$, so its negation would be "$a \geq b$ **or** $b \geq c$"

Theorem 2.2.1 ▸ Negatives Flip Inequality

Let $\mathbb{F}$ be any ordered field, and let $a \in \mathbb{F}$. If $a < 0$, then $-a > 0$.

Proof. Let $\mathbb{F}$ be an ordered field, and let $a \in \mathbb{F}$ where $a < 0$. By the additive property, we can add $-a$ to both sides of the inequality. Then $(-a) + a < (-a) + 0$ which simplifies to $0 < -a$. Therefore, $-a > 0$. ▢

Theorem 2.2.2 ▸ $0 < 1$

$0 < 1$ in any ordered field.

Proof. Suppose for contradiction that $1 < 0$. Since Negatives Flip Inequality, then $-1 > 0$. Hence, we can apply the multiplicative property to $0 < -1$ as such:

$$\begin{aligned} 0(-1) &< (-1)(-1) \\ &= -(-1) \\ &= 1 \end{aligned}$$

That is, $0 < 1$, which contradicts our supposition that $1 < 0$. Thus, it must be true that $0 \leq 1$ (the negation of $1 < 0$). Since the field axioms strictly state $0 \neq 1$, then $0 < 1$. ▢

2.3 Completeness

Completeness deals with the idea of existence of bounds.

Definition 2.3.1 ▸ Upper Bound

$M \in \mathbb{F}$ is an **upper bound** for A if $M \geq x$ for all $x \in A$.

Definition 2.3.2 ▸ Lower Bound

$M \in \mathbb{F}$ is a **lower bound** for A if $M \leq x$ for all $x \in A$.

We say a set is **bounded above** if there exists an upper bound for that set. Similarly, we say a set is **bounded below** if there exists a lower bound for that set.

Definition 2.3.3 ▸ Supremum

$s \in \mathbb{F}$ is a **supremum** of A ($\sup A$) if:

1. s is an upper bound for A, and
2. $s \leq M$ for all upper bounds M of A.

Definition 2.3.4 ▸ Infimum

$s \in \mathbb{F}$ is an **infimum** of A ($\inf A$) if:

1. s is a lower bound for A, and
2. $s \geq M$ for all lower bounds M of A.

Definition 2.3.5 ▸ Maximum

$s \in \mathbb{F}$ is a **maximum** of A ($\max A$) if s is a supremum of A and $s \in A$.

Definition 2.3.6 ▸ Minimum

$i \in \mathbb{F}$ is a **minimum** of A ($\min A$) if i is an infimum of A and $i \in A$.

Now we can finally tackle the notion of "completeness".

Definition 2.3.7 ▸ Complete Field

An ordered field $\mathbb{F}$ is **complete** if every $A \subseteq \mathbb{F}$ that is bounded above has a supremum.

Definition 2.3.8 ▸ Real Numbers ($\mathbb{R}$)

The set of **real numbers** is the unique complete ordered field.

The rational numbers are **not** complete. Consider the following set:

$$A \coloneqq \{r \in \mathbb{Q} : r^2 < 2\} \subseteq \mathbb{Q}$$

A natural choice for a supremum might be $\sqrt{2}$, but note that $\sqrt{2}$ is not a rational number (proven in Example 3.4.6).

Theorem 2.3.1 ▸ Approximation Property for the Supremum

Let $A \subseteq \mathbb{R}$ be nonempty and bounded above. Then $s = \sup A$ if and only if:

1. $\forall(x \in A)(s \geq x)$
2. $\forall(\epsilon > 0)\exists(x \in A)(s - \epsilon < x)$

Proof. We will show that the definition of supremum and the proposed criteria in this proof are logically equivalent.

First, let's assume $s = \sup A$.

1. By definition, s is an upper bound of A, so $\forall(x \in A)(s \geq x)$.
2. Suppose for contradiction that our second criterion does not hold. That is:

$$\exists(\epsilon > 0)\forall(x \in A)(x \leq s - \epsilon)$$

   Then $s - \epsilon$ is an upper bound of A. However, this contradicts our assumption that s was the supremum for a. Therefore, our second criterion holds.

Next, let's assume our two criteria are true.

1. By the first criterion, s is an upper bound of A.
2. Suppose for contradiction there exists an upper bound m of A such that $s > m$. Let $\epsilon \coloneqq s - m$. Then by our second criterion:

$$\exists(x \in A)(s - (s - m) < x) \iff \exists(x \in A)(m < x)$$

   This contradicts the idea that m is an upper bound of A. Therefore, $s \leq m$ for all upper bounds m of A.

This proves the entire logical equivalence. ▢

2.4 Absolute Value

Definition 2.4.1 ▸ Absolute Value

For any $x \in \mathbb{R}$, the **absolute value** of x is:

$$|x| := \begin{cases} x, & x \geq 0 \\ -x, & x < 0 \end{cases}$$

Absolute value of a real number can be thought as the magnitude or "distance" from zero. Similarly, the absolute value $|x - y|$ can be thought of as the "distance" between x and y.

Example 2.4.1 ▸ $|x||y| = |xy|$

For all $x, y \in \mathbb{R}$, $|x||y| = |xy|$.

Proof. Let $x, y \in \mathbb{R}$. There are four cases to consider:

1. If $x \geq 0$ and $y \geq 0$, then $xy \geq 0$. Thus, $|x| = x$, $|y| = y$, and $|xy| = xy$. Then $|x||y| = xy = |xy|$.
2. If $x \geq 0$ and $y < 0$, then $xy \leq 0$. Thus, $|x| = x$, $|y| = -y$, and $|xy| = -xy$. Then $|x||y| = x(-y) = -xy = |xy|$.
3. If $x < 0$ and $y \geq 0$, then the proof is similar to case 2.
4. If $x < 0$ and $y < 0$, then $xy > 0$. Thus, $|x| = -x$, $|y| = -y$, and $|xy| = xy$. Then $|x||y| = (-x)(-y) = xy = |xy|$.

□

Example 2.4.2 ▸ Bounds of Absolute Value

For all $x \in \mathbb{R}$ and $M \geq 0$, $|x| \leq M$ if and only if $-M \leq x \leq M$.

Proof. First, suppose that $|x| \leq M$.

- If $x \geq 0$, then $|x| = x$, so $-M \leq 0 \leq x = |x| \leq M$.
- If $x < 0$, then $|x| = -x$, so $-M \leq -|x| = x < 0 \leq M$.

In either case, $-M \leq x \leq M$.

Next, suppose that $-M \leq x \leq M$.

- If $x \geq 0$, then $|x| = x \leq M$
- If $x < 0$, then $|x| \leq -(-M) = M$

□

Theorem 2.4.1 ▸ Triangle Inequality

For all $x, y \in \mathbb{R}$, $|x + y| \leq |x| + |y|$

Proof. For any $x \in \mathbb{R}$, we have $|x| \leq |x|$. Thus, by Example 2.4.2, we have $-|x| \leq x \leq |x|$. Similarly, for any $y \in \mathbb{R}$, then $-|y| \leq y \leq |y|$. That is:

$$-|x| - |y| \leq x + y \leq |x| + |y|$$

$$-(|x| + |y|) \leq x + y \leq |x| + |y|$$

Therefore, we have $|x + y| \leq |x| + |y|$. □

Example 2.4.3 ▸ Reverse Triangle Inequality

For all $x, y \in \mathbb{R}$, $|x - y| \geq |x| - |y|$.

Proof. Let $x, y \in \mathbb{R}$. By the Triangle Inequality, we have:

$$|x| = |x - y + y| \leq |x - y| + |y|$$

Thus, we have $|x| \leq |x - y| + |y|$. Subtract both sides by $|y|$, we get:

$$|x| - |y| \leq |x - y|$$

. □

Example 2.4.4 ▸ Approximating Polynomials

Show that if $|x + 1| \leq 3$, then $|x^2 + 3x + 2| \leq 12$.

Proof. Let $x \in \mathbb{R}$ where $|x + 1| \leq 3$. Note that $x^2 + 3x + 2 = (x + 1)(x + 2)$. Because $|x||y| = |xy|$, we have:

$$|x^2 + 3x + 2| = |(x + 1)(x + 2)| = |x + 1||x + 2|$$

Since $|x + 1| \leq 3$, then:

$$|x + 2| = |(x + 1) + 1| \leq |x + 1| + |1| \leq 3 + 1 = 4$$

Thus:

$$|x^2 + 3x + 2| = |x + 1||x + 2| \leq 3 \cdot 4 = 12$$

Therefore, $|x^2 + 3x + 2| \leq 12$. □

3 Integers and Induction

Overview

- Formal definitions of the natural numbers ($\mathbb{N}$) and integers ($\mathbb{Z}$)
- Properties of the integers, Well-Ordering Principle
- Principle of Induction and its uses
- Divisibility, prime numbers, and prime factorizations

3.1 Definitions of $\mathbb{N}$ and $\mathbb{Z}$

Now that we have defined the real numbers $\mathbb{R}$, we can use some interesting definitions to derive the natural numbers $\mathbb{N}$.

Definition 3.1.1 ▸ Closed Under Addition

A set X is **closed under addition** if $x_1 + x_2 \in X$ for any $x_1, x_2 \in X$.

$$\forall (x_1, x_2 \in X)(x_1 + x_2 \in X)$$

Definition 3.1.2 ▸ Supernatural

A set X is **supernatural** if X is closed under addition and $1 \in X$.

Definition 3.1.3 ▸ Natural Numbers ($\mathbb{N}$)

The **natural numbers** $\mathbb{N}$ is a set defined as:

$$\mathbb{N} \coloneqq \{x \in \mathbb{R} : x \in X \text{ for every supernatural set } X\}$$

We can think of the natural numbers as being the intersection of every possible supernatural set.

Example 3.1.1 ▸ $\mathbb{N}$ is Supernatural

(1) $\mathbb{N}$ is supernatural, and (2) if $A \subseteq \mathbb{R}$, is supernatural, then $\mathbb{N} \subseteq A$.

Proof. Let $A \subseteq \mathbb{R}$ be supernatural.

1. $1 \in B$ for every supernatural set B, so $1 \in \mathbb{N}$ by the definition of $\mathbb{N}$. Let $x, y \in \mathbb{N}$. Then $x, y \in B$ for every supernatural set B. Therefore, $x + y \in B$ for every supernatural set B. That is, $x + y \in \mathbb{N}$, so $\mathbb{N}$ is closed under addition. Thus, $\mathbb{N}$ is supernatural.
2. Suppose that $A \subseteq \mathbb{R}$ is supernatural. Let $x \in \mathbb{N}$. By definition of $\mathbb{N}$, then $x \in A$. Thus, $\mathbb{N} \subseteq A$.

□

The previous lemma confirms our intuition that $\mathbb{N}$ is the "smallest" supernatural subset of $\mathbb{R}$. This idea is made precise in the next corollary.

Theorem 3.1.1 ▸ Gap Theorem

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

Theorem 3.1.2 ▸ Well-Ordering Principle

Every non-empty subset of $\mathbb{N}$ has a minimum.

Proof. Let $S \subseteq \mathbb{N}$ where $S \neq \varnothing$. We know that 0 is the smallest natural number, so 0 is a lower bound of S. Note that $\mathbb{N} \subseteq \mathbb{R}$, so $S \subseteq \mathbb{R}$. Since $\mathbb{R}$ is a Complete Field and $S \subseteq \mathbb{R}$, then S has an infimum. Let $b \coloneqq \inf S$. It follows that $b + 1$ is **not** a lower bound of S. Thus, for some $n \in S$:

$$n < b + 1$$

Suppose for contradiction that $n \neq \min S$. Then there exists $m \in S$ such that:

$$\begin{aligned} b \leq m < n < b + 1 &\implies b - m \leq 0 < n - m < b - m + 1 \\ &\implies 0 < n - m < (b - m) - (b - m) + 1 \\ &\implies 0 < n - m < 1 \end{aligned}$$

However, by the Gap Theorem, there does not exist any natural number between 0 and 1. Hence, $n = b = \min S$. □

Definition 3.1.4 ▸ Integers ($\mathbb{Z}$)

The set of **integers** is defined as:

$$\mathbb{Z} := \{0\} \cup \mathbb{N} \cup \{n : -n \in \mathbb{N}\}$$

It also follows that the integers are closed both addition and multiplication. Moreover, the gap theorem still applies, and a slightly modified version of the Well-Ordering Principle applies.

Theorem 3.1.3 ▸ $\mathbb{Z}$ is Closed Under Addition

$\mathbb{Z}$ is closed under addition.

