Emory University

MATH 250 - Foundations of Mathematics Learning Notes

Jiuru Lyu

March 2, 2023

Contents

Preface

These is my personal notes for Emory University MATH 250 Foundations of Mathematics course.

This course requires Calculus II as pre-requisite. This course focuses on Mathematical proofs and lays foundation for any other higher level math courses, such as Real Analysis, Complex Variables, Abstract Vector Space, and Abstract Algebra. The book used for this course is *An Introduction to Abstract Mathematics* by Robert Bond.

Throughout this personal note, I use different formats to differentiate different contents, including definitions, theorems, proofs, examples, extensions, and remarks. To be more specific:

Definition 0.0.1 (Terminology). This is a **definition**.

Theorem 0.0.1 (Theorem Name). This is a **theorem**.

Example 0.0.1. This is an **example**.

Answer. This is the *answer* part of an **example**. □

Remark. This is a **remark** of a definition, theorem, example, or proof.

***Proof* (1).**
This is a **proof** of a theorem.

■

Extension. This is a **extension** of a theorem, proof, or example.

This is a hard course, and practice will make critical thinking, mathematical thinking, and mathematical proof skills better. Even though I put efforts into making as few flaws as possible when encoding these learning notes, some errors may still exist in this note. If you find any, please contact me via email: lvjiuru@hotmail.com.

I hope you will find my notes helpful when developing mathematical thinking skills.

Cheers,
Jiuru Lyu

1 Mathematical Reasoning

1.1 Statement

Definition 1.1.1 (Statement). A **statement** is any declarative sentence that is either true or false.

Remark. A statement cannot be ambiguous, cannot be both true and false, and cannot be sometimes true or false.

Example 1.1.1. Examples and Non-Examples:

- All integers are rational numbers. – True statement
- π is irrational. – True statement
- $1 = 0$. – False statement
- $\sqrt{2} \in \mathbb{Z}$. – False statement
- Every student in this class is a math major. – False statement. (To prove this false, find a student that is not a math major.)
- Solve the equation $2x = 3$. – Not a statement
- Chocolate chip is the best ice cream flavor. – Not a statement
- $x + 5 = 3$. – Not a statement. (Turn it into a statement: When $x = 1$, $x + 5$=3; or when $x \neq -2,\ x + 5 \neq 3$.)

Remark. $\in$ means belongs to, and $\mathbb{Z}$ is the notation for integers.

Remark. We denote statements by letters.

Example 1.1.2. P: "Today is a sunny day;" Q: "3 is a prime number.

If the statement's truth depends on a variable, we include the variable in the notation.

Example 1.1.3. $R(x)$: "x is an integer;" $P(x)$: $x + 5 = 3$. $P(x)$ where $x \neq -2$ is false; $P(-2)$ is true.

Example 1.1.4. $R(f)$: "f is an increasing function."

- If $f(x) = e^x$, then $R(f)$ is true.
- If $f(x) = x^2$, then $R(f)$ is false.

Notation 1.1 (Quantifiers). We use the symbol $\forall$ for "for all" or "for any" and the symbol $\exists$ for "there exists." $\forall$ and $\exists$ are called **quantifiers**. $\forall$ is the **universal quantifier** and $\exists$ is the **existential quantifier**.

Example 1.1.5. 1. For any $\varepsilon > 0$, there is a $\delta > 0$.

$$\forall \varepsilon > 0,\ \exists \delta > 0.$$

2. The square of every real number is non-negative.

$$\forall x \in \mathbb{R},\ x^2 \geq 0.$$

3. There is a real number whose square is negative.

$$\exists x \in \mathbb{R}\ s.t.\ x^2 < 0.$$

4. For every real number x, there is an integer n such that $n > x$.

$$\forall x \in \mathbb{R},\ \exists n \in \mathbb{Z}\ s.t.\ n > x.$$

5. For all rational numbers x, there exist integers a and b such that $x = \frac{a}{b}$.

$$\forall x \in \mathbb{Q},\ \exists a, b \in \mathbb{Z}\ s.t.\ x = \frac{a}{b}.$$

Example 1.1.6. 1. $\forall n \in \mathbb{Z},\ \exists m \in \mathbb{Z},\ s.t.\ m = n + 5$: For every integers n, there exists integers m such that $m = n + 5$.

2. $\forall \varepsilon > 0,\ \exists \delta > 0,\ s.t.\ \forall x, y \in \mathbb{R},$ we have $|x - y| < \varepsilon \implies |x^2 - y^2| < \delta$: For every ε greater than 0, there exists a δ greater than 0 such that for all real x and y with $|x - y|$ les than ε, we have $|x^2 - y^2|$ is less than δ.

Remark. $\forall \varepsilon \exists \delta$ and $\exists \delta \forall \varepsilon$ are not the same.
In $\forall \varepsilon \exists \delta$, δ depends on ε, but δ is independent in $\exists \delta \forall \varepsilon$, meaning the same δ works for all ε.

Example 1.1.7. Compare $\forall n \in \mathbb{Z},\ \exists m \in \mathbb{Z}\ s.t.\ m = n^2$ to $\exists n \in \mathbb{Z}\ s.t.\ \forall m \in \mathbb{Z},\ m = n^2$.
Answer.

1. $\forall n \in \mathbb{Z},\ \exists m \in \mathbb{Z}\ s.t.\ m = n^2$: True. The square of an integer is an integer.

2. $\exists n \in \mathbb{Z}\ s.t.\ \forall m \in \mathbb{Z},\ m = n^2$.: False: n^2 is just one integer and cannot be represented by all $m \in \mathbb{Z}$.

□

Definition 1.1.2 (Negations). If P is a statement, the **negation** of P, written as $\neg P$ (read as "not P" or "negation of P") is the statement "P is false."

$$\begin{cases} P \text{ is true} \\ \neg P \text{ is false} \end{cases} \qquad \begin{cases} P \text{ is false} \\ \neg P \text{ is true} \end{cases}$$

Example 1.1.8. Write the negation of P: "All apples are fruits" and check the truth value of both P and $\neg P$.

Answer. $\neg P$: Not all apples are fruits / Some apples are not fruits / There exists an apple that is not a fruit.

P is true and $\neg P$ is false. □

Example 1.1.9. Write the negation of P: "Everyday this week was hot."

Answer. $\neg P$: Somedays this week were not hot. / Not all days this week were hot. / There was a day this week that was not hot. □

Example 1.1.10. P all primes are odd.

$\neg P$: There exists ($\exists$) a prime that is even / Some primes are not odd. (True: 2 is even.)

Example 1.1.11. Q: $\forall x \in \mathbb{R},\ x^2 > x$

$\neg Q$: $\exists x \in \mathbb{R},\ s.t.\ x^2 \leq x$ (True: for $x = \dfrac{1}{2},\ x^2 = \frac{1}{4} < x$)

Example 1.1.12. R: There exists a real solution to $x^2 + 1 = 0$ / $\exists x \in \mathbb{R}\ s.t.\ x^2 + 1 = 0$

$\neg R$: $\forall x \in \mathbb{R},\ x^2 + 1 \neq 0$ – (True .)

Remark (Negating Quantifiers). In general:

$$\neg(\forall x \in S, P(x)) = \exists x \in S\ s.t.\ \neg P(x).$$

$$\neg(\exists x \in S, P(x)) = \forall x \in S, \neg P(x).$$

Example 1.1.13. $\exists n > 0\ s.t.\ \forall m > 0, m < n$

Negation: $\forall n > 0, \exists m > 0\ s.t.\ m \geq n.$

Example 1.1.14. For all $x \in \mathbb{R}$, there exists a $y \in \mathbb{R}$, $s.t.\ xy = 1$

Negation: $\exists x \in \mathbb{R}\ s.t.\ \forall y \in \mathbb{R},\ xy \neq 1$

1.2 Compound Statements

Definition 1.2.1 (Conjunction and Disjunction). The **conjunction** of P and Q, denoted $P \wedge Q$, is the statement "Both P and Q are true." The **disjunction** of P and Q, denoted $P \vee Q$, is the statement "P is true or Q is true."

Example 1.2.1. Which of the following are true statements?

1. The function x^2 is even and it is concave up.

   P: x^2 is even (True), Q: x^2 is concave up (True).

   $$\therefore P \wedge Q \text{ is true.}$$

2. Every student in this class is a math major and a human being.

   P: Every student in this class is a math major (False), Q: Every student in this class is a human being (True).

   $$\therefore P \wedge Q \text{ is false.}$$

3. Every student in this class is a math major or a human being.

   $$P \vee Q \text{ is true.}$$

Example 1.2.2. The following inequality can be written in conjunctions or disjunctions.

1. $|x| < 3$: $(-3 < x < 3)$ Conjunction: $x > -3$ AND $x < 3$
2. $|x| > 3$: Disjunction: $x < -3$ OR $x > 3$

Remark. $\vee$ is **inclusive or**, meaning if both P and Q are true, then $P \vee Q$ is also true, as opposed to **exclusive or**, meaning "either P or Q but not both."

Definition 1.2.2 (Truth Tables). Truth tables are a handy way to organize information.

Example 1.2.3. Write the truth table for the statement form: $P \vee \neg Q$.

Answer.