Proof. If $x, y \in \mathbb{Z}$, then $x + y \in \mathbb{Z}$. TODO: Finish proof ▢

Theorem 3.1.4 ▸ Gap Theorem for $\mathbb{Z}$

If $n \in \mathbb{Z}$, then $(n, n+1) \cap \mathbb{Z} = \varnothing$.

Proof. TODO: Finish proof ▢

Theorem 3.1.5 ▸ Well-Ordering Principle for $\mathbb{Z}$

Every nonempty subset of $\mathbb{Z}$ that is bounded above has a maximum.

Proof. ▢

Example 3.1.2 ▸ Floor and Ceiling Functions

We can use the Well-Ordering Principle for $\mathbb{Z}$ to define the floor and ceiling functions. Let $x \in \mathbb{R}$ be arbitrary.

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z} : n \leq x\}$$
$$\lceil x \rceil = \min\{n \in \mathbb{Z} : n \geq x\}$$

The maximum and minimum of these two sets is guaranteed. For floor, we are taking the maximum of a set bounded above by x. For ceiling, we are taking the minimum of a set bounded below by x.

3.2 Basic Properties of the Integers

Theorem 3.2.1 ▸ $\mathbb{N}$ is not Bounded Above

$\mathbb{N}$ is not bounded above.

Proof. Suppose for contradiction that $\mathbb{N}$ is bounded above. Then there exists $s := \sup \mathbb{N}$ where $n \leq s$ for all $n \in \mathbb{N}$. Since $\mathbb{N}$ is closed under addition, if $n \in \mathbb{N}$ then $n + 1 \in \mathbb{N}$. Hence $n + 1 \leq s$, so $n \leq s - 1$. Thus, $s - 1$ is an upper bound of $\mathbb{N}$. This contradicts s being the supremum of $\mathbb{N}$. ▢

Theorem 3.2.2 ▸ Archimedean Principle

For every $a, b \in \mathbb{R}$ where $b > 0$, there exists an $n \in \mathbb{N}$ such that $nb > a$.

Proof. Let $a, b \in \mathbb{R}$ where $b > 0$. Suppose for contradiction that $nb \leq a$ for all $n \in \mathbb{N}$. Then $n \leq a/b$ for all $n \in \mathbb{N}$, meaning $\mathbb{N}$ is bounded above by a/b. Since we know $\mathbb{N}$ is not bounded above, then $nb > a$ for some $n \in \mathbb{N}$. ▢

Example 3.2.1 ▸ Inverse Gap Theorem

If $a, b \in \mathbb{R}$ satisfy $b > a + 1$, then there exists $n \in \mathbb{N}$ such that $a \leq n < b$.

$$\forall (a, b \in \mathbb{R})(b > a + 1 \implies \exists (n \in \mathbb{N})(a \leq n < b))$$

Proof. Let $E = \{m \in \mathbb{Z} : m \geq a\}$. Because $\mathbb{Z}$ is not bounded above, then there must exist $m \geq a$, so E is non-empty (otherwise, a is an upper bound for $\mathbb{Z}$). Also, a is a lower bound for E, so $m = \min E$ exists by the Well-Ordering Principle for $\mathbb{Z}$. Because $m \in E$, we have $m \geq a$ Assume for contradiction that $m > a+1$. Then $m-1 \in \mathbb{Z}$ and $m-1 > a$, so $m - 1 \in E$. This contradicts $m = \min E$. Thus, $m \leq a + 1$, so $a \leq m \leq a + 1 < b$. ▢

The Archimedean Principle allows us to prove some suprema and infima of sets.

Example 3.2.2 ▸ Finding Supremum/Infimum of Weird Sets

Let $A \coloneqq \left\{ \frac{n+1}{n} : n \in \mathbb{N} \right\}$. Find $\sup A$ and $\inf A$, and prove that your answers are correct.

$$A = \left\{ 2, \frac{3}{2}, \frac{4}{3}, \frac{5}{4}, \ldots \right\}$$

$\sup A = 2$

Proof. For any $n \in N$, we know $n \geq 1$, so $n + n \geq n + 1$ or more simply $2n \geq n + 1$. Thus $2 \geq \frac{n+1}{n}$, so 2 is an upper bound of A. Also, $\frac{1+1}{1} = 2 \in A$, so $\max A = 2$ (exercise 2.19). Therefore, $\sup A = 2$. □

$\inf A = 1$

Proof. For any $n \in \mathbb{N}$, we have $n + 1 > n$, so $\frac{n+1}{n} > 1$. That is, 1 is a lower bound for A. Also, A is non-empty, so $\inf A$ exists. Assume for contradiction that $\inf A > 1$. Then there exists $m > 1$ such that m is a lower bound of A. That is, $m - 1 > 0$, so $\frac{1}{m-1} > 0$. By the Archimedean Principle, there exists some $n \in \mathbb{N}$ such that $n \cdot 1 > \frac{1}{m-1}$, so

$$\begin{aligned} n \cdot 1 &> \frac{1}{m-1} \\ n(m-1) &> 1 \\ nm - n &> 1 \\ nm &> n + 1 \\ m &> \frac{n+1}{n} \end{aligned}$$

This contradicts m being a lower bound for A. Thus, $\inf A \leq 1$. Because 1 is a lower bound for A, $\inf A = 1$. □

Theorem 3.2.3 ▸ Principle of Induction

For all $n \in \mathbb{N}$, let $P(n)$ be some statement. Suppose that:

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

Then $P(n)$ is true for all $n \in \mathbb{N}$.

Proof. For contradiction, let's assume the negation of our original statement. That is, let's assume conditions 1 and 2 are satisfied, but $P(n)$ is false for some $n \in \mathbb{N}$.

Let $A \coloneqq \{n \in \mathbb{N} : \neg P(n)\}$. Since A is not empty, then by the Well-Ordering Principle, A has a minimum. Let $m \coloneqq \min A$. Because $m \in A$, then $P(m)$ is false. Since $P(1)$ is true, then $m > 1$. Therefore, $m - 1 \in \mathbb{N}$, and because $m = \min A$, then $m - 1 \notin A$. Therefore, $P(m-1)$ is true (otherwise, $m - 1 \in A$). Thus, by condition 2, we have $P(m)$ is also true. This contradicts $m \in A$, so $P(n)$ is true for all $n \in \mathbb{N}$. ▢

Technique 3.2.1 ▸ Basic Proof by Induction

To prove that "$P(n)$ is true for all $n \in \mathbb{N}$" using the Principle of Induction:

1. **Base Case:** Prove $P(1)$ in a simple direct proof.
2. **Induction Hypothesis:** Assume that $P(n)$ is true for some $n \in \mathbb{N}$.
3. **Inductive Step:** Prove $P(n) \implies P(n+1)$.

Example 3.2.3 ▸ $\mathbb{Z}$ is Closed Under Multiplication

If $m, n \in \mathbb{Z}$, then $mn \in \mathbb{Z}$

Proof. Suppose that $n = 0$. Then $mn = m \cdot 0 = 0$ for any $m \in \mathbb{Z}$. So $mn \in \mathbb{Z}$.

Suppose that $n > 0$ (i.e. $n \in \mathbb{N}$). Fix some $m \in \mathbb{Z}$ (i.e. choose one specific integer m). Let $P(n)$ be the statement $mn \in \mathbb{Z}$.

1. $P(1)$ is true because $m \cdot 1 = m \in \mathbb{Z}$.
2. Now suppose that $P(n)$ is true for some $n \in \mathbb{N}$. Then $mn \in \mathbb{Z}$, so $m(n+1) = mn + m \in \mathbb{Z}$ by the induction hypothesis and closure of $\mathbb{Z}$ under addition. Thus, $P(n+1)$ is true.

Now that we have our base case and inductive step proved, we can safely say that $P(n)$ is true for all $n \in \mathbb{N}$. Thus, $mn \in \mathbb{Z}$ for all $m \in \mathbb{Z}$ and $n \in \mathbb{N}$.

Suppose that $n < 0$. Then $-n > 0$, so $n \in \mathbb{N}$. Thus, $mn = -(m(-n)) \in \mathbb{Z}$ by the proof above. ▢

Definition 3.2.1 ▸ Integer Powers

For any $a \in \mathbb{R}$:

- $a^0 = 1$
- $a^{n+1} = a^n \cdot a$

If $a \neq 0$:

- $a^0 = 1$
- $a^n = \frac{1}{a^{-n}}$ for $n < 0$

Example 3.2.4 ▸ Multiplication of Powers

If $m, n \in \mathbb{N}$, then $a^m a^n = a^{m+n}$

Proof. Fix some $m \in \mathbb{N}$. For each $n \in \mathbb{N}$, let $P(n)$ be the statement $a^m a^n = a^{m+n}$.

1. $a^m a^1 = a^m a = a^{m+1}$ by definition of positive integer powers. Thus, $P(1)$ is true.
2. Suppose $P(n)$ is true for some $n \in \mathbb{N}$. Then $a^m a^{n+1} = a^m(a^n a) = (a^m a^n)a = a^{m+n}a = a^{m+n+1}$. So $P(n+1)$ is true.

Therefore, $P(n)$ is true for all $n \in \mathbb{N}$. □

Example 3.2.5 ▸ Nested Powers

If $a \in \mathbb{R}, a \neq 0$, and $m, n \in \mathbb{Z}$, then $(a^m)^n = a^{mn}$

Proof. Consider the three following cases:

1. If $n = 0$, then $(a^m)^0 = 1 = a^0 = a^m$
2. For all $n \in \mathbb{N}$, let $P(n)$ be the statement $(a^m)^n = a^{mn}$ where $m \in \mathbb{Z}$ is fixed.
   (a) $(a^m)^1 = a^m = a^{m \cdot 1}$, so our base case $P(1)$ is true.
   (b) Assume $P(n)$ is true for some $n \in \mathbb{N}$. Then:

$$(a^m)^{n+1} = (a^m)^n a^m = a^{mn} a^m = a^{mn+m} = a^{m(n+1)}$$

   So $P(n+1)$ is true. That is, $P(n)$ is true for all $n \in \mathbb{N}$.
3. If $n \in -\mathbb{N}$, then $-n \in \mathbb{N}$, so:

$$(a^m)^n = \frac{1}{(a^m)^{-n}} = \frac{1}{a^{-mn}} = a^{mn}$$

□

Definition 3.2.2 ▸ Rational Numbers ($\mathbb{Q}$)

The set of **rational numbers** is defined as:

$$\mathbb{Q} \coloneqq \left\{ \frac{p}{q} \in \mathbb{R} : p, q \in \mathbb{Z}, q \neq 0 \right\}$$

We can simply define the **irrational numbers** as $\mathbb{R} \setminus \mathbb{Q}$.

Theorem 3.2.4 ▶ $\mathbb{Q}$ is Closed Under Addition and Multiplication

$\mathbb{Q}$ is closed under addition and multiplication.

Proof. Let $x, y \in \mathbb{Q}$. By definition of rational numbers:

1. There exist $a, b \in \mathbb{Z}$ where $b \neq 0$ and $x = a/b$, and
2. There exist $c, d \in \mathbb{Z}$ where $d \neq 0$ and $y = c/d$

We will use the idea that the integers are closed under addition and multiplication (Proposition 3.1.9 and Theorem 3.2.7). The two following equations were proven on page 24 of the textbook.

1. $x + y = a/b + c/d = ad+bc/bd$. Since the integers are closed under addition and multiplication, then $ad + bc$ and bd are both integers. Also, $b \neq 0$ and $d \neq 0$, so $bd \neq 0$. Thus, $x + y = ad+bc/bd \in \mathbb{Q}$.
2. $xy = a/b \cdot c/d = ac/bd$. Since the integers are closed under multiplication, then ac and bd are both integers. And, because $b \neq 0$ and $d \neq 0$, then $bd \neq 0$. Thus, $xy = ac/bd \in \mathbb{Q}$.

□

3.3 Applications of Induction

Example 3.3.1 ▸ Triangular Numbers

$\forall(n \in \mathbb{N})\left[\sum_{i=1}^{n} i = \frac{n(n+1)}{2}\right]$

Proof. We will use proof by induction. Let's first prove our base case:

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

Suppose that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ for some $n \in \mathbb{N}$.

$$\begin{aligned}\sum_{i=1}^{n+1} i &= \left(\sum_{i=1}^{n} i\right) + (n+1)\\ &= \frac{n(n+1)}{2} + (n+1)\\ &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2}\\ &= \frac{(n+1)(n+2)}{2}\\ &= \frac{(n+1)((n+1)+1)}{2}\end{aligned}$$

□

Example 3.3.2 ▸ Sum of Consecutive Odd Numbers

$\forall(n \in \mathbb{N})\left[\sum_{i=1}^{n}(2i-1) = n^2\right]$

$$\begin{aligned}\sum_{i=1}^{n}(2i = 1) &= 2\left(\sum_{i=1}^{n} i\right) - \left(\sum_{i=1}^{n} 1\right) \\ &= 2\frac{n(n+1)}{2} - n \\ &= n(n+1) - n \\ &= n^2 + n - n \\ &= n^2\end{aligned}$$

Example 3.3.3 ▸ Cool

If $p \in \mathbb{R}$ and $p > -1$, then $(1+p)^n \geq 1 + np$ for all $n \in \mathbb{N}$.