P	Q	$\neg Q$	$P \vee \neg Q$
T	T	F	T
T	F	T	T
F	T	F	F
F	F	T	T

□

Definition 1.2.3 (Logically Equivalent). Suppose P and Q are statements. We say P and Q are **logically equivalent**, denoted as $P \equiv Q$, if they are either both true or both false.

Note: If two statements are logically equivalent, their truth values match up line by line in a truth table. We use this techniques to prove two statements mathematically (logically) equivalent.

Example 1.2.4. Proving the following using truth tables.

1. $\neg(\neg P) \equiv P$.

   Answer.

P	$\neg P$	$\neg(\neg P)$
T	F	T
F	T	F

□

2. $P \vee Q \equiv Q \vee P$.

Answer.

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

□

3. $\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$.

Answer.

P	Q	$\neg P$	$\neg Q$	$P \vee Q$	$\neg(P \vee Q)$	$(\neg P) \wedge (\neg Q)$
T	T	F	F	T	F	F
T	F	F	T	T	F	F
F	T	T	F	T	F	F
F	F	T	T	F	T	T

□

4. $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$.

Answer.

P	Q	R	$Q \vee R$	$P \vee (Q \vee R)$	$P \vee Q$	$(P \vee Q) \vee R$
T	T	T	T	T	T	T
T	T	F	T	T	T	T
T	F	T	T	T	T	T
T	F	F	F	T	T	T
F	T	T	T	T	T	T
F	T	F	T	T	T	T
F	F	T	T	T	T	T
F	F	F	F	F	F	F

□

Theorem 1.2.1 (Negating Compound Statements).

$$\neg(P \wedge Q) = \neg P \vee \neg Q$$

$$\neg(P \vee Q) = \neg P \wedge \neg Q$$

Example 1.2.5. It is not true that the numbers x and y are both even.

P: x is even; Q: y is even.

$\neg(P \wedge Q)$: x is odd ($\neg P$) OR y is odd ($\neg Q$).

Example 1.2.6. It is not true that 9 is prime or 9 is even.

P: 9 is prime; Q: 9 is even.

$\neg(P \vee Q)$: 9 is not prime ($\neg P$) AND 9 is odd ($\neg Q$)

Theorem 1.2.2 (Distributivity).

$$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$$

$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$$

Remark. Truth tables can balloon in size. Indeed, if you have $P_1, \cdots, P_n$ statements involved in your statement form, your truth table will contain 2^n rows.

Sometimes, prove logical equivalences without using truth tables by taking advantage of the logical equivalences already proven is more approachable.

Example 1.2.7. Prove or disprove without using ruth tables.

1. $\neg(P \wedge (\neg Q)) \equiv (\neg P) \vee Q$.

   ***Proof* (1).**

$$\begin{aligned} \neg(P \wedge (\neg Q)) &\equiv \neg P \vee (\neg(\neg Q)) \\ &\equiv \neg P \vee Q \qquad \text{[Negation of } \neg Q \equiv Q\text{]} \end{aligned}$$

   ■

2. $P \wedge ((Q \vee R) \vee S) \equiv (P \wedge Q) \vee (P \wedge R) \vee (P \wedge S)$.

   ***Proof* (2).**

$$\begin{aligned} P \wedge ((Q \vee R) \vee S) &\equiv (P \wedge (Q \vee R)) \vee (P \wedge S) \qquad \text{[Distributivity]} \\ &\equiv (P \wedge Q) \vee (P \wedge R) \vee (P \wedge S) \qquad \text{[Distributivity]} \end{aligned}$$

   ■

3. $P \vee ((Q \wedge R) \wedge S) \equiv (P \vee Q) \wedge (P \vee R) \wedge (P \vee S)$.

   ***Proof* (3).**

$$\begin{aligned} P \vee ((Q \wedge R) \wedge S) &\equiv (P \vee (Q \wedge R)) \wedge (P \vee S) \qquad \text{[Distributivity]} \\ &\equiv (P \vee Q) \wedge (P \vee R) \wedge (P \vee S) \qquad \text{[Distributivity]} \end{aligned}$$

   ■

Definition 1.2.4 (Tautology). A statement form that is true in all possible cases (for example, regardless of the truth values of P and Q) is called a **tautology**.

Definition 1.2.5 (Contradiction). A statement that is false in all possible cases (for example, regardless of the truth values for P and Q) is called a **contradiction**.

Example 1.2.8. Classify each of the following as a tautology, a contradiction, or neither.

1. $P \vee \neg P$

P	$\neg P$	$P \vee \neg P$
T	F	T
F	T	T

$\therefore$ Tautology.

2. $P \wedge \neg P$

P	$\neg P$	$P \wedge \neg P$
T	F	F
F	T	F

$\therefore$ Contradiction.

3. $P \vee Q$

P	A	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

$\therefore$ Neither.

1.3 Implications

Definition 1.3.1 (Implications or Conditional Statements). The symbol $\Rightarrow$ means "implies." So $P \Rightarrow Q$ means "P implies Q" or "If P, then Q."

Example 1.3.1.

- If this is an apple, then it is a fruit.
- If a function f is differentiable, then it is continuous.

Remark. In mathematics, the truth value of an implication is **not** determined by causality. That is, the statement $P \Rightarrow Q$ means that in all circumstances in which P is true, Q is also true.

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

The only way for $P \Rightarrow Q$ to be false is when P is true but Q is false. This implies that false assumptions can lead to any conclusions.

Definition 1.3.2. Sufficient Condition and Necessary Condition If $P \Rightarrow Q$ is true, then P is called a **sufficient condition** for Q, and Q is called a **necessary condition** for P. There are many different ways to write $P \Rightarrow Q$in English:

$$P \implies Q \begin{cases} \text{If } P, \text{ then } Q. \\ Q \text{ if } P. \\ Q \text{ whenever } P. \\ Q, \text{ provided that } P \\ \text{Whenever } P, \text{ then also } Q. \\ P \text{ is a sufficient condition for } Q. \\ \text{For } Q, \text{ it is sufficient that } P. \\ Q \text{ is a necessary condition for } P. \\ \text{For } P, \text{ it is necessary that } Q. \\ P \text{ only if } Q. \end{cases}$$

Theorem 1.3.1 (Negation of Implications). Negation of an implication is a conjunction:

$$\neg(P \Rightarrow Q) \equiv P \wedge \neg Q$$

Example 1.3.2. Negate the following:

$$\forall \varepsilon \; \exists \delta > 0, \; |x - y| < \varepsilon \implies |x^2 - y^2| < \delta.$$

Answer.

$$\exists \varepsilon \; s.t. \; \forall \delta > 0, \; |x - y| < \varepsilon \text{ and } |x^2 - y^2| \geq \delta.$$

□

Example 1.3.3. Write in symbols and negate the statement P: "For any positive ε there exists a positive M such that $|f(x) - b| < \varepsilon$ whenever $x > M$."

Answer.

$$P: \; \forall \varepsilon > 0, \; \exists M > 0 \; s.t. \; x > M \implies |f(x) - b| < \varepsilon.$$

$$\neg P: \; \exists \varepsilon > 0 \; s.t. \; \forall M > 0, \; x > M \text{ and } |f(x) - b| \geq \varepsilon.$$

□

Definition 1.3.3 (Axiom). An **axiom** is a statement which is regarded as being established, accepted, or self-evidently true.

Definition 1.3.4 (Theorem). A **theorem** is a statement that is true and has been verified as true.

Definition 1.3.5 (Proposition). A **proposition** is a smaller, less important theorem.

Definition 1.3.6 (Lemma). A **lemma** is a theorem whose main purpose is to help prove another theorem.

Definition 1.3.7 (Corollary). A **corollary** is a result that is the immediate consequence of a theorem.

Remark (Proving a theorem). Want to show (*WTS*) $P \Rightarrow Q$: If P is false, $P \Rightarrow Q$ is automatically true, so there's nothing to show here. However, if P is true, we need to show Q is true (for $P \Rightarrow Q$ to be true)l.

First line of a direct proof: Suppose P.

Last line of a direct proof: Therefore Q.

Definition 1.3.8 (Divisibility). Let a and b be integers, with a non-zero. We say a **divides** b, written $a \mid b$, if there exists an *integer* k such that $b = ak$.

In this case, we way that a is a **factor** of b, and that b is a **multiple** of a.

Also note that $a \nmid b$ means that a does not divide b. That is, $\nexists k \in \mathbb{Z}$, such that $b = ak$.

Definition 1.3.9 (Even). Let n be integer. We say n is **eve** if $2 \mid n$.

Definition 1.3.10 (Odd). Let n be an integer. We say n is **odd** if $2 \nmid n$, $n = 2k + 1$, or $n = 2k - 1$ for some (*f.s.*) $k \in \mathbb{Z}$.

Extension. The possible remainders if we divide an integer by 5 is 0, 1, 2, 3, 4, so we can suppose n to be $5k$, $5k + 1$, $5k + 2$, $5k + 3$, $5k + 4$, respectively.

Axiom 1.1. Integers are closed under addition.

Axiom 1.2. If $k \in \mathbb{Z}, (-k) \in \mathbb{Z}$.

`Let` a, b `and` c `be integers, with` a `non-zero. If` $a \mid b$ `and` $a \mid c$, `then` $a \mid (b+c)$.

***Proof* (1).**

Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$.

Suppose $a \mid b$ and $a \mid c$. Then, by definition of divides, $\exists k, l \in \mathbb{Z}$ *s.t.*

$$b = ak \qquad \text{and} \qquad c = al.$$

Then, $b + c = ak + al = a(k + l)$.

Since $k + l \in \mathbb{Z}$ (Axiom 1.1), by definition, $a \mid (b + c)$.

■

Let a and b be integers, with a non-zero. If $a \mid b$, then $a \mid (-b)$ and $(-a) \mid b$.

***Proof* (2).**

Let $a, b \in \mathbb{Z}$, with $a \neq 0$.

Suppose $a \mid b$. Then by definition of divides, $\exists k \in \mathbb{Z}$ *s.t.* $b = ak$.

Multiple both sides of this equation by (-1):

$$-b = -ak = a(-k).$$

Since $(-k) \in \mathbb{Z}$, we get $a \mid (-b)$. [Axiom1.2]

Multiple $-b = a(-k)$ by (-1) on both sides:

$$b = (-a)(-k)$$

Since $(-k) \in \mathbb{Z}$, we see that $(-a) \mid b$.

■

Let a, b, and c be integers, with a and b non-zero. If $(ab) \mid (ac)$, then $b \mid c$.

***Proof* (3).**

Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$ and $b \neq 0$.

Suppose $(ab) \mid (ac)$. Then $\exists k \in \mathbb{Z}$ *s.t.* $ac = (ab)k$.

Divide both sides of the equation by a:

$$c = bk.$$

Since $k \in \mathbb{Z}$, by definition of divides, $b \mid c$.

■

Let n be an integer. If n is of the form $3k+1$ for some integer k, then n^2 is again of the form $4k'+1$ for some integer k'.

***Proof* (4).**

Let $n \in \mathbb{Z}$.

Suppose $n = 3k + 1$ *f.s.* $k \in \mathbb{Z}$.

Squaring both sides:

$$\begin{aligned} n^2 = (3k+1)^2 &= 9k^2 + 6k + 1 \\ &= 3(3k^2 + 2k) + 1. \end{aligned}$$

Set $k' = 3k^2 + 2k$.

As $k \in \mathbb{Z}$, $3k^2, 2k \in \mathbb{Z}$, $k' = 3k^2 + 2k \in \mathbb{Z}$.

Then, n^2 is in the form of $3k' + 1$ *f.s.* $k' \in \mathbb{Z}$.

■

Let n and m be integers. If n and m are even, then $n+m$ is even.

***Proof* (5).**

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

Suppose n and m are even. Then $\exists s, t \in \mathbb{Z}$ *s.t.*

$$n = 2s \qquad \text{and} \qquad m = 2t.$$

Then

$$\begin{aligned} n + m &= 2s + 2t \\ &= 2(s + t) \end{aligned}$$

Since $(s + t) \in \mathbb{Z}$, by definition, $n + m$ is even.

■

Let n and m be integers. If m is even, then mn is even.

***Proof* (6).**

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

Suppose m is even. Then $\exists k \in \mathbb{Z},$ *s.t.* $m = 2k$.

So, $mn = (2k)n = 2(kn)$.

Since $(kn) \in \mathbb{Z}$, by definition, mn is even.

■

Definition 1.3.11 (Parity). If x and y have the same **parity**, then x and y both are odd or both are even.

If $x \in \mathbb{Z}$, then x and x^2 have the same parity.

Remark. Sometimes, it is helpful to do a case analysis!

***Proof* (7).**

Let $x \in \mathbb{Z}$

Case 1 Suppose x is even.

Then, by definition, $x = 2k$ *f.s.* $k \in \mathbb{Z}$.

So, $x^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Since $(2k^2) \in \mathbb{Z}$, by definition, x^2 is even.

Case 2 Suppose x is odd.

Then, by definition, $x = 2l + 1$ *f.s.* $l \in \mathbb{Z}$.

So, $x^2 = (2l + 1)^2 = 4l^2 + 4l + 1 = 2(2l^2 + 2l) + 1$

Since $(2l^2 + 2l) \in \mathbb{Z}$, by definition, x^2 is odd.

■

1.4 Contrapositive and Converse

Let n be an integer. Prove that if $3 \nmid n$, then $3 \mid n^2 - 1$.

***Proof* (1).**

Let $n \in \mathbb{Z}$. Suppose $3 \nmid n$.

Case 1 Then $n = 3k + 1$ *f.s.* $k \in \mathbb{Z}$.

$$\begin{aligned} n^2 - 1 &= (3k+1)^2 - 1 \\ &= 9k^2 + 6k + 1 - 1 \\ &= 9k^2 + 6k \\ &= 3(3k^2 + 2k) \end{aligned}$$

Since $(3k^2 + 2k) \in \mathbb{Z}$, by definition, $3 \mid n^2 - 1$.

Case 2 Then $n = 3l + 2$ *f.s.* $l \in \mathbb{Z}$.

$$\begin{aligned} n^2 - 1 &= (3l+2)^2 - 1 \\ &= 9l^2 + 18l + 4 - 1 \\ &= 9l^2 + 18l + 3 \\ &= 3(3l^2 + 6l + 1) \end{aligned}$$

Since $(3l^2 + 6l + 1) \in \mathbb{Z}$, by definition, $3 \mid n^2 - 1$.

■

Sometimes, we can form new implications from old ones. Let P and Q to be statement, and consider the implication $P \Rightarrow Q$.

Definition 1.4.1 (Converse). The **converse** of $P \Rightarrow Q$ is the implication $Q \Rightarrow P$.

Definition 1.4.2 (Contrapositive). The **contrapositive** of $P \Rightarrow Q$ is the implication $\neg Q \Rightarrow \neg P$.

Remark. A question that we are interested in is that "are these equivalent to the original implication?"

Theorem 1.4.1.

$$\neg Q \Rightarrow \neg P \equiv P \Rightarrow Q.$$

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg Q$	$\neg Q \Rightarrow \neg P$
T	T	T	F	F	T
T	F	F	F	T	F
F	T	T	T	F	T
F	F	T	T	T	T

Since the contrapositive of an implication is logically equivalent to the original implication, we sometimes prove the contrapositive in order to prove the original statement.

Prove that if the product of two integers x and y is even, at least one of them must be even.

***Proof* (2).**

We will prove the contrapositive: "If x and y are both odd, then xy is odd."

Let $x, y \in \mathbb{Z}$. Suppose x and y are odd.

Then $\exists k, l \in \mathbb{Z}$ *s.t.* $x = 2k + 1$ and $y = 2l + 1$.

So,

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

Since $2kl + k + l \in \mathbb{Z}$, we see that xy is odd.

■

Let $x \in \mathbb{Z}$. Prove that if $x^2 - 4x + 7$ is even, then x is odd.

Contrapositive: If x is even, then $x^2 - 4x + 7$ is odd.

***Proof* (3).**

We will prove the contrapositive.

Let $x \in \mathbb{Z}$. Suppose x is even. Then $x = 2k$ *f.s.* $k \in \mathbb{Z}$.

Then

$$\begin{aligned} x^2 - 4x + 7 &= (2k)^2 - 4(2k) + 7 \\ &= 4k^2 - 8k + 7 \\ &= 2(2k^2 - 4k + 3) + 1 \end{aligned}$$

Since $2k^2 - 4k + 3 \in \mathbb{Z}$, by definition, $x^2 - 4x + 7$ is odd.

■

Let $n \in \mathbb{Z}$. Prove that if n^2 is even, then n is even.

Contrapositive: If n is odd, then n^2 is odd.

Remark. This is a special case of Proof (2), where $x = y$ and is odd.

***Proof* (4).**

We will prove the contrapositive.

Let $n \in \mathbb{Z}$. Suppose n is odd. Then $n = 2k + 1$ *f.s.* $k \in \mathbb{Z}$.

Then

$$\begin{aligned} n^2 = (2k+1)^2 &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned}$$

Since $(2k^2 + 2k) \in \mathbb{Z}$, we see n^2 is odd.

■

Prove that every even number is of the form $4k$ or $4k+2$ for some $k \in \mathbb{Z}$.

***Proof* (5).**

We will prove the contrapositive: If x is of the form $4k+1$ or $4k+3$, then x is odd.

Suppose $x \in \mathbb{Z}$.

Case 1 Suppose $x = 4k+1$ *f.s.* $k \in \mathbb{Z}$.

Then $x = 4k+1 = 2(2k)+1$.

Since $2k \in \mathbb{Z}$, by definition, x is odd.

Case 2 Suppose $x = 4k+3$ *f.s.* $k \in \mathbb{Z}$.

Then $x = 4k+3 = 2(2k+1)+1$

Since $2k+1 \in \mathbb{Z}$, by definition, x is odd.

■

Prove that every odd number is of the form $4k+1$ or $4k+3$ for some $k \in \mathbb{Z}$.

Remark. This implication is the converse of as the contrapositive of the previous one. Here, the implication and the converse of it is both true.

***Proof* (6).**

We will prove the contrapositive: If x is of the form $4k$ or $4k+2$, then x is even.

Suppose $x \in \mathbb{Z}$.

Case 1 Suppose $x = 4k$ *f.s.* $k \in \mathbb{Z}$.

Then $x = 4k = 2(2k)$.