Proof. Let $n = 1$. Then $(1+p)^1 = 1 + p = 1 + 1 \cdot p$, so $(1+p)^1 \geq 1 + 1 \cdot p$.

Next, suppose that $(1+p)^n \geq 1 + np$ for some $n \in \mathbb{N}$. Then:

$$\begin{aligned}(1+p)^{n+1} &= (1+p)^n(1+p) \\ &\geq (1+np)(1+p) \\ &= 1 + p + np + np^2 \\ &= 1 + (n+1)p + np^2 \\ &\geq 1 + (n+1)p\end{aligned}$$

□

Variants of Induction

Two important variants of proof by induction are using a base case other than $n = 1$, and using **strong induction**.

Theorem 3.3.1 ▸ Induction with Base Case n_0

Let $P(n)$ be a statement for each $n \in \mathbb{N}$ such that

1. $P(n_0)$ is true, and
2. for all $n \in \mathbb{N}$ where $n \geq n_0$, if $P(n)$ is true then $P(n+1)$ is true

   i.e. $P(n) \implies P(n+1)$

Then $P(n)$ is true for all $n \in \mathbb{N}, n \geq n_0$.

Theorem 3.3.2 ▸ Strong Induction

Let $P(n)$ be a statement for each $n \in \mathbb{N}$ such that

1. $P(1)$ is true, and
2. for all $n \in \mathbb{N}$, if $P(n)$ is true for all $k \leq n$ then $P(n+1)$ is true

   i.e. $[P(1) \wedge P(2) \wedge \ldots \wedge P(n)] \implies P(n+1)$

Then $P(n)$ is true for all $n \in \mathbb{N}$.

Definition 3.3.1 ▸ Factorial

The **factorial** of a non-negative integer n is defined as:

$$n! = \begin{cases} 1 & \text{if } n = 0 \\ n(n-1)! & \text{if } n > 0 \end{cases}$$

Note: 0! can be thought of as an "empty product", or the multiplicative identity times nothing.

Example 3.3.4 ▸ Factorials and Induction

For all $n \geq 4$, $n! > 2^n$

Proof. Let $n = 4$. Then $n! = 4! = 24$ and $2^n = 2^4 = 16$. Because $4! > 2^4$, the statement is true when $n = 4$.

Assume that $n! > 2^n$ is true for some $n \in \mathbb{N}$ where $n \geq 4$. Then:

$$\begin{aligned}(n+1)! &= n! \cdot (n+1) \\ &> 2^n \cdot (n+1) \\ &> 2^n \cdot 2 \\ &= 2^{n+1}\end{aligned}$$

Therefore, $n! > 2^n$ for all $n \geq 4$. ▢

Definition 3.3.2 ▸ Binomial Coefficient

The notation $\binom{n}{k}$ is called a **binomial coefficient**.

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \text{ for } 0 \leq k \leq n$$

For $n, k \geq 0$, $\binom{n}{k}$ also represents the number of ways to choose k objects from a set of n objects. We can read $\binom{n}{k}$ as "n choose k".

Example 3.3.5 ▸ B.C. Identities

1. $\binom{n}{k} = \binom{n}{n-k}$

$$\binom{n}{n-k} = \frac{n!}{(n-k)!\,[n-(n-k)]!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$$

2. $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$ (Additive Property for Pascal's Triangle)

$$\begin{aligned}
\binom{n-1}{k-1} + \binom{n+1}{k} &= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-1-k)!} \\
&= \frac{(n-1)!k}{k!(n-k)!} + \frac{(n-1)!(n-k)}{k!(n-k)!} \\
&= \frac{(n-1)!(k+n-k)}{k!(n-k)!} \\
&= \frac{(n-1)!n}{k!(n-k)!} \\
&= \frac{n!}{k!(n-k)!} \\
&= \binom{n}{k}
\end{aligned}$$

Definition 3.3.3 ▸ Pascal's Triangle

The binomial coefficients can be arranged in a triangular pattern which makes it easy to expand the binomial $(a+b)^n$

Example 3.3.6 ▸ Binomial Expansion

The coefficient of a^k (NOTES ON PHONE)

$$\begin{aligned}
(x-2)^4 &= \binom{4}{0}x^4(-2)^0 + \binom{4}{1}x^3(-2)^1 + \binom{4}{2}x^2(-2)^2 + \binom{4}{3}x^1(-2)^3 + \binom{4}{4}x^0(-2)^4 \\
&= 1x^4 1 + 4x^3(-2) + 6x^2(4) + 4x(-8) + 1\cdot 1\cdot 16 \\
&= x^4 - 8x^3 + 24x^2 - 32x + 16
\end{aligned}$$

Theorem 3.3.3 ▸ Binomial Theorem

For all $a, b \in \mathbb{R}$ and all $n \in \mathbb{N}$:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Proof of the Binomial Theorem is on page 53 of *Introduction to Abstract Mathematics*.

Example 3.3.7 ▸ Using Binomial Theorem

If $a, b \geq 0$ and $n \geq 2$ then:

$$(a+b)^n = a^n + na^{n-1}b + \sum_{k=0}^{n-1} \binom{n}{k} a^k b^{n-k} \geq a^n + na^{n-1}b$$

Proof. From the binomial theorem, we know:

$$\begin{aligned}(a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\ &= \binom{n}{n} a^n b^0 + \binom{n}{n-1} a^{n-1} b^1 + \sum_{k=0}^{n-2} \binom{n}{k} a^k b^{n-k} \\ &\geq a^n + na^{n-1}b \text{ remember: } \binom{n}{n-1} = 1\end{aligned}$$

□

Example 3.3.8 ▸ Using Binomial Theorem

Show that $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ for all $n \in \mathbb{N}$

Proof.

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k}$$

□

Example 3.3.9 ▸ Using Binomial Theorem

Show that $\sum_{k=0}^{n}(-1)^K\binom{n}{k} = 0$ for all $n \in \mathbb{N}$

Proof.

$$0 = 0^n = (-1+1)^n = \sum_{k=0}^{n}\binom{n}{k}(-1)^k 1^{n-k} = \sum_{k=0}^{n}(-1)^k\binom{n}{l}$$

□

3.4 Divisibility

Definition 3.4.1 ▸ Divides

For $a, b \in \mathbb{Z}$, a **divides** b if and only if $b = ac$ for some integer c.

$$a \mid b \iff \exists(c \in \mathbb{Z})(b = ac)$$

In this context, we call a the **divisor** of b. We say that a is a **proper divisor** of b if $a > 0$ and $a \neq |b|$. If $c \mid a$ and $c \mid b$ then c is a **common divisor** of a and b.

Theorem 3.4.1 ▸ 1 divides any integer

Proof. Let $b \in \mathbb{Z}$. Then $b = 1 \cdot b$, so $1 \mid b$. □

Theorem 3.4.2 ▸ Every integer divides itself and 0

Proof. Let $a \in \mathbb{Z}$. Then $a = a \cdot 1$, so $a \mid a$. Also, $0 = a \cdot 0$, so $a \mid 0$. □

Theorem 3.4.3 ▸ 0 only divides 0

Proof. If $0 \mid b$ for some $b \in \mathbb{Z}$, then $b = 0 \cdot c$ for some $c \in \mathbb{Z}$. That is, $b = 0 \cdot c = 0$, so 0 only divides 0. □

Theorem 3.4.4 ▸ If $a \mid b$, then $\pm a \mid \pm b$

Proof. Let $a \mid b$. Then $b = ac$ for some $c \in \mathbb{Z}$. Then:

- $-b = a(-c)$ where $(-c) \in \mathbb{Z}$, so $a \mid (-b)$
- $-b = (-a)c$ where $c \in \mathbb{Z}$, so $(-a) \mid (-b)$
- $b = (-a)(-c)$ where $(-c) \in \mathbb{Z}$, so $(-a) \mid b$

Therefore, $\pm a \mid \pm b$. ▢

Theorem 3.4.5 ▸ If $a \mid b$, then $a \leq b$

If $a, b \in \mathbb{N}$ and $a \mid b$, then $a \leq b$. If a is a proper divisor of b, then $a < b$.

Proof. Because $a \mid b$, we have $b = ac$ for some $c \in \mathbb{Z}$. Also, $c > 0$ because $a > 0$ and $b > 0$. Thus, $c \in \mathbb{N}$, so $c \geq 1$. Therefore, $b = ac \geq a$ by the multiplicative property.

If a is a proper divisor of b, then $a \neq b$ by definition, so $a < b$ by trichotomy. ▢

Theorem 3.4.6 ▸ Divisibility of Linear Combinations

If $a, b, c \in \mathbb{Z}$, and $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for any $m, n \in \mathbb{Z}$.

1. Write $b = ax, c = ay$ where $x, y \in \mathbb{Z}$.
2. Then find a way to write $mb + nc$ as $az$where $z \in \mathbb{Z}$.

Example 3.4.1 ▸ Simple Dividing Example

Suppose $a, b \in \mathbb{N}$ and $a \mid b$. Then $a \leq b$. Also, if a is a proper divisor of b, then $a < b$.

Proof. By definition, there exists $c \in \mathbb{Z}$ where $b = ac$. Since b and a are positive numbers, then c must also be positive. Also, since $c \geq 1$, then $b \geq a$. If a is a proper divisor, then $a \neq b$. Thus, $c > a$, so $b > a$. ▢

Definition 3.4.2 ▸ $a\mathbb{Z}$

For any $a \in \mathbb{Z}$ we define $a\mathbb{Z}$ as:

$$\begin{aligned} a\mathbb{Z} &:= \{n \in \mathbb{Z} : a \mid n\} \\ &= \{n \in \mathbb{Z} : n = ka \text{ for some } k \in \mathbb{Z}\} \end{aligned}$$

Theorem 3.4.7 ▸ $a\mathbb{Z}$ is Closed Under Addition and Multiplication

For any $a \in \mathbb{Z}$, $a\mathbb{Z}$ is closed under addition and multiplication.

Proof. Let $x, y \in a\mathbb{Z}$. By definition, $x = am$ and $y = an$ for some $m, n \in \mathbb{Z}$. Then:

$$x + y = am + an = a(m + n)$$

Since $m + n \in \mathbb{Z}$, then $a(m + n) = x + y \in a\mathbb{Z}$. Moreover:

$$xy = (am)(an) = a(man)$$

Since $man \in \mathbb{Z}$, then $a(man) = xy \in a\mathbb{Z}$. ▢

Example 3.4.2 ▸ $a\mathbb{Z}$ Example

For all $a, b \in \mathbb{Z}$, $a \mid b$ if and only if $b\mathbb{Z} \subseteq a\mathbb{Z}$.

Suppose that $a \mid b$. Then there exists some $c \in \mathbb{Z}$ such that $b = ac$. Suppose that $x \in b\mathbb{Z}$. By definition, $b \mid x$. That is, there is some $d \in \mathbb{Z}$ such that $x = bd$. Then:

$$x = bd = (ac)d = a(cd)$$

Since $cd \in \mathbb{Z}$, then $a(cd) = x \in a\mathbb{Z}$. Therefore, $b\mathbb{Z} \subseteq a\mathbb{Z}$.

Now suppose that $b\mathbb{Z} \subseteq a\mathbb{Z}$. Because $b \mid b$, we then know that $b \in b\mathbb{Z} \subseteq a\mathbb{Z}$, so $b \in a\mathbb{Z}$. Then, $a \mid b$ by definition of $a\mathbb{Z}$.

Definition 3.4.3 ▸ Parity

Parity describes whether an integer is even or odd. For any integer $n \in \mathbb{Z}$:

- n is **even** if $n = 2k$ for some $k \in \mathbb{Z}$
- n is **odd** if $n = 2k + 1$ for some $k \in \mathbb{Z}$

Theorem 3.4.8 ▸ Every integer is either even or odd

Every integer must be either even or odd, never both.

Proof. First, consider the parity of 0 and 1:

1. 0 is even since $0 = 2 \cdot 0$
2. 1 is odd since $1 = 2 \cdot 0 + 1$

Next, let's use induction for integers greater than 0. Assume that $n \in \mathbb{N}$ is either even or odd.

1. If n is even, then $n = 2k$ for some $k \in \mathbb{Z}$. Then, $n + 1 = 2k + 1$, so $n + 1$ is odd.
2. If n is odd, then $n = 2k + 1$ for some $k \in \mathbb{Z}$. Then, $n + 1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1)$, so $n + 1$ is odd.

Now, let's prove the same for negative numbers. If $n \in -\mathbb{N}$, then $-n \in \mathbb{N}$, so $-n$ is either even or odd.

1. If $-n$ is even, then $-n = 2k$ for some $k \in \mathbb{Z}$. Then $n = 2(-k)$ where $(-k) \in \mathbb{Z}$, so n is even.
2. If $-n$ is odd, then $-n = 2k + 1$ for some $k \in \mathbb{Z}$. Then $n = -(2k + 1) = 2(-k) - 1 = 2(-k - 1) + 1$. Since $(-k - 1) \in \mathbb{Z}$, then n is odd.

This completes the proof. ▢

Example 3.4.3 ▸ Addition/Multiplication of Odd Numbers

Prove that the sum of two odd integers is even, and the product of two odd integers is odd.

Proof. Let $m, n \in \mathbb{Z}$ be odd integers. Then $m = 2k+1$ and $n = 2l+1$ for some $m, n \in \mathbb{Z}$. Then:

$$\begin{aligned} m + n &= (2k+1) + (2l+1) \\ &= 2k + 2l + 2 \\ &= 2(k + l + 1) \end{aligned}$$

Since $k + l + 1 \in \mathbb{Z}$, then $m + n$ is even. Similarly:

$$\begin{aligned} mn &= (2k+1)(2l+1) \\ &= 4kl + 2k + 2l + 1 \\ &= 2(kl + k + l) + 1 \end{aligned}$$

Since $kl + k + l \in \mathbb{Z}$, then mn is odd. ▢

Example 3.4.4 ▸ Induction on Odd Integers

Prove that $7^n + 13^n$ is divisible by 5 for all odd $n \in \mathbb{N}$.

Proof. We will use induction on $k \in \mathbb{Z}$ were $n = 2k + 1$. First, if $k = 0$:

$$7^n + 13^n = 7^{2\cdot 0+1} + 13^{2\cdot 0+1} = 7^1 + 13^1 = 20 = 5(4)$$

That is, $5 \mid (7^1 + 13^1)$.

Next, Suppose that $5 \mid (7^{2k+1} + 13^{2k+1})$ for some $k \in \mathbb{Z}$ where $k \geq 0$. Then:

$$\begin{aligned} 7^{2(k+1)+1} + 13^{2(k+1)+1} &= 7^{2k+3} + 13^{2k+3} \\ &= 7^2 + 7^{2k+1} \\ &= 7^2 \cdot 7^{2k+1} + 13^2 \cdot 13^{2k+1} \\ &= 49 \cdot 7^{2k+1} + 169 \cdot 13^{2k+1} \\ &= 49(7^{2k+1} + 13^{2k+1}) + 120 \cdot 13^{2k+1} \end{aligned}$$

By the induction assumption, we know that $7^{2k+1} + 13^{2k+1} = 5c$ for some $c \in \mathbb{Z}$. Thus:

$$\begin{aligned} 7^{2k+3} + 13^{2k+3} &= 49(7^{2k+1} + 13^{2k+1}) + 120 \cdot 13^{2k+1} \\ &= 49(5c) + 5(24 \cdot 13^{2k+1}) \\ &= 5(49c + 24 \cdot 13^{2k+1}) \end{aligned}$$

Because $(49c + 24 \cdot 13^{2k+1}) \in \mathbb{Z}$, then $5 \mid (7^{2k+3} + 13^{2k+3})$. Therefore, $5 \mid (7^n + 13^n)$ for all odd integers n. ▢

Definition 3.4.4 ▸ Greatest Common Divisor

Given $a, b \in \mathbb{Z}$, the **greatest common divisor** of a and b is (informally) the largest integer d that divides both a and b.

$$d = \gcd(a, b)$$

Theorem 3.4.9 ▸ Greatest Common Divisors

If $a, b \in \mathbb{Z}$, then there is a common divisor d of a and b such that:

1. $d = am + bn$ for some $mn \in \mathbb{Z}$
2. d is non-negative
3. every common divisor of a and b divides d
4. if a and b are not both zero, and c is a common divisor of a and b, then $c \leq d$

If a and b are not both zero, then the divisor d is called the **greatest common divisor** of a and b, denoted $d = \gcd(a, b)$.

Proof. We will first prove that d exists when both $a, b \geq 0$. Let's assume without loss of generality that $a \leq b$ (i.e. if $a \not\leq b$, swap the two and continue the proof).

1. If $a = 0$, then $b \mid a$ and $b \mid b$, so b is a common divisor of a and b. Then, we can choose d as a linear combination of a and b:

$$d = 0 \cdot a + 1 \cdot b = b$$

Let $a + b = k$, and let $P(k)$ be the statement: "If $a + b = k$, then there is a common divisor d of a and b such that $d = ma + nb$ for $mn \in \mathbb{Z}$"

Base Case: If $k = 0$, then $a = b = 0$, so $P(0)$ is true from above.

S.I. Hypothesis: Suppose that $P(k)$ is true for $0 \leq k \leq n$ where $n \geq 0 \in \mathbb{Z}$.

Let $a, b \geq 0 \in \mathbb{Z}$ such that $a + b = n + 1$. If $a = 0$, then we are done. Otherwise, $1 \leq a \leq b$, so $0 \leq b - a < b$. Let $c = b - a$. Then:

$$a + c = a + b - a = n + 1 - a \leq n$$

By our induction hypothesis, there is a common divisor d of a and c, and there exist $m, n \in \mathbb{Z}$ such that:

$$\begin{aligned} d &= ma + nc \\ &= ma + n(b - a) \\ &= (m - n)a + nb \end{aligned}$$

Because d is the common divisor of a and $b-a$, then d also divides any linear combination of a and $b-a$, primarily $a+(b-a)=b$. Thus d is a common divisor of a and b, and $d=am+bn$ for some $m,n\in\mathbb{Z}$. That is, $P(n+1)$ is true by strong induction. In particular, property 1 holds.

2. If the common divisor d from part 1 is negative, then $-d>0$ is also a common divisor of a and b. Also, $-d=a(-m)+b(-n)$ where $-m,-n\in\mathbb{Z}$. Thus, we can assume that $d\geq 0$.

3. Let c be a common divisor of a and b. Then $c\mid(am+bn)$ for all $m,n\in\mathbb{Z}$, so in particular, $c\mid d$.

4. Suppose that at least one of a and b is not zero. Let c be a common divisor of a and b. Then $c\neq 0$ (otherwise, $a=b=0$).

   - If $c<0$, then $c<d$ because $d\geq 0$.
   - If $c>0$, then a and b are both non-negative, and $d>0$. Consequently, $c,d\in\mathbb{N}$. We know $c\mid d$ from part 3, so $c\leq d$.

□

Example 3.4.5 ▸ Rational Numbers

Let $r\neq 0$ and $r\in\mathbb{Q}$. Then $r=m/n$ where $m,n\in\mathbb{Z}$ and $\gcd(m,n)=1$.

Proof. Because $r\in\mathbb{Q}$ and $r\neq 0$, we can write $r=a/b$ where $a,b\in\mathbb{Z}$ and $a,b\neq 0$. By Theorem 3.4.9, there exists $d=\gcd(a,b)$ where $a=md$ and $b=nd$. Thus:

$$r=\frac{a}{b}=\frac{md}{nd}=\frac{m}{n}$$

Suppose for contradiction that $k:=\gcd(m,n)>1$. Then $m=kp$ and $n=kq$ for some $p,q\in\mathbb{Z}$. Thus:

$$a=md=(kp)d=p(kd)$$

$$b=nd=(kq)d=q(kd)$$

That is, kd is a common divisor of a and b, and $kd>d$ since $k>1$. This contradicts our assumption that d was the greatest common divisor of a and b. Therefore, $\gcd(m,n)\leq 1$. Since gcd is non-negative and both a and b are non-zero, then $\gcd(m,n)=1$. □

Example 3.4.6 ▸ $\sqrt{2}$ is irrational

Proof. Suppose for contradiction that $r^2 = 2$ for some $r \in \mathbb{Q}$ where $r > 0$. Then $r = a/b$ where $\gcd(a, b) = 1$. Now, $r^2 = a^2/b^2 = 2$, so $a^2 = 2b^2$. This means that a^2 is even. Thus, by Exercise 3.25, a is also even. Hence, $a = 2c$ for some $c \in \mathbb{Z}$. Thus:

$$\begin{aligned}(2c)^2 &= 2b^2\\ 4c^2 &= 2b^2\\ 2c^2 &= b^2\end{aligned}$$

Similarly, since b^2 is even, b is also even. Then, $b = 2d$ for some $d \in Z$. That is, 2 is a common divisor of a and b, so $\gcd(a, b) \geq 2$. This contradicts our assumption that $gcd(a, b) = 1$. Therefore, $\sqrt{2}$ is not rational. ▢

3.5 Prime Factorization

Theorem 3.5.1 ▸ Division Algorithm

For all real numbers $0 < d < a$, there exists a unique integer q (the **quotient**) and a unique real number r (the **remainder**) such that $0 \leq r < d$ and $a = qd + r$

Proof. Let $E = \{m \in \mathbb{Z} : md \leq a\}$. We know E is nonempty since both 0 and 1 must be in this set. Also, E bounded above by a/d. Therefore, by the Well-Ordering Principle for $\mathbb{Z}$, E has a maximum. Let $q := \max E$, so $qd \leq a$. Let $r = a - qd \geq 0$. Because $q + 1 \notin E$, we know that $(q+1)d > a$, so $qd + d > a$, so $qd + d > a$, and thus $r = a - qd < d$. That is, $0 \leq r < d$ and $a = qd + r$. This proves the existence of q and r.

To prove uniqueness, assume that q' and r' satisfy the Division Algorithm. That is:

$$0 \leq r' < d \quad \text{and} \quad a = q'd + r'$$

We need to show $q = q'$ and $r = r'$. Assume without loss of generality that $q' \leq q$. Thus:

$$(q - q')d = qd - q'd = (a - r) - (a - r') = r' - r$$

(The first $a = qd + r$ and the second $a = q'd + r'$). We know $r \geq 0$ and $r' < d$, so $r' - r < d$. Also, $d \mid (r' - r)$, so either $d \leq r' - r$ which is a contradiction. Thus, $r' - r = 0$, so $r' = r$. Thus $(q - q')d = 0$ and $d \neq 0$, so $q - q' = 0$. That is, $q = q'$. Therefore, the quotient ad the remainder in the division algorithm are unique. □

A more general version where we allow $a \leq 0$ is the following:

"If $a, d \in R$ where $d \neq 0$, then there exists a unique $q \in \mathbb{Z}$ and a unique $r \in R$ such that $0 \leq r < |d|$ and $a = qd + r$".

Example 3.5.1 ▸ Using Uniqueness of the Division Algorithm

Prove that if $a, b \in \mathbb{N}$ where $a, b > 1$, then $ab + 1$ is **not** divisible by a or b.

Proof. Suppose for contradiction that $a \mid (ab+1)$. Then there exists $c \in \mathbb{Z}$ where $ab+1 = ac$. This violates the uniqueness of the division algorithm. Let $m \coloneqq ab + 1$. Then:

$$m = \underbrace{b}_{\text{quotient}} \cdot a + \underbrace{1}_{\text{remainder}}$$

$$m = \underbrace{c}_{\text{quotient}} \cdot a + \underbrace{0}_{\text{remainder}}$$

Because we have two **different** remainders when dividing m by a, this violates the uniqueness of the division algorithm. Therefore, $ab + 1$ is **not** divisible by a.

A similar proof shows $ab + 1$ is not divisible by b. ▢

Definition 3.5.1 ▸ Prime Numbers

A natural number p is **prime** if $p > 1$ and p has no proper divisors.

Theorem 3.5.2 ▸ Infinite Primes

There are an infinite number of prime numbers.

Proof. Suppose for contradiction that there are a finite number of primes.

$$p_1, p_2, \dots, p_k$$

Let $n = p_1 p_2 \cdot p_k + 1$. As we proved previously, none of the p_i divide n. Hence, either n is prime, or there exists a prime number q that divides n but q does not equal any p_i. ▢

Definition 3.5.2 ▸ Prime Factorization

For a natural number $a \geq 2$, a **prime factorization** of a is a product $a = p_1 p_2 \cdots p_k$ where each p_i is prime and $p_1 \leq p_2 \leq \cdots \leq p_k$.

Ordering on the primes guarantees that each natural number $n \geq 2$ has a unique prime factorization. The prime numbers themselves are not necessarily distinct.