Since $2k \in \mathbb{Z}$, by definition, x is even.

Case 2 Suppose $x = 4k+2$ *f.s.* $k \in \mathbb{Z}$.

Then $x = 4k+ = 2 = 2(2k+1)$

Since $2k+1 \in \mathbb{Z}$, by definition, x is even.

■

Theorem 1.4.2 (Prove by Contradiction). To prove P, we assume $\neg P$ and show that this implies an absurd statement (like $1 = 0$ or $0 < 0$).

Definition 1.4.3 (Simplest-form). Let m and n be integers, with n non-zero. We say the fraction $\frac{m}{n}$ is in **simplest-form** if m and n have no common factors.

Definition 1.4.4 (Rational Numbers). Let x be a real number. The number x is said to be **rational** if there exists integers m and n, with n non-zero, such that $x = \frac{m}{n}$.

Axiom 1.3. After a finite number of cancellations, any fraction $\frac{m}{n}$ can be written in simplest form.

`Prove that` $\sqrt{2}$ `is irrational.`

***Proof* (7).**

Assume for the sake of contradiction that $\sqrt{2}$ is rational.

Then, by definition, $\exists p, q \in \mathbb{Z}$, with $q \neq 0$ *s.t.* $\sqrt{2} = \frac{p}{q}$. We can assume that p and q have no common factors.

Note that $\sqrt{2}q = p$, squaring both sides, we see that $2q^2 = p^2$.

Since $q^2 \in \mathbb{Z}$, by definition, p^2 is even. From Proof (4), if p^2 is even, then p must be even. By definition, $\exists k \in \mathbb{Z}$ *s.t.* $p = 2k$.

Plugging this back to our equation: $2q^2 = (2k)^2 = 4k^2$, $q^2 = 2k^2$.

Since $k^2 \in \mathbb{Z}$, we see that q^2 is even. Again, from Proof (4), if q^2 is even, then q is even.

⁎ This contradicts the fact that p, q had no common factors.

So, $\sqrt{2}$ must, in fact, be irrational.

■

`Let` $0 < \alpha < 1$. `Prove that` $\sqrt{\alpha} > \alpha$.

***Proof* (8).**

We will use the Proof by Contradiction.

Suppose $0 < \alpha < 1$. Assume for the sake of contradiction that $\sqrt{\alpha} < \alpha$.

Since $\alpha, \sqrt{\alpha} > 0$ and $f(x) = x^2$ is an increasing function for positive x, squaring both sides, we have $\alpha \leq \alpha^2$.

So, $\alpha^2 - \alpha \geq 0$. Then $\alpha(\alpha - 1) \geq 0$.

$$\begin{cases} \alpha \geq 0 \\ \alpha - 1 \geq 0 \end{cases} \qquad \text{or} \begin{cases} \alpha \leq 0 \\ \alpha - 1 \leq 0 \end{cases}$$

We have $\alpha \geq 1$ or$\alpha \leq 0$.

⁎ This contradicts with the fact that $0 < \alpha < 1$.

So, $\sqrt{\alpha} > \alpha$.

■

Another way to prove is by contrapositive.

***Proof* (9).**

We will prove the contrapositive: If $\sqrt{\alpha} \leq \alpha$, then $\alpha \leq 0$ or $\alpha \geq 1$.

Suppose $\alpha \in \mathbb{R}$ and $\sqrt{\alpha} \leq \alpha$.

As $\sqrt{\alpha}$ exists, $\alpha \geq 0$.

Since $\alpha, \sqrt{\alpha} \geq 0$ and $f(x) = x^2$ is an increasing function for $x \geq 0$: $\alpha \leq \alpha^2$.

Then $\alpha^2 - \alpha \geq 0$, $\alpha(\alpha - 1) \geq 0$.

Since $\alpha \geq 0$, $\alpha - 1$ must also be greater than 0.

So, we have $\begin{cases} \alpha \geq 0 \\ \alpha - 1 \geq 0 \end{cases}$

Hence, we have $\alpha \geq 1$.

■

Prove that there are no integer solutions to the equation $x^2 = 4y + 2$.

***Proof* (10).**

Assume for the sake of contradiction that $\exists x, y \in \mathbb{Z}$ *s.t.* $x^2 = 4y + 2$.

$$x^2 = 4y + 2 = 2(2y + 1)$$

Since $2y + 1 \in \mathbb{Z}$, x^2 is an even number, and thus x is also an even number.

Then, $\exists k \in \mathbb{Z}$ *s.t.* $x = 2k$.

$$\therefore x^2 = (2k)^2 = 4k^2 = 4y + 1$$
$$2k^2 = 2y + 1$$

Method 1

Since $k^2 \in \mathbb{Z}$, $2k^2$ is even. Since $y \in \mathbb{Z}$, $2y + 1$ is odd.

Then the equation indicates an even number equals to an odd number.

⁎ This contradicts with the fact that even numbers cannot equal to an odd number.

Method 2

$$2k^2 = 2y + 1$$
$$2(k^2 - y) = 1$$
$$k^2 - y = \frac{1}{2}$$

⁎ This contradicts with the fact that since $k, y \in \mathbb{Z}$, so does $k^2 - y$.

So, our assumption is wrong. There is no integer solutions for $x^2 = 4y + 2$.

■

Definition 1.4.5 (Prime Numbers). A prime number is a natural number that is only divisible by 1 and itself.

Example 1.4.1. 2, 3, 5, 7, 11, 13, 17, 19, ...

Prove there are infinitely many primes

Remark. This is a very revealing proof by contradiction. It reveals a way to find a larger prime based on the primes that we already have.

***Proof* (11).**

Assume for the sake of contradiction that there are exactly n primes, where $n \in \mathbb{N}$. Let's list them as $p_1,\ p_2,\ p_3, \cdots, p_n$, where $p_1 = 2,\ p_2 = 3, \cdots,\ p_n$ is the largest prime.

Consider the number $q = \underbrace{p_1p_2p_3\cdots p_n}_{\text{product}} + 1$. Then notice that since $p_i \geq 2 \forall i$, we have $q > p_n$.

Since $q > p_n$, q cannot be prime, based on our assumption.

So, $\exists p_k \in \{p_1,\ p_2,\ \cdots,\ p_n\}$ *s.t.* $p_k \mid q$. Then, by definition, $q = cp_k$ *f.s.* $c \in \mathbb{Z}$.

So,

$$c = \frac{q}{p_k} = \frac{p_1p_2p_3\cdots p_n + 1}{p_k} = \frac{p_1p_2p_3\cdots p_n}{p_k} + \frac{1}{p_k}$$

Then,

$$\frac{1}{p_k} = c - \frac{p_1p_2p_3\cdots p_n}{p_k}$$

Note that since p_k is one prime among $p_1, \cdots p_n$, $\dfrac{p_1p_2p_3\cdots p_n}{p_k} \in \mathbb{Z}$.

Since $c \in \mathbb{Z}$, then $\dfrac{1}{p_k} \in \mathbb{Z}$.

⁂ This is a contradiction because $p_k \nmid 1$ as $p_k \geq 2 \forall k$.

So, there must be infinitely many primes

■

`If` $n \in \mathbb{Z}$, `then` $5n^2 + 3n + 7$ `is odd.`

***Proof* (12).**

Suppose $n \in \mathbb{Z}$.

Case 1 If n is even. Then $\exists k \in \mathbb{Z}$ *s.t.* $n = 2k$.

$$5n^2 + 3n + 7 = 5(2k)^2 + 3(2k) + 7 = 20k^2 + 6k + 7 = 2(10k^2 + 3k + 3) + 1$$

Since $10k^2 + 3k + 3 \in \mathbb{Z}$, $5n^2 + 3n + 7$ is odd.

Case 2 If n is odd. Then $\exists k \in \mathbb{Z}$ *s.t.* $n = 2k + 1$.

$$5n^2 + 3n + 7 = 5(2k+!)^2 + 3(2k + 1) + 7 = 20k^2 + 26k + 15 = 2(10k^2 + 13k + 7) + 1$$

Since $10k^2 + 13k + 7 \in \mathbb{Z}$, $5n^2 + 3n + 7$ is odd.

■

Definition 1.4.6 (Equivalence). The prove $P \iff Q$ (equivalence or biconditional, "if and only if" or "*iff*") we must prove the forward implication $P \implies Q$ and the backward

implication $Q \implies P$.

Prove that for $x, y \in \mathbb{R}$, $(x+y)^2 = x^2 + y^2$ if and only if $x = 0$ or $y = 0$.

***Proof* (13).**

($\Rightarrow$): We will show that $(x+y)^2 = x^2 + y^2 \implies x = 0$ or $y = 0$.

Suppose $x, y \in \mathbb{Z}$ *s.t.* $(x+y)^2 = x^2 + y^2$. So we have

$$x^2 + y^2 + 2xy = x^2 + y^2$$

That is, $2xy = 0$ or $xy = 0$. So $x = 0$ or $y = 0$ $\square$

($\Leftarrow$): We will show that $x = 0$ or $y = 0 \implies (x+y)^2 = x^2 + y^2$.

Notice that the equation retains symmetry.

Suppose $x, y \in \mathbb{R}$. Assume $x = 0$ or $y = 0$.

Without loss of generality (WLOG), we may assume that $x = 0$.