Theorem 3.5.3 ▸ Existence of Prime Factorization

Every natural number can be written as a product of primes.

Proof. Note that $n = 1$ is an **empty product**. Also, $n = 2$ is prime, so 2 can be written as a product of primes.

Assume that for some $n \geq 2$, every natural number $2 \leq k \leq n$ can be written as a product of primes.

- If $n + 1$ is prime, then $n + 1$ is automatically a product of primes.
- If $n + 1$ is not prime, then $n + 1 = ab$ where a and b are proper divisors of $n + 1$ (i.e. $2 \leq a \leq n$ and $2 \leq b \leq n$). By the induction hypothesis, each of a and b can be written as a product of primes.

$$a = p_1 p_2 \cdots p_k$$

$$b = q_1 q_2 \cdots q_l$$

Hence, $n + 1 = ab = (p_1 p_2 \cdots p_k)(q_1 q_2 \cdots q_l)$, so $n + 1$ is a product of primes.

By principle of strong induction, our theorem holds. ▢

Theorem 3.5.4 ▸ Fundamental Theorem of Arithmetic

Every natural number $a \geq 2$ has a unique prime factorization.

Proof. Let $a \in \mathbb{N}$ where $a \geq 2$. We know a prime factorization for a exists from our previous proof. If some natural number does not have a unique prime factorization, then by the Well-Ordering Principle there exists a smallest such number. Assume $a \geq 2$ is the smallest natural number with more than 1 prime factorization. That is, we can write a as:

$$\begin{aligned} a = p_1 p_2 \cdots p_k \quad &\text{where} \quad p_1 \leq p_2 \leq \cdots \leq p_k \quad \text{and} \\ a = q_1 q_2 \cdots q_l \quad &\text{where} \quad q_1 \leq q_2 \leq \cdots \leq q_l \end{aligned}$$

where $p_i \neq q_i$ for some $i \in \mathbb{Z}$. Now we need to show that these two prime factorizations are different. Assume for contradiction that $p_1 = q_1$. Then, $p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_l < a$. We then have a natural number smaller than a with two distinct prime factorizations. Hence, this contradicts our choice of a as the smallest such number. Therefore, we know $p_1 \neq q_1$.

Next, without loss of generality, we can assume that $p_1 < q_1$ (i.e. if $p_1 > q_1$, swap all p_i with q_i and continue). By the Division Algorithm, we can write $q_1 = qp_1 + r$ where $q_1 r \in \mathbb{N}$ and $0 < r < p_1$. (If $r = 0$, then $q_1 = qp_1$, giving q_1 a proper divisor, so $r \neq 0$.)

Let $w = rq_2 q_3 \cdots q_l < a$ (because $r < p_1 < q_1$). Because $r < p_1$ and $p_1 < q_i$ for all $i \in \mathbb{Z}$ such that $2 \leq i \leq l$, then the prime p_1 does not appear in this product. But:

$$\begin{aligned} w &= rq_2 q_3 \cdots q_l \\ &= (q_1 - qp_1) q_2 q_3 \cdots q_l \\ &= q_1 q_2 \cdots q_l - qp_1 q_2 q_3 \cdots q_l \\ &= p_1 p_2 \cdots p_k - qp_1 q_2 q_3 \cdots q_l \\ &= p_1 (p_2 p_3 \cdots p_k - q\, q_2 q_3 \cdots q_l) \end{aligned}$$

Thus, by writing $p_2 p_3 \cdots p_k - qq_2 q_3 \cdots q_l$ as a product of primes, we will have a prime factorization of w that contains p_1. That is, $w < a$ has two distinct prime factorizations. This contradicts a being the smallest number with two distinct prime factorizations. Therefore, every $n \in \mathbb{N}$ where $n \geq 2$ has a unique prime factorization. ▢

Consequences of Unique Prime Factorizations

- If $a \in \mathbb{N}$ and p is a prime such that $p \mid a$, then p is in the prime factorization of a.
- If $a, b \in \mathbb{N}$ and $a, b \geq 2$, then the factors in the prime factorization of ab consist of precisely one prime for each instance of a prime in the prime factorizations of a and b.
- Suppose that $p \in \mathbb{N}$ where $p \geq 2$. Then p is prime if and only if the following property holds: "If $a, b \in \mathbb{N}$ and $p \mid ab$, then $p \mid a$ or $p \mid b$. In particular, if $p \mid a^2$ then $p \mid a$".

4 Additional Topics

In this chapter, we will introduce new concepts build on past concepts. Primarily, we will take a closer look at functions and their properties.

Overview

- Injective, surjective, and bijective functions as well as function inverses and compositions
- Relations, equivalence relations, and equivalence classes
- Modular congruence/equivalence, modular arithmetic using equivalence classes
- Cardinality of finite sets, Principle of Inclusion and Exclusion, Pigeonhole Principle
- Cardinality of infinite sets and countability

4.1 One-to-one and Onto Functions

Definition 4.1.1 ▸ One-to-one Function

A function $f : X \to Y$ is **one-to-one** (injective) if:

$$\forall (x_1, x_2 \in X)\,[f(x_1) = f(x_2) \implies x_1 = x_2]$$

Note that the converse statement $x_1 = x_2 \implies f(x_1) = f(x_2)$ is automatically true by definition of a function.

Definition 4.1.2 ▸ Onto Function

A function $f : X \to Y$ is **onto** (surjective) if:

$$\forall (y \in Y) \exists (x \in X)(f(x) = y)$$

Definition 4.1.3 ▸ Bijective Function

A function $f : X \to Y$ is **bijective** if f is both one-to-one and onto.

Example 4.1.1

$f : X \to Y$ is an onto function if and only if $f[X] = Y$

Proof. First, suppose $f : X \to Y$ is onto. By definition of a function, $f[X] \subseteq Y$, so we need to show $Y \subseteq X$. Let $y \in Y$ be arbitrary. Because f is onto, then there exists $x \in X$ such that $f(x) = y$. That is, $y \in f[X]$, so $Y \subseteq f[X]$. Therefore, $f[X] = Y$.

Next, suppose $f[X] = Y$, and let $y \in Y$ be arbitrary. Then $y \in f[X]$, so $y = f(x)$ for some $x \in X$. Because this is true for all $y \in Y$, then f is an onto function. ▢

Example 4.1.2

If $f : X \to Y$ is a one-to-one function, then $f(A \cap B) = f[A] \cap f[B]$ for all $A, B \subseteq X$.

Proof. From section 1.3, we know that $f(A \cap B) \subseteq f[A] \cap f[B]$. Suppose f is one-to-one. Let $y \in f[A] \cap f[B]$. That is, $y \in f[A]$ and $y \in f[B]$. Thus, there exists some $x_1 \in A$ such that $f(x_1) = y$, and there exists some $x_2 \in B$ such that $f(x_2) = y$. That is, $f(x_1) = f(x_2)$. Because f is one-to-one, that means $x_1 = x_2$. Hence, $x_1 \in A \cap B$, so $y = f(x_1) \in f(A \cap B)$. Therefore, $f[A] \cap f[B] \subseteq f(A \cap B)$. ▢

Example 4.1.3

$f : X \to Y$ is an onto function if and only if $f(f^{-1}[B]) = B$ for all $B \subseteq Y$.

Proof. First, assume f is an onto function. From section 1.3, we know that $f(f^{-1}[B]) \subseteq B$ for all $B \subseteq Y$. Let $y \in B$. Because f is onto, there exists $x \in X$ such that $f(x) = y$. Because $y \in B$, then $x \in f^{-1}[B]$. Thus, we can apply the image to both sides to attain $y = f(x) \in f(f^{-1}[B])$. Therefore, $B \subseteq f(f^{-1}[B])$, so $B = f(f^{-1}[B])$.

Next, assume that $f(f^{-1}[B]) = B$ for all $B \subseteq Y$. Let $y \in Y$ be arbitrary. If $y \in B$, then by our initial assumption, $y \in f(f^{-1}[B])$. Thus, there exists $x \in f^{-1}[B]$ such that $f(x) = y$. But then $x \in X$ and $f(x) = y$, so f is onto. ▢

Example 4.1.4

$f : X \to Y$ is one-to-one if and only if $f^{-1}(f[A]) = A$ for all $A \subseteq X$.

Proof. Assume f is one-to-one. From section 1.3, we know that $A \subseteq f^{-1}(f[A])$ for all $A \subseteq X$. Let $x_1 \in f^{-1}(f[A])$. Then $f(x_1) \in f[A]$, so there exists $x_2 \in A$ such that $f(x_1) = f(x_2)$. Because f is one-to-one, then $x_1 = x_2$. Consequently, $x_1 \in A$. Therefore, $f^{-1}(f[A]) \subseteq A$, so $f^{-1}(f[A]) = A$.

Suppose that $f^{-1}(f[A]) = A$ for all $A \subseteq X$. We need to show that as a consequence, f is a one-to-one function. Let $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$. Let $A = \{x_1\}$. By assumption:

$$\begin{aligned} f^{-1}(f[A]) &= \{x \in X : f(x) \in f[A]\} \\ &= \{x \in X : f(x) = f(x_1)\} \end{aligned}$$

Because $x_2 \in X$ and $f(x_2) = f(x_1)$, then $x_2 \in f^{-1}(f[A])$. By our initial assumption, we also have $x_2 \in A$. However, we defined A as having only one distinct element. As such, $x_1 = x_2$ and $f(x_1) = f(x_2)$, satisfying the definition of a one-to-one function. ▢

Definition 4.1.4 ▸ Inverse Function

Let $f : X \to Y$ be a function. A function $g : Y \to X$ is an inverse of f if:

1. $\forall(y \in Y)(f(g(y)) = y)$
2. $\forall(x \in X)(g(f(x)) = x)$

The standard notation for the inverse of $f : X \to Y$ is f^{-1}. This is consistent with our earlier definition of $f^{-1}[B]$ as the inverse image of $B \subseteq Y$. It is possible that the inverse of a function does not exist, but we can still apply the inverse image to subsets of the co-domain.

Example 4.1.5

Show that if g is an inverse of f, then f is an inverse of g

Proof. Because g is an inverse function of f, we know that $g : Y \to X$ satisfies $f(g(y)) = y$ for all $y \in Y$, and $g(f(x)) = x$ for every $x \in X$. But then $f : X \to Y$ satisfies $g(f(x)) = x$ for $x \in X$, and $f(g(y)) = y$ for all $y \in Y$. That is, f is an inverse of g. ▢

Theorem 4.1.1 ▸ Existence of Inverse Functions

Let $f : X \to Y$ be a function. Then f has an inverse if and only if f is bijective.

Proof. We will need to prove both directions of the logical equivalence. First, let's assume that $f : X \to Y$ has an inverse function called $g : Y \to X$. Then:

- $\forall (y \in Y)\,[f(g(y)) = y]$, and
- $\forall (x \in X)\,[g(f(x)) = x]$

We need to show f is both one-to-one and onto. Let $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$. Then:

$$\begin{aligned} x_1 &= g(f(x_1)) \\ &= g(f(x_2)) \\ &= x_2 \end{aligned}$$

Thus, f is a one-to-one function.

Let $y \in Y$. Then $y = f(g(y))$ and $g(y) \in X$. Thus, f is an onto function. Since f is both one-to-one and onto, then f is a bijective function.

Next, we need to prove the converse statement. Suppose that f is a bijective function. Then f is onto, so for any $y \in Y$ there exists $x \in X$ such that $y = f(x)$. Define $g : Y \to X$ by $\underbrace{g(y) = x \text{ if and only if } y = f(x)}_{\text{only works for one-to-one}}$. That is:

1. If $f(x) = y$, then $g(f(x)) = g(y) = x$ for all $x \in X$.
2. If $g(y) = x$, then $f(g(y)) = f(x) = y$ for all $y \in Y$.

Therefore, g is an inverse function of f. ▢

Theorem 4.1.2 ▸ Uniqueness of Inverse Functions

If $f : X \to Y$ has an inverse, then the inverse is unique.

Suppose that $g_1 : Y \to X$ and $g_2 : Y \to X$ are both inverse functions of $f : X \to Y$. We need to prove $g_1 = g_2$ by showing that for every $y \in Y$ $g_1(y) = g_2(y)$. Let $y \in Y$. Because f is onto, there is some $x \in X$ such that $y = f(x)$. Then:

$$\begin{aligned} g_1(y) &= g_1(f(x)) \\ &= x \\ &= g_2(f(x)) \\ &= g_2(y) \end{aligned}$$

Therefore, $g_1 = g_2$, so f has a unique inverse.

Example 4.1.6

Let $f : X \to Y$ be surjective (onto), and let $g : Y \to X$ satisfy $g(f(x)) = x$ for all $x \in X$. Show that f is bijective and that $g = f^{-1}$.