Then,

$$(x+y)^2 = (0+y)^2 = y^2$$
$$x^2 + y^2 = 0^2 + y^2 = y^2$$

So, $(x+y)^2 = x^2 + y^2$.

■

2 Sets

2.1 Sets and Subsets

Definition 2.1.1 (Set, Element). A **set** is a collection of objects, called **elements**. A set is typically denoted by a capital letter and a set's elements are listed in {}.

Example 2.1.1.

- $A = \{1, 2, 3\}$
- $F = \{1, 2, 3, 5, 8, 13, ...\}$ the set of Fibonacci numbers
- $\mathbb{N} = \{1, 2, 3, 4, 5, ...\}$ the **natural numbers** (Does not include 0.)
- $\varnothing$ the **empty set**
- $M = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$
- {Ludacris, T.I., Killer Mike, Big Boi, Andre 3000, Latto}

Definition 2.1.2. We write $a \in A$ (a is in A) to indicate a is an element of A and $a \notin A$ (a is not in A) to indicate a is not an element of A.

Definition 2.1.3 (Cardinality). The **cardinality** of a set A is the number of elements in A and is denoted $|A|$.

Remark. When listing the elements of a set, each element is listed only once (for example, $\{1, 1\}$ is not a set) and the order of the elements doesn't matter ($\{1, 2\} = \{2, 1\}$).

Notation 2.1 (Set Builder Notation). We can use the set builder notation to describe a general property of the elements.

Example 2.1.2. $\{2n \mid n \in \mathbb{N}\}$ is "the set of elements of the form $2n$ such that n is a natural number."

Remark. We use $2\mathbb{Z}$ to represent $\{2k \mid k \in \mathbb{Z}\}$. Similarly, we have $5\mathbb{Z}, 10\mathbb{Z}, ...$

Definition 2.1.4 (Subset). We say a set A is a **subset** of a set B, denoted $A \subseteq B$, if every element of A is an element of B (If $a \in A$, then $a \in B$). We write $A \nsubseteq B$ if A is not a subset of B ($\neg(A \subseteq B) = a \in A$ and $a \notin B$.)

- $A \subseteq B$: "A is a subset of B"
- $B \supseteq A$: "B contains A"
- $A \subsetneq B$: "A is a proper subset of B" or "A is a subset of B, but $A \neq B$."

Remark. By definition, $A \subseteq A$ (every set is a subset of itself).

Remark. $\varnothing$ is a subset of any set.

Theorem 2.1.1. A set of n elements has 2^n subsets.

***Proof* (1).**

For every element in the set, they have two options: in the subset or out the subset. Hence, there will be in total 2^n subsets.

■

Definition 2.1.5. Building New Sets From Old

- **Intersection**: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
- **Union**: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
- **Difference**: $A - B = A \backslash B = \{x \mid x \in A \text{ and } x \notin B\}$

Theorem 2.1.2.

$$A \cup B = B \cup A$$

$$A \cap B = B \cap A$$

$$A - B \neq B - A$$

Definition 2.1.6 (Universal Set). A **universal set** of A is a set within which A exists.

Definition 2.1.7 (Complement). The **complement** of A in its universal set U is $\overline{A} = A^C = U - A$.

Theorem 2.1.3.

$$A \cup \overline{A} = U$$

$$A \cap \overline{A} = \varnothing$$

Specially, if U is finite, $|U| = |A| + |\overline{A}|$

Theorem 2.1.4 (De Morgan's Laws).

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

Set Theoretic Proofs: Prove $a \in A$: To prove an element belongs to a set, we must prove the element satisfies the required properties of the set.

`Prove that` $14 \in \{4a + 7b : \ a, b \in \mathbb{Z}\}$

***Proof* (2).**

Note that $14 = 4(0) + 7(2)$

Since $0, 2 \in \mathbb{Z}$, by definition, $14 \in \{4a + 7b \mid a, b \in \mathbb{Z}\}$.

■

Theorem 2.1.5. Proving $A \subseteq B$: To prove $A \subseteq B$, we must prove that if $a \in A$, then $a \in B$. We can do so using any technique:

- Direct proof: Suppose $a \in A$..... Therefore, $a \in B$.
- Contrapositive proof: Suppose $a \notin B$..... Therefore, $a \notin A$.
- Contradiction: Suppose $a \in A$. Assume for the sake of contradiction that $a \in B$.....⁂

`Prove that for all` $m, n \in \mathbb{Z}$, `we have` $\{x \in \mathbb{Z} : mn \mid x\} \subseteq \{x \in \mathbb{Z} : m \mid n\} \cap \{x \in \mathbb{Z} : n \mid x\}$.

***Proof* (3).**

Let $x \in \mathbb{Z}$ *s.t.* $x \in \{x \in \mathbb{Z} : mn \mid x\}$. Then, $mn \mid x$, and so $x = kmn$ *f.s.* $k \in \mathbb{Z}$.

So, $x = m(kn)$, and since $kn \in \mathbb{Z}$, $x \in \{x \in \mathbb{Z} : m \mid x\}$.

Also, $x = n(km)$, and since $km \in \mathbb{Z}$, $x \in \{x \in \mathbb{Z} : n \mid x\}$.

By definition of intersection, $x \in \{x \in \mathbb{Z} : m \mid x\} \cap \{x \in \mathbb{Z} : n \mid x\}$.

■

Definition 2.1.8 (Equal). We say two sets A and B are **equal**, denoted $A = B$, if they have the same elements.

Remark. $A = B \iff A \subseteq B$ and $B \subseteq A$

`If` A, B, `and` C `are sets, prove` $(A \cap B) - C = (A - C) \cap (B - C)$

***Proof* (4).**

($\subseteq$): $(A \cap B) - C \subseteq (A - C) \cap (B - C)$

Suppose $x \in (A \cap B) - C$ (WTS: $x \in (A - C) \cap (B - C)$)

By definition of intersection, $x \in A$ and $x \in B$

By definition of difference, $x \notin C$.

Since $x \in A$ and $x \notin C$, $x \in A - C$. Similarly, since $x \in B$ and $x \notin C$, $x \in B - C$.

By definition of intersection, $x \in (A - C) \cap (B - C)$ □

($\supseteq$): $(A - C) \cap (B - C) \subseteq (A \cap B) - C$

Let $x \in (A - C) \cap (B - C)$.

By definition of intersection, $x \in A - C$ and $x \in B - C$.

By definition of difference, $x \in A$, $x \notin C$ and $x \in B$, $x \notin C$.

Since $x \in A$ and $x \in B$, $x \in (A \cap B)$

Further since $x \notin C$, by definition of difference, $x \in (A \cap B) - C$.

■

If A and B are sets, prove that $A \subseteq B$ if and only if $\overline{B} \subseteq \overline{A}$.

***Proof* (5).**

($\Rightarrow$): $A \subseteq B \implies \overline{B} \subseteq \overline{A}$.

Suppose $A \subseteq B$. [WTS: $\overline{B} \subseteq \overline{A}$]

Suppose $x \in \overline{B}$. [WTS: $x \in \overline{A}$]

Since $x \in \overline{B}$, then $x \notin B$. Note that since $A \subseteq B$, by definition, if $x \in A$, then $x \in B$.

By contrapositive, $x \notin B \implies x \notin A$

Since $x \notin B$, by assumption, $x \notin A$. That is $x \in \overline{A}$. $\square$

($\Leftarrow$): $\overline{B} \subseteq \overline{A} \implies A \subseteq B$.

Suppose $\overline{B} \subseteq \overline{A}$ [WTS: $A \subseteq B$]

Suppose $x \in A$ [WTS: $x \in B$]

Since $x \in A$, then $x \notin \overline{A}$. Since$\overline{B} \subseteq \overline{A}$, by contrapositive,

$$x \notin \overline{A} \implies x \in \overline{B}.$$

Since $x \notin \overline{A}$, by assumption, $x \notin \overline{B}$. That is, $x \in B$.

■

2.2 Combining Sets

Prove that $A \subseteq B$ if and only if $A - B = \varnothing$.

***Proof* (1).**

($\Rightarrow$): WTS: $A \subseteq B \implies A - B = \varnothing$.

Let A, B be sets. Suppose $A \subseteq B$.

Assume for the sake of contradiction that $A - B \neq \varnothing$. Then $x \in A - B$.

By definition of set difference, $x \in A$ and $x \notin B$.

⁎ This contradicts with the fact that $A \subseteq B$, and thus

$$A \subseteq B \implies A - B = \varnothing. \quad \square$$

($\Leftarrow$): WTS: $A - B = \varnothing \implies A \subseteq B$.

Method 1 We will prove the contrapositive: $A \nsubseteq B \implies A - B \neq \varnothing$.

Suppose $A \nsubseteq B$. Then $\exists x \in A$ *s.t.* $x \notin B$.

By definition of set difference, $x \in A - B$, so $A - B \neq \varnothing$ as desired.

Method 2 Direct proof.

Suppose $A - B = \varnothing$.

By definition of set difference, $\forall x \in A, x \in B$.

By definition of subsets, $A \subseteq B$.

■

Definition 2.2.1 (Power set). The **power set** of A, denoted $\mathcal{P}(A)$, is the set of all subset of A. Therefore, $|\mathcal{P}(A)| = 2^n$ when $|A| = n$.

Theorem 2.2.1.

$$x \in \mathcal{P}(A) \iff x \subseteq A$$

Let A, B be sets. Prove that $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$

***Proof* (2).**

Let A, B be sets.

Suppose $X \in \mathcal{P}(A) \cup \mathcal{P}(B)$ [Notation: Capital X because X is a set!]

Then, by definition of union, $X \in \mathcal{P}(A)$ or $X \in \mathcal{P}(B)$.

WLOG, suppose $X \in \mathcal{P}(A)$. By definition of the power set, $X \subseteq A$.

Since $A \subseteq A \cup B$, if $X \subseteq A$, then $X \subseteq A \cup B$.

By definition of the power set, $X \in \mathcal{P}(A \cup B)$.

Hence, $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

■

Definition 2.2.2 (Cartesian Product). The **Cartesian product** of two sets A and B, denoted $A \times B$, is the set of ordered pairs (or tuples) (a, b) where $a \in A$ and $b \in B$, so

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

Remark. In general, $A \times B \neq B \times A$.

Theorem 2.2.2.

$$|A \times B| = |A| \times |B|$$

Let A, B, and C be sets. Prove that if $B \subseteq C$, then $A \times B \subseteq A \times C$.

***Proof* (3).**

Let A, B, and C be sets. Suppose $B \subseteq C$. WTS: $A \times B \subseteq A \times C$.

Let $x \in A \times B$. Then $x = (a, b)$ where $a \in A$ and $b \in B$.

Since $B \subseteq C$, if $b \in B$, then $b \in C$.

So, $x = (a, b) \in A \times C$.

Hence, $A \times B \subseteq A \times C$.

■

Definition 2.2.3 (Cartesian Power). For a set A and $n \in \mathbb{N}$, the **Cartesian power** A^n is the set

$$A^n = A \times A \times A \times \cdots \times A = \{\underbrace{(a_1, a_2, a_3, \cdots, a_n)}_{n\text{-tuple}} \mid a_1, a_2, a_3, \cdots, a_n \in A\}.$$

Example 2.2.1. Most common example: the Euclidean space: $\mathbb{R}^n$.

2.3 Collection of Sets

Definition 2.3.1 (Indexed Sets).

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n = \{x \mid x \in A_i \text{ f.s. } i\}$$

and

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n = \{x \mid x \in A_i \ \forall i\}$$

This notation also works when we don't have specified stopping point: $\bigcup_{i=1} A_i = \{x \mid x \in A_i \text{ f.s. } i\}$ and $\bigcap_{i=1} A_i = \{x \mid x \in A_i \ \forall i\}$

Example 2.3.1. Given the indexed sets, compute the unions and intersections:

1. $A_i = [0, i)$ for $i = 1, \cdots, n$

   (a) $\bigcup_{i=1}^{n} A_i = [0, n)$

   ***Proof* (1).**

   Claim: $\bigcup_{i=1}^{n} A_i = [0, 1)$.

   ($\subseteq$) Let $x \in \bigcup_{i=1}^{n} A_i$. So, $\exists k \in \{1, 2, \cdots, n\}$ *s.t.* $x \in A_k$.

   By definition of A_k, $x \in [0, k)$.

   That is, $0 \geq x < k$.

   Since $k \leq n$, this inequality gives us that $0 \leq x < k \leq n$.

   So, $x \in [0, n)$ as desired. $\square$

   ($\supseteq$) Let $x \in [0, n)$.

   Since $x \in [0, n)$, note that $[0, n) = A_n$.

   So $x \in A_n$.

   By definition of union, $x \in \bigcup_{i=1}^{n} A_i$

   Remark. To show $x \in \bigcup_{i=1}^{n} A_i$, find a specific i that works.

   ■

   (b) $\bigcap_{i=1}^{n} A_i = [0, 1)$

   ***Proof* (2).**

   Claim: $\bigcap_{i=1}^{n} A_i = [0, 1)$.

($\subseteq$) Let $x \in \bigcap_{i=1}^{n} A_i$.

So, $x \in A_i \ \forall i \in \{1, 2, \cdots, n\}$.

Specifically, $x \in A_1 = [0, 1)$. $\square$

($\supseteq$) Let $x \in [0, 1)$ [WTS: $x \in A \ \forall i \in \{1, 2, c \ldots, n\}$]

Let $k \in \{1, 2, \cdots, n\}$. We will show $x \in A_k$.

We know that $k \geq 1$ and $0 \leq x < 1$, so we have $0 \leq x < 1 \leq k$.

That is, $x \in [0, k)$.

So, $x \in A_k$

Since $k \in \{1, 2, \cdots, n\}$ was ***arbitrary***, we have shown that $x \in A_k \ \forall k \in \{1, 2, \cdots, n\}$.

So, $x \in \bigcap_{i=1}^{n} A_i$.

■

Remark. If $i \in \mathbb{Z}$, we have

(a) $\bigcup_{i=1}^{\infty} A_i = [0, \infty)$

(b) $\bigcap_{i=1}^{\infty} A_i = [0, 1)$

2. $A_i = [i - 1, i]$ for $i = 1, \cdots, n$

(a) $\bigcup_{i=1}^{n} A_i = [0, n]$

(b) $\bigcap_{i=1}^{n} A_i = \begin{cases} [0, 1] & \text{if } n = 1 \\ \{1\} & \text{if } n = 2 \\ \varnothing & \text{if } n > 2 \end{cases}$

Remark. If $i \in \{1, 2, \cdots\} = \mathbb{N}$, then we have

(a) $\bigcup_{i=1}^{\infty} A_i = [0, \infty)$

(b) $\bigcap_{i=1}^{n} A_i = \varnothing$

`Prove or disprove: If` A, B, `and` C `are sets, and` $A \times C = B \times C$, `then` $A = B$.

***Proof* (3).**

If $C = \varnothing$, then $A \times C = \varnothing = B \times C$

But A and B could be dramatically different.

■

Prove or disprove: If A, B, and C are sets, with $C \neq \varnothing$, and $A \times C = B \times C$, then $A = B$.

***Proof* (4).**

Suppose A, B, and C are sets.

Suppose $\exists a, c \in \mathbb{Z}$ *s.t.* $(a, c) = A \times C$

By definition of Cartesian product, $a \in A$ and $c \in C$.

Suppose $\exists b, c \in \mathbb{Z}$ *s.t.* $(b, c) \in B \times C$

Similarly, $b \in B$.

Suppose $A \times C = B \times C$. Then $A \times C \subseteq B \times C$ and $B \times C \subseteq A \times C$

($\subseteq$) WTS: $A \subseteq B$.

If $A \times B \subseteq B \times C$, we have $(a, c) \in B \times C$

Then, $a \in B$.

Since $a \in A$, we know $A \subseteq B$.

($\supseteq$) WTS: $B \subseteq A$

Similarly, since $B \times C \subseteq A \times C$, we have $(b, c) \in A \times C$.

Then, $b \in A$.

Since $b \in B$, we see $B \subseteq A$.

By definition of set equality, $A = B$.

■

Definition 2.3.2 (Partition). Let A be sets. A **partition** of A is a subset of the power set of A, $\mathscr{P} \subseteq \mathcal{P}(A)$, satisfying the following three properties:

1. If $X \in \mathscr{P}$, then $X \neq \varnothing \longrightarrow$ non-empty subsets of A
2. $\bigcup_{X \in \mathscr{P}} X = A$
3. If $X, Y \in \mathscr{P}$ and $X \neq Y$, then $X \cap Y = \varnothing \longrightarrow$ mutually disjoint.

Example 2.3.2. Let $A = \mathbb{Z}$ and consider the collection of subsets:

$$\mathscr{P} = \{\{\cdots, -4, -2, 0, 2, 4, \cdots\}, \{\cdots, -3, -1, 1, 3, 5, \cdots\}\}$$

Remark. Divisibility partisions $\mathbb{Z}$: Pick $n \in \mathbb{N},\ n > 1$. For every $m \in \mathbb{Z}$:

$$m = kn + r,$$

where r is the remainder, and $r = \{0, 1, 2, 3, \cdots, n - 1\}$

Theorem 2.3.1 (The Pigeonhole Principle - Idea). You have m pigeons and n pigeonholes (boxes for the pigeons). If $m > n$, then there will be at least one pigeonhole with more than pigeon. If $m < n$, then you will have at least one empty pigeonhole.

Theorem 2.3.2 (The Pigeonhole Principle). Let $A_1, A_2, \cdots, A_n$ be a collection of finite mutually disjoint sets. Let $A = \bigcup_{i=1}^{n} A_i$. if $|A| = k$ and $k > n$, then $|A_i| \geq 2$ *f.s. i.*

`Given any 11 integers, there is a pair of numbers whose difference is divisible by 10.`

***Proof* (5).**

Let $\{a_1, a_2, \cdots, 1_n\}$ be 11 integers.

Then, $a_i = 10k_i + r_i$ for $i \in \{1, \cdots, 11\}$, for $r_i = \{0, 1, 2, \cdots, 9\}$, and for $k_i \in \mathbb{Z}$.

Then, there are 10 possibilities for r_i, but there are 11 integers.

So, by the Pigeonhole Principle, at least 2 integers in our list must leave the same remainder on division by 10.