Proof. We already know that f is onto, so we only need to show that f is one-to-one. Let $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$. Then:

$$\begin{aligned} x_1 &= g(f(x_1)) \\ &= g(f(x_2)) \\ &= x_2 \end{aligned}$$

Thus, f is one-to-one and is therefore a bijective function.

Next, we need to show $g = f^{-1}$ (i.e. $f(g(y)) = y$ for all $y \in Y$). Note that f is onto, so for any $y \in Y$ there exists $x \in X$ such that $f(x) = y$. Therefore:

$$\begin{aligned} f(g(y)) &= f(g(f(x))) \\ &= f(x) \\ &= y \end{aligned}$$

Thus, g is the inverse function of f. ▢

Definition 4.1.5 ▸ Composition

If $f : X \to Y$ and $g : Y \to Z$ are functions, then the **composition** of f and g is the function $g \circ f : X \to Z$ where $(g \circ f)(x) = g(f(x))$.

Example 4.1.7

Suppose that $f : X \to Y$ and $g : Y \to Z$ are functions such that g is one-to-one and $g \circ f$ is onto. Show that f is also onto.

Proof. Let $y \in Y$. Then $g(y) = z$ for some $z \in Z$. Because $g \circ f$ is onto, there exists $x \in X$ such that $(g \circ f)(x) = g(f(x)) = z$. That is, $g(y) = g(f(x))$. Because g is one-to-one, we have $y = f(x)$ where $x \in X$. Therefore, f is an onto function. ▢

Example 4.1.8 ▸ Composition Preserves Injectivity

Show that if $f : X \to Y$ and $g : Y \to Z$ are both one-to-one, then $g \circ f$ is one-to-one.

Proof. Let $x_1, x_2 \in X$ such that $(g \circ f)(x_1) = (g \circ f)(x_2)$. That is, $g(f(x_1)) = g(f(x_2))$. Because g is one-to-one, we have $f(x_1) = f(x_2)$. Because f is one-to-one, we have $x_1 = x_2$. Therefore, $g \circ f$ is one-to-one. ▢

Example 4.1.9 ▸ Composition Preserves Surjectivity

Suppose that $f : X \to Y$ and $g : Y \to Z$ are functions such that $g \circ f$ is one-to-one.

We can prove f is one-to-one.

Proof. Let $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$. Then $g(f(x_1)) = g(f(x_2))$, so $(g \circ f)(x_1) = (g \circ f)(x_2)$. Because $g \circ f$ is one-to-one, then $x_1 = x_2$. Therefore, f is one-to-one. ▢

However, g is not necessarily one-to-one.

Definition 4.1.6 ▸ Identity Function

For a non-empty set A, the identity function on A is the function $\mathrm{id}_A : A \to A$ defined by:

$$\forall (a \in A)(\mathrm{id}_A(a) = a)$$

This allows us to rephrase the definition of an inverse function as follows:

Let $f : X \to Y$ be a function. A function $g : Y \to X$ is an inverse of f if:

$$g \circ f = \mathrm{id}_X \quad \text{and} \quad f \circ g = \mathrm{id}_Y$$

4.2 Equivalence Relations

Recall that for two sets X and Y the **Cartesian product** $X \times Y$ is the set of ordered pairs where

$$X \times Y = \{(x, y) : x \in X \text{ and } y \in Y\}$$

Definition 4.2.1 ▸ Relation

A **relation** on $X \times Y$ is any subset of $X \times Y$.

A **relation** on X is any subset of $X \times X$.

Note that any function is also a relation. Recall the formal definition of a function f:

$$f = \{(x, y) : y = f(x)\} \subseteq X \times Y$$

We use a special notation for functions where $(x, y) \in f$ can be written as $y = f(x)$. Non-function relations also have a special notation:

$$(x, y) \in R \iff \underbrace{x \, R \, y}_{\text{“}x \text{ is related to } y\text{”}}$$

That is, $R = \{(x, y) : x \, R \, y\}$.

Example 4.2.1

Let $L \coloneqq \{(x, y) : x, y \in \mathbb{R}, x < y\} \subseteq \mathbb{R}^2$. Then:

$$(x, y) \in L \iff x \, L \, y \iff x < y$$

Definition 4.2.2 ▸ Equivalence Relation

Let X be a non-empty set, and let R be a relation on X. R is an **equivalence relation** if:

1. R is **reflexive** $\quad \forall(x \in X)(x \; R \; x)$
2. R is **symmetric** $\quad x \; R \; y \implies y \; R \; x$
3. R is **transitive** $\quad x \; R \; y \wedge y \; Z \; z \implies x \; R \; z$

An equivalence relation is often denoted using the symbol $\sim$.

Example 4.2.2 ▸ Equivalence Relations

1. $R = \{(a, b) \in \mathbb{N}^2 : a \mid b\}$

   $a|a$ for all $a \in \mathbb{N}$, so R is reflexive. Also, if $a \mid b$ and $b \mid c$, then $a \mid c$, so R is transitive. However, $2 \mid 4$ but $4 \nmid 2$, so R is not symmetric. Therefore, R is not an equivalence relation.

2. For $x, y \in \mathbb{R}$, $x \; R \; y$ if $x^2 = y^2$

   $x^2 = x^2$ so $x \; R \; x$ and thus R is reflexive. Also, if $x^2 = y^2$ then $y^2 = x^2$, so R is symmetric. And, if $x^2 = y^2$ and $y^2 = z^2$ then $x^2 = z^2$, so R is also transitive. Therefore, R is an equivalence relation.

Example 4.2.3 ▸ Reflexivity, Symmetry, and Transitivity

For $x, y \in \mathbb{R}$, define $x \; R \; y$ to mean that $|x - y| < 1$

1. $|x - x| = 0 < 1$, so R is reflexive.
2. $|x - y| = |y - x|$, so if $|x - y| < 1$ then $|y - x| < 1$. That is, R is symmetric.
3. $|0 - 0.5| = 0.5$ so $0 \; R \; 0.5$, and $|0.5 - 1| = 0.5 < 1$ so $0.5 \; 1$. However, $|0 - 1| = 1$, so $0 \not R \; 1$. Thus, R is not transitive.

Example 4.2.4 ▸ Proving a Relation is an Equivalence Relation

Suppose that the relation R on X is reflexive, and satisfies the "twisted transitive law":

$$\forall(x, y, z \in X)(x \ R \ y \wedge x \ R \ z \implies y \ R \ z)$$

Show that R is an equivalence relation.

Proof. Let R be a relation on X that is reflexive and satisfies the "twisted transitive law". We need to show that the relation is symmetric and transitive. Let $x, y, z \in X$ be arbitrary.

1. Assume $x \ R \ y$. Since R is reflexive, then $x \ R \ x$. Then by the "twisted transitive law", $y \ R \ x$. Thus, R is symmetric.
2. Assume $x \ R \ y$ and $y \ R \ z$. Then $y \ R \ x$ because R is symmetric. Applying the "twisted transitive law" to $y \ R \ x$ and $y \ R \ z$ gives $x \ R \ z$. Thus, R is transitive.

Therefore, R is an equivalence relation. □

Definition 4.2.3 ▸ Equivalence Class

Suppose that $\sim$ is an equivalence relation on X. For each $x \in X$, the set

$$\overline{x} = \{y \in X : x \sim y\}$$

is called the **equivalence class** of x.

Theorem 4.2.1 ▸ Distinct Equivalence Classes

Let X be a set with equivalence relation $\sim$. If $x, y \in X$ and $\overline{x} \cap \overline{y} \neq \emptyset$, then $\overline{x} = \overline{y}$.

Proof. Since $\overline{x} \cap \overline{y} \neq \emptyset$, then there exists some $w \in \overline{x} \cap \overline{y}$. That is, $w \in \overline{x}$ and $w \in \overline{y}$, so $x \sim w$ and $y \sim w$. Suppose $z \in \overline{x}$. Then $x \sim z$ and $z \sim x$. Since $z \sim x$ and $x \sim w$, then by transitivity, $z \sim w$. By symmetry, $w \sim z$. From $y \sim w$ and $w \sim z$ we have $y \sim z$ by transitivity. Thus, $z \in \overline{y}$. Therefore, $\overline{x} \subseteq \overline{y}$. By a similar argument, we can also prove $\overline{y} \subseteq \overline{x}$, so $\overline{x} = \overline{y}$. □

If any two equivalence classes intersect each other, then they must be the same equivalence class. Two distinct equivalence classes are always disjoint.

Example 4.2.5

If X is a set with equivalence relation $\sim$, $y \in \overline{x}$, then $\overline{x} = \overline{y}$.

Proof. Because $\sim$ is reflexive, we know that $y \in \overline{y}$. That is, $\overline{x} \cap \overline{y} \neq \emptyset$. Therefore, $\overline{x} = \overline{y}$ by the previous theorem. ▢

Definition 4.2.4 ▸ Partition

A **partition** of a set X is a collection P of subsets of X such that:

1. for all $x \in X$, there exists $A \in P$ such that $x \in A$, and
2. if $A, B \in P$ and $A \cap B \neq \emptyset$, then $A = B$.

That is, a partition of X divides X into disjoint subsets that cover X. No two distinct subsets of a partition may contain any same elements.

Also note that no two equivalence classes of a set will contain any same elements. If we have an equivalence relation on X, then grouping each element of X into its respective equivalence class forms a partition of X. If X is a set with equivalence relation $\sim$, then the equivalence classes form a partition of X.

Given a nonempty set X, there are two "trivial" equivalence relations:

1. $x \sim y$ if and only if $x = y$

   In this case, equivalence classes are the sets $\overline{x} = \{x\}$.

2. $x \sim y$ for all $x, y \in X$

   In this case, there is only one distinct equivalence class where $\overline{x} = X$ for all $x \in X$.

Example 4.2.6

For two sets A and B, define $A \sim B$ to mean that there is a bijection $f : A \to B$. Show that $\sim$ is an equivalence relation.

Proof. For a set A, the function $\mathrm{id}_A : A \to A$ is a bijection, so $\sim$ is reflexive.

Suppose that $A \sim B$. That is, there exists a bijection $f : A \to B$. Then $f^{-1} : B \to A$ is a bijection, so $B \sim A$. Thus, $\sim$ is symmetric.

Suppose that $A \sim B$ and $B \sim C$. That is, there exists a bijection $f : A \to B$ and a bijection $g : B \to C$. Then $g \circ f : A \to C$ is a bijection. Thus, $\sim$ is transitive.

Therefore, $\sim$ is an equivalence relation. ▢

4.3 Modular Arithmetic

Definition 4.3.1 ▸ Modular Equivalence

For $m, n \in \mathbb{Z}$ and $k \in \mathbb{N}$, we say that m **is equivalent to** n **modulo** k if $k \mid (m - n)$.

$$\underbrace{m \equiv n \pmod{k}}_{\text{“}m \text{ is equivalent to } n \bmod k\text{”}} \iff \underbrace{k \mid (m-n)}_{m-n=kc \text{ for } c \in \mathbb{Z}}$$

Note that modular equivalence is an equivalence relation on $\mathbb{Z}$.

1. Reflexive: For $m \in \mathbb{Z}$, $m - m = 0 \cdot k$, so $m \equiv m \pmod{k}$
2. Symmetric: If $m \equiv n \pmod{k}$, then $m - n = kc$ for some $c \in \mathbb{Z}$. Thus, $n - m = k(-c)$ where $c \in \mathbb{Z}$, so $n \equiv m \pmod{k}$.
3. Transitive: If $l \equiv m \pmod{k}$ and $m \equiv n \pmod{l}$, then $l - m = ka$ and $m - n = kb$ where $a, b \in \mathbb{Z}$. That is:

$$l - n = (l - m) + (m - n) = ka + kb = k(a + b) \in \mathbb{Z}$$

Therefore, $l \equiv n \pmod{k}$.

The set of equivalence classes modulo k is denoted $\mathbb{Z}_k$.

Example 4.3.1 ▸ $\mathbb{Z}_2$

In $\mathbb{Z}_2$, we will have two equivalence classes, $\overline{0}$ and $\overline{1}$. That is, $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$

$$\overline{0} = \{x \in \mathbb{Z} : 2 \mid (x-0)\} = \{\dots, -4, -2, 0, 2, 4, \dots\}$$
$$\overline{1} = \{x \in \mathbb{Z} : 2 \mid (x-1)\} = \{\dots, -3, -1, 1, 3, 5, \dots\}$$

Similarly, $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$.

Theorem 4.3.1 ▸ $Z_k = \{\overline{0}, \dots, \overline{k-1}\}$

For all $k \in \mathbb{N}$, $\mathbb{Z}_k = \{\overline{0}, \overline{1}, \dots, \overline{k-1}\}$, and these equivalence classes are distinct.