Say:

$$a_l = 10k_l + r \qquad \text{and} \qquad a_m = 10k_m + r \qquad \text{where} r \in \{0, 1, 2, \cdots, 9\}$$

Then,

$$\begin{aligned} a_l - a_m &= 10k_l + r - (10k_m + r) \\ &= 10k_l - 10k_m = 10(k_l - k_m) \end{aligned}$$

Since $k_l - k_m \in \mathbb{Z}$, we say that $10 \mid (a_l - a_m)$.

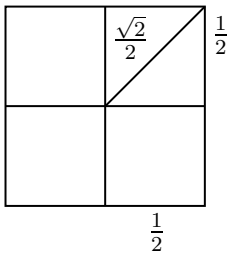
■

`Given 5 points in a unit square, there are two points within` $\frac{\sqrt{2}}{2}$ `of each other.`

Remark. Think carefully about the partition that gives the result!

***Proof* (6).**

Split the square horizontally and vertically by picking the midpoints of each side.



This divides our square into 4 bins.

Since there are 4 bins and 5 points, by the Pigeonhole Principle, at least 2 must be in the same bin.

Further note that in each bin, the largest distance between two points is $\frac{\sqrt{2}}{2}$.

Hence, there are 2 points with $\frac{\sqrt{2}}{2}$ of each other.

■

3 Functions

4 Binary Operations and Relations

4.1 Binary Operations

4.2 Equivalence Relations

Definition 4.2.1 (Relation). A **relation** R on a set A is a subset of $A \times A = \{(a, b) \mid a, b \in A.\}$

Notation 4.1. If two elements $a, b \in A$ are related, we write $(a, b) \in R$ or aRb. If a and b are not related, we write $(a, b) \notin A$ or $a \not Rb$.

Extension. More generally, if A and B are sets, then a relation R from A to B is a subset of $A \times B$.

Example 4.2.1. Describe the following relations by listing the elements of the relation

1. Let $A = \{1, 2, 3, 4, 5\}$ and $R_<$ is the relation "strictly less than."

   Answer. aRb if $a < b$.

   $$R_< = \{(1,2), (1,3), (1,4), (1,5), (2,3), (2,4), (2,5), (3,4), (3,5), (4,5)\}.$$

   □

2. Let $A = \{1, 2, 3, 4, 5\}$ and $R_|$ is the relation "divides."

   Answer.

   $$R_| = \{(1,1), (1,2), (1,3), (1,4), (1,5), (2,2), (2,4), (3,3), (4,4), (5,5)\}.$$

   □

3. Let $A = \mathbb{R}$ and $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y\}$.

   Answer. This relation describes the line of $y = x$ in a Cartesian plane. □

   Remark. Any subset of $A \times A$ is a relation. A relation does not have to have a actual meaning such as "strictly less than" or "divides."

Definition 4.2.2 (Reflexive, Symmetric, Antisymmetric, Transitive). A relation R on a set A is

- <u>Reflexive</u> if $(a, a) \in R \quad \forall a \in A$.

  ***Proof* (1).**

  Suppose $a \in A$. We'll show that $(a, a) \in R$.

  ■

  ***Disproof* (2).**

  $\exists a \in A$ *s.t.* $(a, a) \notin R$.

  ■

- **Symmetric** if $\forall a, b \in A$, if $(a, b) \in R$,then $(b, a) \in R$.

  ***Proof* (3).**

  Suppose $a, b \in A$. Suppose $(a, b) \in R$.

  We'll show that $(b, a) \in R$.

  ■

  ***Disproof* (4).**

  $\exists a, b \in A$ *s.t.* $(a, b) \in R$ and $(b, a) \notin R$.

  ■

- **Antisymmetric** if $\forall a, b \in A$, if $(a, b) \in R$ and $(b, a) \in R$, then $a = b$.

  ***Proof* (5).**

  Suppose $a, b \in A$. Suppose (a, b) and $(b, a) \in R$.

  We'll show that $a = b$.

  ■

  ***Disproof* (6).**

  $\exists a, b \in A$ *s.t.* (a, b) and $(b, a) \in R$ and $a \neq b$.

  ■

- **Transitive** if $\forall a, b, c \in A$, if $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$.

  ***Proof* (7).**

  Suppose $a, b, c \in A$. Suppose (a, b) and $(b, c) \in R$

  We'll show that $(a, c) \in R$.

  ■

Example 4.2.2. Show if the following relations are reflexive, symmetric, antisymmetric, or transitive.

1. Suppose $A \subseteq \mathbb{Z}$ or $\mathbb{N}$. Consider $R_<$.

   - **Reflexive**: False.

     Counterexample. $(1, 1) \notin R_<$. □

   - **Symmetric**: False.

     Counterexample. $(1, 2) \in R_<$, but $(2, 1) \notin R_<$. □

   - **Antisymmetric**: True.

     ***Proof* (8).**

     Impossible for (a, b) and $(b, a) \in R$. So the assumption part of the implication is wrong, which means the implication overall is true.

     ■

- **Transitive**: True

  ***Proof* (9).**

  Suppose $a, b, c \in A$ *s.t.* $a < b,\ b < a$

  Then, $a < c$. That is, $(a, c) \in R$.

■

2. Suppose $A \subseteq \mathbb{Z}$ or $\mathbb{N}$. Consider $R_|$.

- **Reflexive**: True

  ***Proof* (10).**

  Recall that $a \mid b$ if $b = ak$ *f.s.* $k \in \mathbb{Z}$.

  So, when $k = 1$, $b = a$. That is, $a \mid a \forall a \in Z$.

  That is, $(a, a) \in R$.

■

- **Symmetric**: False.

  Counterexample. $(1, 2) \in R_|$, but $(2, 1) \notin R_|$. □

- **Antisymmetric**: True if $A = \mathbb{N}$; False if $A = \mathbb{Z}$.

  ***Proof* (11).**

  Suppose $a, b \in A$ *s.t.* $a \mid b$ and $b \mid a$.

  Then, $b = ak$ and $a = bl$ *f.s.* $k, l \in \mathbb{Z}$.

  So, $a = (ak)l = akl$.

$$\begin{aligned} a - akl &= 0 \\ a(1 - kl) &= 0 \\ a = 0 \quad \text{or} \quad kl &= 1 \\ k = l = 1 \quad \text{or} \quad k &= l = -1. \end{aligned}$$

  That is, $a = 0$ or $a = b$ or $a = -b$. So the relation is antisymmetric if $A = \mathbb{N}$ because then only the option $a = b$ makes sense. If $A = \mathbb{Z}$, all three options are possible.

■

- **Transitive**: True.

  ***Proof* (12).**

  $a \mid b \implies b = ak \qquad b \mid c \implies c = bl$

  $\implies c = (ak)l = a(kl) \implies a \mid c.$

■

3. Consider the relation $R = \{(x, y) \in R^2 \mid x^2 + y^2 = 1\}$.

- **Reflexive**: False.

  Counterexample. $(0, 0) \notin R$ because $0^2 + 0^2 \neq 1$. □

- **Symmetric**: True

  ***Proof* (13).**

  Let $x, y \in \mathbb{R}$ *s.t.* xRy. Then, $x^2 + y^2 = 1$.

  Then, $y^2 + x^2 = 1$. That is, yRx.

  ■

- **Antisymmetric**: False.

  Counterexample. Consider $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ and $\left(\frac{\sqrt{3}}{2}, \frac{1}{2}\right) \in R$, but $\frac{\sqrt{3}}{2} \neq \frac{1}{2}$

  Or, consider $(0, 1)$ and $(1, 0) \in R$, but $0 \neq 1$. □

- **Transitive**: False.

  Counterexample. $(0, 1) \in R$ and $(1, 0) \in R$, but $(0, 0) \notin R$. □

4. Consider the relation $R_{\leq} = \{(x, y) \in \mathbb{R}^2 \mid x \leq y\}$.

   - **Reflexive**: True.
   - **Symmetric**: False.

     Counterexample. $(1, 2) \in R$, but $(2, 1) \notin R$. □

   - **Antisymmetric**: True.

     ***Proof* (14).**

     If $a \leq b$ and $b \leq a$, then $a = b$.

     ■

   - **Transitive**: True.

     ***Proof* (15).**

     If $a \leq b$ and $b \leq c$, then $a \leq c$.

     ■

5. Let S be the set of all finite subsets of $\mathbb{Z}$. Consider the relation R on S by ARB if $|A| = |B|$.

   - **Reflexive**: True.

     ***Proof* (16).**

     $|A| = |A|$.

     ■

   - **Symmetric**: True.

     ***Proof* (17).**

     If $|A| = |B|$, then $|B| = |A|$.

     ■

   .

- **Antisymmetric**: False.

  Counterexample. If $A = \{1, 2\}$ and $B = \{2, 3\}$, then $|A| = |B|$, but $A \neq B$. □

- **Transitive**: True.

  ***Proof* (18).**

  If $|A| = |B|$ and $|B| = |C|$, then $|A| = |C|$.

■

Definition 4.2.3 (Equivalence Relation). A relation R on a set A is an **equivalence relation** on A if it is reflexive, symmetric, and transitive.

Notation 4.2. When R is an equivalence relation, it is common to write $a \sim b$ (read as "a is equivalent to b") instead of aRb.

Remark. Equivalence relations are a way to generalize the idea of "equality."