Proof. Let $m \in \mathbb{Z}$. By the division algorithm, we can write $m = qk + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r \leq k-1$. Then, $m - r = qk$, so $m \equiv r \pmod{k}$. That is $\overline{m} = \overline{r}$, so $\overline{m}$ is one of the classes $\overline{0}, \overline{1}, \dots, \overline{k-1}$. Suppose for contradiction $\overline{m} = \overline{n}$ where $0 \leq n < m \leq k-1$. Because they are the same equivalence class, then $k \mid (m-n)$. However, $k > m - n$ which contradicts $k \mid (m-n)$. Thus, the classes $\overline{0}, \overline{1}, \dots, \overline{k-1}$ are all distinct. ▢

Moreover, for any $k \in \mathbb{N}$ and $m \in \mathbb{Z}$, we have $\overline{m} = \overline{0}$ in $\mathbb{Z}_k$ if and only if $k \mid m$.

Example 4.3.2

In $\mathbb{Z}_6$:

$$\overline{0} = \{\dots, -12, -6, 0, 6, 12, \dots\} = \{m \in \mathbb{Z} : 6 \mid m\}$$

- $\overline{19} = \overline{1}$ because $19 = 3 \cdot 6 + 1$
- $\overline{43} = \overline{1}$ because $43 = 7 \cdot 6 + 1$
- $\overline{-38} = \overline{4}$ because $-38 = -7 \cdot 6 + 4$

To perform arithmetic in $\mathbb{Z}_k$, we need to define addition and multiplication.

Definition 4.3.2 ▸ Modular Addition

For $\overline{x}, \overline{y} \in \mathbb{Z}_k$, **modular addition** is defined as:

$$\overline{x} + \overline{y} \coloneqq \overline{x + y}$$

Also, we need to check that these operations are **well-defined**.

This operation is well-defined if:

$$\overline{x} = \overline{w} \wedge \overline{y} = \overline{z} \implies \overline{x+y} = \overline{w+z}$$

Since there are many elements we can choose to "represent" an equivalence class in our definition of Modular Addition, we need to ensure that every possible choice follows the definition.

If $\overline{x} = \overline{w}$, then $x - w = ak$ for some $a \in \mathbb{Z}$. Similarly, if $\overline{y} = \overline{z}$, then $y - z = bk$ for some $b \in \mathbb{Z}$.

$$\begin{aligned}(x+y)-(w+z) &= (x-w)+(y-z)\\ &= ak + bk\\ &= (a+b)k, \quad \text{where } a+b \in \mathbb{Z}\end{aligned}$$

Thus, $x + y \equiv w + z \pmod{k}$, so $\overline{x+y} = \overline{w+z}$.

Similarly, we can show that $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$ is well-defined.

For all $k \in \mathbb{N}$, the set $\mathbb{Z}_k$ with addition and multiplication satisfies the field axioms except possibly the existence of multiplicative inverses.

Example 4.3.3 ▸ $\mathbb{Z}_3$ is a Field

$\mathbb{Z}_3$ is a field.

Proof. All we need to show is the existence of multiplicative inverses. The multiplicative identity is $\overline{1}$.

$$\overline{1} \cdot \overline{1} = \overline{1} \quad \text{so} \quad \overline{1}^{-1} = \overline{1} \quad \text{in } \mathbb{Z}_3$$

$$\overline{2} \cdot \overline{2} = \overline{4} \cdot \overline{1} \quad \text{so} \quad \overline{2}^{-1} = \overline{2} \quad \text{in } \mathbb{Z}_3$$

This proves that all elements except the additive identity have a multiplicative inverse. Therefore, $\mathbb{Z}_3$ is a field. ▢

Theorem 4.3.2 ▸ Zero Product Property in Modular Arithmetic

If $p \in \mathbb{N}$ is prime, and $a, b \in \mathbb{Z}$ where $\overline{ab} = \overline{0}$ in $\mathbb{Z}_p$, then $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$.

Proof. If $\overline{ab} = \overline{0}$ in $\mathbb{Z}_p$, then $ab = kp$ for some $k \in \mathbb{Z}$. Therefore, $p \mid ab$, so $p \mid a$ or $p \mid b$ (Corollary 3.5.6).

- If $p \mid a$, then $a = mp$ for some $m \in \mathbb{Z}$. Thus, $\overline{a} = \overline{0}$.
- If $p \mid b$, then $b = np$ for some $n \in \mathbb{Z}$. Thus, $\overline{b} = \overline{0}$.

One of the above statements must be true. Therefore, $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$. ▢

Example 4.3.4

If $k \in \mathbb{N}$ is not prime, then there exist $a, b \in \mathbb{Z}$ such that $\overline{ab} = \overline{0}$ in $\mathbb{Z}_k$ but $\overline{a} \neq \overline{0}$ and $\overline{b} \neq \overline{0}$.

Proof. Because k is not prime, we can write $k = ab$ where $a, b \in \mathbb{Z}$ and $1 < a < k$, $1 < b < k$. Then, $k \nmid a$ because $k > a$, so $\overline{a} \neq \overline{0}$. Similarly, $k \nmid b$, so $\overline{b} \neq \overline{0}$. However, $\overline{ab} = \overline{k} = \overline{0}$. ▢

This shows that Z_k is **not** a field when k is not prime.

4.4 Finite Sets

Definition 4.4.1 ▸ Restriction

If $f : X \to Y$ is a function, and $A \subseteq X$, then the **restriction** of f to A is the function:

$$f|_A : A \to Y$$

defined by $f|_A = f(x)$ for all $x \in A$.

We can read this as "f restricted to domain A".

Example 4.4.1

If $f : X \to Y$ is injective and $A \subseteq X$, then $f|_A$ is injective.

Proof. Let $g := f|_A$. Suppose there exist $x_1, x_2 \in A$ such that $g(x_1) = g(x_2)$. By definition of restriction, we have $f(x_1) = g(x_1)$ and $f(x_2) = g(x_2)$. Hence, $f(x_1) = f(x_2)$. Since f is injective, then $x_1 = x_2$. Therefore, $f|_A$ is injective. ▢

Definition 4.4.2 ▸ Corestriction

The **corestriction** of f is the function $f : X \to f[X]$.

In other words, the corestriction replaces the codomain with the range. As such, a corestriction is **always** onto. Although this is a different function, we typically use the same name.

Example 4.4.2

Consider $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$. The corestriction of f is $f : \mathbb{R} \to [0, \infty)$.

If f is an injection, then the corestriction of f is a bijection. An important use of bijections is defining the **cardinality** of a set.

Definition 4.4.3 ▸ Cardinality

The **cardinality** of a set is a measure of the amount of elements in that set.

For finite sets, cardinality follows our intuition of "size". We can denote the cardinality of a set using the absolute value notation.

- If $A = \varnothing$, then $|A| = 0$.
- If there exists a bijection $f : A \to \{i \in \mathbb{N} : i \leq n\}$, then $|A| = n$.
- If A and B are nonempty, and there exists a bijection $f : A \to B$, then $|A| = |B|$

In these cases, we say A is finite with cardinality $|A|$. We will write $\{i \in \mathbb{N} : i \leq n\}$ simply as $\{1, \dots, n\}$, and we can list a finite set as $A = \{a_1, a_2, \dots, a_n\}$.

Our intuition of cardinality as "size" can deceive us when dealing with infinite sets.

Example 4.4.3 ▸ Cardinality of $\mathbb{Z}_2$

The sets $\mathbb{Z}$ and $2\mathbb{Z}$ have the same cardinality.

Proof. Let $f : \mathbb{Z} \to 2\mathbb{Z}$ be defined by $f(x) = 2x$. f is a bijection, so $|\mathbb{Z}| = |2\mathbb{Z}|$. ▢

Although our intuition serves well in understanding cardinalities of finite sets, it can be difficult giving a logically sound explanation.

Example 4.4.4 ▸ Cardinality of Subsets

If A is finite and $B \subseteq A$, then B is finite and $|B| \leq |A|$.

Proof. If $A = \varnothing$ and $B \subseteq A$, then $B = \varnothing$. Thus, B is finite, and $|A| = |B| = 0$, so $|B| \leq |A|$.

Otherwise, $A = \{a_1, \dots, a_n\}$ for some $n \in \mathbb{N}$. We can then use induction. For our base case, suppose $n = 1$. Then $|A| = 1$. If $B \subseteq A$, then either $B = \varnothing$ or $B = A$. Then $|B| = 0$ or $|B| = 1$ respectively. In either case, $|B| \leq |A|$.

Now, suppose the lemma is true for some $n \in \mathbb{N}$ where $n \geq 1$. Let $A = \{a_1, \dots, a_{n+1}\}$. By the induction hypothesis, there exists a bijection $f : \{a, \dots, a_n\} \to \{1, \dots, n\}$. If $B \subseteq A$, then one of the following must be true:

- $B = \varnothing$, so $|B| = 0 \leq n + 1 = |A|$
- $B = A$, so $|B| = |A|$
- $0 \subsetneq B \subsetneq A$, so there exists $a_m \in A \setminus B$, $1 \leq m \leq n + 1$.

Let $g : A \to \{1, \dots, n + 1\}$ be a function defined as such:

- $g(a_j) = f(a_j)$ if $j \neq n + 1$ and $j \neq m$
- $g(a_m) = n + 1$
- $g(a_{n+1}) = f(a_m)$

Thus, g is a bijection (exercise 4.22). Let $h \coloneqq g|_B$. Then h is a bijection, and $h[B] \subseteq \{1, \dots, n\}$. This is finite by the induction hypothesis, so $|h[B]| \leq n$. But $h : B \to h[B]$ is a bijection, so $|B| = |h[B]| \leq n < |A|$. Therefore, B is finite, and $|B| \leq |A|$. ▢

Theorem 4.4.1 ▸ Principle of Inclusion and Exclusion

Let A and B be finite sets. Then $A \cup B$ and $A \cap B$ are finite, and $|A \cup B| = |A| + |B| - |A \cap B|$. If A and B are disjoint, then $|A \cup B| = |A| + |B|$.

Example 4.4.5

If A is finite and B is a proper subset of A, then $|B| < |A|$.

Proof. Outline:

- If $B \subsetneq A$, then $A \cup B = A$ and $A \cap B = B$ and $A \setminus B \neq \varnothing$ (so $|A \setminus b| > 0$) and $B \setminus A = \varnothing$.
- Disjoint Union Lemma: $A \cup B = (A \setminus B) \cup (A \cap B) \cup (B \setminus A)$

□

If $A_1, A_2, \ldots, A_n$ is a finite collection of sets, then we can define their union and intersection as:

$$A_1 \cup A_2 \cup \cdots \cup A_n = \{x : x \in A_i \text{ for some } i, 1 \leq i \leq n\}$$
$$A_1 \cap A_2 \cap \cdots \cap A_n = \{x : x \in A_i \text{ for all } i, 1 \leq i \leq n\}$$

Definition 4.4.4 ▸ Big Union

$$\bigcup_{i=1}^{n} A_i = \{a : a \in A_i \text{ for } \textbf{some } 1 \leq i \leq n\}$$

Definition 4.4.5 ▸ Big Intersect

$$\bigcap_{i=1}^{n} A_i = \{a : a \in A_i \text{ for } \textbf{all } 1 \leq i \leq n\}$$

Example 4.4.6 ▸ Partition Preserves Cardinality

If A is a finite set and $\{A_1, \dots, A_n\}$ is a partition of A, then $|A| = \sum_{i=1}^{n} |A_i|$.

Proof. Let A be a finite set. We will use induction in this proof. For convenience, let $P(n)$ be the statement $|A| = \sum_{i=1}^{n} |A_i|$. Note that A is finite and $A_i \subseteq A$ for all i, so A_i is also finite.

We will first prove $P(1)$. If $A_1 = A$, and $|A_1| = |A| = \sum_{i=1}^{1} |A_i|$.

Next, assume $P(n)$ is true for some $n \in \mathbb{N}$. Let $\{A_1, \dots, A_{n+1}\}$ be a partition of A. Let $B \coloneqq \bigcup_{i=1}^{n} A_i$. Then $\{A_1, \dots, A_n\}$ is a partition of B. By the induction hypothesis, $|B| = \sum_{i=1}^{n} |A_i|$. Note that B and A_{n+1} is disjoint (otherwise, our collection of A_1 to A_n would not be a partition). Also note that $A = B \cup A_{n+1}$. Thus, by the Principle of Inclusion and Exclusion:

$$\begin{aligned} |A| &= |B| + |A_{n+1}| \\ &= \sum_{i=1}^{n} |A_i| + |A_{n+1}| \\ &= \sum_{i=1}^{n+1} |A_i| \end{aligned}$$

Therefore, by the Principle of Induction, $P(n)$ is true for all $n \in \mathbb{N}$ (so long as we can partition A into n sets). ▢

Example 4.4.7

Let $f : X \to Y$ be a function where $|X| = |Y| > 0$. Then f is onto if and only if f is one-to-one. (That is, if f is a surjection, then f is a bijection.)

Theorem 4.4.2 ▸ Pigeonhole Principle

Let $f : X \to Y$ be a function where $|X| > |Y| > 0$. Then there exist $x_1, x_2 \in X$ where $f(x_1) = f(x_2)$ but $x_1 \neq x_2$.

Intuitively, we can think of the elements of X as pigeons and the elements of Y as pigeonholes. Our function f tries to put each pigeon into a pigeonhole. If there are more pigeons than there are pigeonholes, then at least two pigeons will share a pigeonhole.

Example 4.4.8

Prove that if $A \subseteq \{1, 2, \ldots, 9\}$ where $|A| = 6$, then there are distinct elements $x, y \in A$ such that $x + y = 10$.

Proof. Let $B \coloneqq \{\{1, 9\}, \{2, 8\}, \{3, 7\}, \{4, 6\}, \{5\}\}$. Then $|B| = 5$. Let $f : A \to B$ be a function defined as follows:

"for each $x \in A$, let $f(x)$ be the unique element of B that contains x."

Note that f is a function between finite sets where $|A| > |B| > 0$. Therefore, by the Pigeonhole Principle, there exist $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$. That is, x and y are in the same set in B, so $x + y = 10$. □

In the above example, we can think of A as our pigeons and B as our pigeonholes.

We know from previous examples that $\mathbb{Z}_k$ satisfies every field axiom except existence of multiplicative inverses if k is not prime. We can prove that if k is prime and $\overline{m} \in \mathbb{Z}_k$ and $\overline{m} \neq \overline{0}$, then $\overline{m}$ has a multiplicative inverse in $\mathbb{Z}_k$.

Theorem 4.4.3 ▸ Conditions for $\mathbb{Z}_k$ being a field

For $k \in \mathbb{N}$ where $k \geq 2$, $\mathbb{Z}_k$ is a field if and only if k is prime.

Proof. Fix $\overline{m} \in \mathbb{Z}_k$ where $\overline{m} \neq \overline{0}$, and define the function $f : \mathbb{Z}_k \to \mathbb{Z}_k$ as $f\left(\overline{n}\right) = \overline{mn}$. If $f\left(\overline{a}\right) = f\left(\overline{b}\right)$ for $\overline{a}, \overline{b} \in \mathbb{Z}_k$, then $\overline{ma} = \overline{mb}$. Thus:

$$\overline{0} = \overline{ma} - \overline{mb} = \overline{m}\left(\overline{a} - \overline{b}\right)$$

Because k is prime, either $\overline{m} = \overline{0}$ or $\overline{a} - \overline{b} = \overline{0}$. But $\overline{m} \neq \overline{0}$, so $\overline{a} - \overline{b} = 0$. That is, $\overline{a} = \overline{b}$, so f is one-to-one. By Corollary 4.3.9, f is also onto, making f a bijection. Thus, there exists $\overline{c} \in \mathbb{Z}_k$ such that $f\left(\overline{c}\right) = \overline{1}$ That is, $\overline{1} = f\left(\overline{c}\right) = \overline{mc} = \overline{m} \cdot \overline{c}$, so $\overline{m}^{-1} = \overline{c}$ in $\mathbb{Z}_k$. Therefore, if k is prime, then every $\overline{m} \in \mathbb{Z}_k$ where $\overline{m} \neq \overline{0}$ has a multiplicative inverse $\mathbb{Z}_k$, so $\mathbb{Z}_k$ is a field. □

4.5 Infinite Sets

Recall that a set A is finite if either:

1. A is empty (finite with cardinality 0), or
2. there exists a bijection $f : A \to \{1, \dots, n\}$ for some $n \in \mathbb{N}$ (finite with cardinality n)

Definition 4.5.1 ▸ Infinite

A set is **infinite** if it is not finite.

Example 4.5.1 ▸ $\mathbb{N}$ is infinite

Proof. Suppose for contradiction that $\mathbb{N}$ is finite with cardinality n. Then, $\{1, \dots, n\}$ is a proper subset of $\mathbb{N}$ with $|\{1, \dots, n\}| = n$. This contradicts the fact that $|B| < |A|$ if $B \subsetneq A$ and A is finite. ▢

Example 4.5.2 ▸ Infinite Primes (Revisited)

The set of all prime numbers is infinite.

Proof. Suppose for contradiction that there exist only a finite number of primes. We can list these primes as $p_1, p_2, \dots, p_k$. Let $n \coloneqq p_1 p_2 \cdots p_k + 1$. By the Division Algorithm, for all $i \in \mathbb{Z}$ where $1 \leq i \leq k$, we can write $n = qp_i + r$ where $q \in \mathbb{Z}$ and $0 \leq r < p_i$. Moreover, q and r are unique. Thus:

$$q = \frac{p_1 p_2 \cdots p_k}{p_i} \quad \text{and} \quad r = 1$$

If $p_i \mid n$ for some i, then $n = sp_i + 0$ for some $s \in \mathbb{Z}$. This contradicts the uniqueness of q and r guaranteed by the Division Algorithm. Hence, none of the primes $p_1, p_2, \dots, p_k$ divide n. This contradicts n having a prime factorization. Therefore, there must exist infinitely many primes. ▢

Recall that two non-empty sets A and B have the same cardinality if there exists a bijection $f : A \to B$.

Definition 4.5.2 ▸ Countably Infinite

A set is **countably infinite** if that set has the same cardinality as $\mathbb{N}$.

Definition 4.5.3 ▸ Uncountably Infinite

A set is **uncountably infinite** if that set is infinite but not countably infinite.

We will categorize all finite and countably infinite sets as as “countable” sets. We will also

categorize all countably infinite and uncountably infinite sets as "infinite" sets.

To help our intuition, we can think of a countable set as having an idea of a "next element". In $\mathbb{N}$, we can list 1, 2, 3, and so on. However, if we start listing real numbers from 0, what is the "next" real number?

Example 4.5.3

Show that if A is countable and $f : A \to B$ is a bijection, then B is countable.

Proof. Since A is countable, then A is either finite or countably infinite.

- If A is finite with cardinality n, then there exists a bijection $g : A \to \{1, \dots, n\}$. Then $g \circ f^{-1} : B \to \{1, \dots, n\}$ is a composition of two bijections and is therefore a bijection itself. Thus, B is finite with cardinality n.
- If A is countably infinite, then there exists a bijection $g : A \to \mathbb{N}$. Again, $g \circ f^{-1} : B \to \mathbb{N}$ is a bijection. Thus, B is countably infinite.

In either case, B is countable (finite or countably infinite). ▢

Example 4.5.4 ▸ $\mathbb{Z}$ is countably infinite

$\mathbb{Z}$ is countably infinite.

Proof. We need to show that there exists a bijection from $\mathbb{Z}$ to $\mathbb{N}$. First, let's define a function $f : \mathbb{N} \to \mathbb{Z}$ with the following:

$$f(n) = \begin{cases} m, & n = 2m \\ -m, & n = 2m + 1 \end{cases}$$
$$= \begin{cases} \frac{n}{2}, & n \text{ is even} \\ \frac{1-n}{2}, & n \text{ is odd} \end{cases}$$

This function is one-to-one and onto, so f is bijective.

For example, to show f is onto, let $m \in \mathbb{Z}$. If $m > 0$, then $f(2m) = m$ where $2m \in \mathbb{N}$. If $m > 0$, then $f(2m) = m$ where $2m \in \mathbb{N}$. If $m \leq 0$, then $f(2(-m) + 1) = -(-m) = m$ where $2(-m) + 1 \in \mathbb{N}$.

Because f is a bijection, then f^{-1} is a bijection. Thus, $f^{-1} : \mathbb{Z} \to \mathbb{N}$ is a bijection, so $|\mathbb{Z}| = |\mathbb{N}|$. Therefore, $\mathbb{Z}$ is countably infinite. ▢

Theorem 4.5.1 ▸ Cantor's Diagonal Argument

The set $[0,1] \subseteq \mathbb{R}$ is uncountable.

Proof. We will use the idea that every real number in $[0,1]$ has a decimal expansion $0.\delta_1\delta_2\delta_3\ldots$ where each δ represents a digit of the number. Conversely, every decimal expansion $0.\delta_1\delta_2\delta_3\ldots$ represents a real number in the interval $[0,1] \in \mathbb{R}$.

> Note that $0.\overline{9} = 1.\overline{0}\ldots$, so we will avoid decimal expansions that end in repeating 9s since they have an equivalent decimal expansion that ends in repeating 0s.

Suppose for contradiction that $f : \mathbb{N} \to [0,1]$ is a bijection. This means we can "list" all the real numbers in the interval $[0,1]$.

$$\begin{aligned} 1 &\mapsto 0.\delta_{11}\delta_{12}\delta_{13}\ldots \\ 2 &\mapsto 0.\delta_{21}\delta_{22}\delta_{23}\ldots \\ 3 &\mapsto 0.\delta_{31}\delta_{32}\delta_{33}.\ldots \\ &\vdots \end{aligned}$$

We can now construct a real number that is **not** in this list. For $n \in \mathbb{N}$, let:

$$\delta_n = \begin{cases} \delta_{nn} - 1, & \delta_{nn} \neq 0 \\ 1, & \delta_{nn} = 0 \end{cases}$$

This new number $0.\delta_1\delta_2\delta_3\ldots \neq 0.\delta_{n1}\delta_{n2}\delta_{n3}\ldots$ for all $n \in \mathbb{N}$ because $\delta_n \neq \delta_{nn}$. That is, $0.\delta_1\delta_2\delta_3\ldots \notin f(\mathbb{N})$, so f is not surjective. This contradicts our initial assumption that f was a bijection. Therefore, $[0,1] \in \mathbb{R}$ is uncountable. ▢

Example 4.5.5

If A is countable and $B \subseteq A$, then B is uncountable

Theorem 4.5.2 ▸ $\mathbb{R}$ is uncountable

$\mathbb{R}$ is uncountable.

Proof. We know from Cantor's Diagonal Argument that $[0,1] \in \mathbb{R}$ is uncountable, so $\mathbb{R}$ itself is uncountable. ▢

We know that $\mathbb{N}$ is countable and $\mathbb{R}$ is uncountable. What about $\mathbb{Q}$?

Example 4.5.6 ▸ Countability of collections of sets

If $\{A_n\}_{n\in\mathbb{N}}$ is a countable collection of countable sets, then $\bigcup_{n\in N} A_n$ is countable.

Proof Sketch. If $f : \mathbb{N} \to A$ is surjective, then A is countable. For each $n \in \mathbb{N}$, let $A_n = \{a_{n1}, a_{n2}, a_{n3}, ...\}$. Because $\{A_n\}_{n\in\mathbb{N}}$ is countable, we can list this collection as $\{A_1, A_2, ...\}$.

$$\begin{aligned} A_1 &: a_{11}\ a_{12}\ a_{13}\ a_{14}\ ... \\ A_2 &: a_{21}\ a_{22}\ a_{23}\ a_{24}\ ... \\ A_3 &: a_{31}\ a_{32}\ a_{33}\ a_{34}\ ... \\ A_4 &: a_{41}\ a_{42}\ a_{43}\ a_{44}\ ... \\ &\vdots \end{aligned}$$

Define $f : \mathbb{N} \to \bigcup A_n$ by listing each diagonal in order.

$$f(1) = a_{11}, \quad f(2) = a_{12}, \quad f(3) = a_{21}, \quad f(4) = a_{13}, ...$$

This function is surjective (but possibly not bijective if there are two non-disjoint A_i). Therefore, $\bigcup A_n$ is countable. ▢

Example 4.5.7 ▸ $\mathbb{Q}$ is countable

The set $\mathbb{Q}$ is countably infinite.

Proof. For each $n \in \mathbb{N}$, define $\mathbb{Q}_n = \left\{\frac{m}{n} : m \in \mathbb{Z}\right\}$. Then let $f : \mathbb{Z} \to \mathbb{Q}_n$ be a bijection defined by $m \mapsto \frac{m}{n}$. Hence, $\mathbb{Q}_n$ is countable, so $\{\mathbb{Q}_n\}_{n\in\mathbb{N}}$ is a countable collection of countable sets, so $\mathbb{Q} = \bigcup_{n\in\mathbb{N}} \mathbb{Q}_n$ is countable by the example 4.5.6. ▢

Index

Definitions

Examples

Techniques

Theorems