Prove that $R_=$ on the set $\mathbb{R}$ is an equivalence relation.

***Proof* (19).**

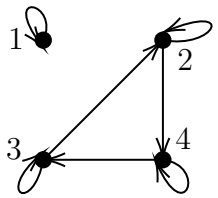
- **Reflexive**: $a = a \quad \forall a \in \mathbb{R}$
- **Symmetric**: $a = b \implies b = a \quad \forall a, b \in \mathbb{R}$.
- **Transitive**: $a = b,\ b = c \implies a = c \quad \forall a, b, c \in \mathbb{R}$.

■

Remark. We can use graphs and arrows to represent a relation.

- **Reflexive**: Every vertex needs a self loop.
- **Symmetric**: Every edge that is not a loop should look like $\iff$
- **Transitive**: We should have something like vector addition for every three vertexes.

Example 4.2.3. The relation $R = \{(1, 1), (2, 2), (2, 4), (3, 2), (3, 3), (4, 3), (4, 4)\}$ on the set $A = \{1, 2, 3, 4)\}$ as the follwoing graph:



From the graph we know that R is reflexive, but R is not symmetric or transitive.

Definition 4.2.4 (Congruence Modulo). Given a natural number $n \neq 1$, we defined a relation R on $\mathbb{Z}$, called **congruence mod** n, by aRb if $a - b = nk$ for some $k \in \mathbb{Z}$. That is, aRb if $n \mid (a - b)$.

Notation 4.3. We write $a \equiv b \mod n$ if a is congruent to b modulo n.

Remark. Two integers a and b are congruent modulo n if they give the same remainder upon division by n.

Let $n \in \mathbb{N}$. Prove that the relation

$$\equiv \mod n$$

on the set $\mathbb{Z}$ is an equivalence relation.

***Proof* (20).**

Let $n \in \mathbb{N}$.

- **Reflexive**: Let $a \in \mathbb{Z}$. [WTS: $a \equiv a \mod n$]

  We can see that $n \mid (a - a) = 0$. So, $a \equiv a \mod n$. □

- **Symmetric**: Let $a, b \in \mathbb{Z}$ *s.t.* $a \equiv b \mod n$. [WTS: $b \equiv a \mod n$]

  By definition 4.2.4, $n \mid (a - b)$ or $a - b = nk$ *f.s.* $k \in \mathbb{Z}$.

  Multiplying by (-1), we get that

  $$-(a - b) = -nk$$
  $$b - a = n(-k).$$

  Since $(-k) \in \mathbb{Z}$, then $n \mid (b - a)$. That is, $b \equiv a \mod n$.

  Hence, R is symmetric. □

- **Transitive**: Let $a, b, c \in \mathbb{Z}$ *s.t.* $a \equiv b \mod n$ and $b \equiv c \mod n$.

  WTS: $a \equiv c \mod n$.

  Since $n \mid (a - b)$ and $n \mid (b - c)$, then $a - b = nk$ and $b - c = nl$ *f.s.* $k, l \in \mathbb{Z}$.

  Adding the two equations, we get

  $$(a - \cancel{b}) + (\cancel{b} - c) = nk + nl$$
  $$a - c = nk + nl = n(k + l)$$

  Since $(k + l) \in \mathbb{Z}$, $n \mid (a - c)$. So, $a \equiv c \mod n$.

  Hence, R is transitive.

■

Definition 4.2.5 (Equivalence Class). Let R be an equivalence relation on a set A. Given $a \in A$, the **equivalence class containing** a is the subset

$$\{a \in A \mid x \sim a\}$$

Note that $\{a \in A \mid x \sim a\} = \{x \in A \mid a \sim x\}$ because x is symmetric.

Notation 4.4. We denote the equivalence class containing a by $[a]$.

Remark. Elements of the same equivalence class are said to be *equivalent*.

Proposition 4.2.1. Let R be an equivalence relation on a set A. Suppose $a, b \in A$. Then, $[a] = [b]$ if and only if aRb.

***Proof* (21).**

Let R be an equivalence relation on a set A. Suppose $a, b \in A$.

($\Rightarrow$): Suppose $[a] = [b]$. [WTS: aRb]

Recall $[a] = \{x \in A \mid x \sim a\}$ and $[b] = \{x \in A \mid x \sim b\}$.

Note that since R is **reflexive**, aRa. So, by definition, $a \in [a]$.

Since $[a] = [b]$, we have $a \in [b]$.

By definition 4.2.5, aRb as desired.

($\Leftarrow$): Suppose aRb. [WTS: $[a] = [b]$, $[a] \subseteq [b]$ and $[b] \subseteq [a]$]

($\subseteq$): Suppose $x \in [a]$ [WTS: $x \in [b]$]

Since $x \in [a]$, by definition, xRa.

Since xRa and aRb, by **transitivity** of R, xRb.

So, $x \in [b]$. Hence, $[a] \subseteq [b]$.

($\supseteq$): Suppose $x \in [b]$ [$x \in [a]$]

Since $x \in [b]$, by definition, xRb.

Since aRb, by **symmetry**, bRa.

Since xRb and bRa, by **transitivity**, xRa.

So, $x \in [a]$. That is, $[b] \subseteq [a]$.

So, $[a] = [b]$.

■

Proposition 4.2.2. Let R be an equivalence relation on a set A. Then the set

$$\{[a] \mid a \in A\}$$

of equivalence classes of R forms a partition of A.

***Proof* (22).**

■

Proposition 4.2.3. Let $\mathscr{P}$ be a partition of a nonempty set A. Define a relation R on A by aRb if a and b are in the same element of the partition. Then R is an equivalence relation on A.

***Proof* (23).**

■

5 The Integers

5.1 Axioms and Basic Properties

Definition 5.1.1 (Binary Operations). Binary operations of integers combine two integers to get another integer.

Axiom 5.1 (Integers). The **integers**, which we denoted by $\mathbb{Z}$, is a set, together with a nonempty subset $\mathbb{P}(\mathbb{Z}^+/\mathbb{N}) \subset \mathbb{Z}$ (which we call the **positive** integers), and two binary operations addition and multiplication, denoted by $+$ and $\cdot$, satisfying the following properties:

- (**Commutativity**) For all integers a, b, we have

$$a + b = b + a \qquad \text{and} \qquad a \cdot b = b \cdot a.$$

- (**Associativity**) For all integers a, b, c, we have

$$a + (b + c) = (a + b) + c \qquad \text{and} \qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

- (**Distributivity**) For all integers a, b, c, we have

$$(a + b) \cdot c = a \cdot c + b \cdot b.$$

- (**Identity**) There exists integers 0 (**additive identity**) and 1 (**multiplicative identity**), such that for all integers a, we have

$$a + 0 = a \qquad \text{and} \qquad a \cdot 1 = a.$$

- (**Additive inverses**) For any integer a, there exists an integer $-a$ such that

$$a + (-a) = 0.$$

- (**Closure for** $\mathbb{Z}^+$) If a, b are positive integers, then $a + b$ and $a \cdot b$ are positive integers.
- (**Trichotomy**) For every integer a, exactly one of the following three possibilities hold: either a is a positive integer, or $a = 0$, or $-a$ is a positive integer.
- (**Well-ordering**) Every nonempty subset of the positive integers has a smallest element.

Remark. We do not talk about the multiplicative inverse because for almost all integers, there does not exist an integer multiplicative inverse. Most of the multiplicative inverse belongs to $\mathbb{Q}$, and only 1 and -1 are two integers that have integer multiplicative inverses.

Claim 5.1.1. Let $a, b, c \in \mathbb{Z}$. If $a + b = a + c$, then $b = c$.

***Proof* (1).**

Since $a \in \mathbb{Z}$, $\exists(-a) \in \mathbb{Z}$ *s.t.* $a + (-a) = 0$ by *additive inverse*.

Adding $(-a)$ to the left side:

$$\begin{aligned}(-a) + (a + b) &= ((-a) + a) + b && [\textit{associativity}] \\ &= 0 + b && [\textit{additive inverse}] \\ &= b && [\textit{additive identity}]\end{aligned}$$

Similarly, we can show $(-a) + (a + c) = c$

So, we show that $b = c$.

■

Claim 5.1.2. Let $a \in \mathbb{Z}$. Then, $a \cdot 0 = 0 \cdot a = 0$.

***Proof* (2).**

Note by *commutativity*, $a \cdot 0 = 0 \cdot a$. So, it's enough to show $a \cdot 0 = 0$.

Notice that

$$\begin{aligned}a \cdot 0 + a \cdot 0 &= a(0 + 0) && [\textit{distributivity}] \\ &= a \cdot 0 && [\textit{additive identity}] \\ &= a \cdot 0 + 0 && [\textit{additive identity}]\end{aligned}$$

So, $a \cdot 0 + a \cdot 0 = a \cdot 0 + 0$. By Claim 5.1.1, we see that $a \cdot 0 = 0$.

■

Claim 5.1.3. Let $a, b \in \mathbb{Z}$. Then $(-a)b = a(-b) = -ab$.

Remark. The three expressions are different: $(-a)b$ means the additive inverse of a and multiplying that by b; and $-ab$ is the additive inverse of the product of a and b.

***Proof* (3).**

In this proof, we will show that $(-a)b = -ab$, and the other side will be left as an exercise.

WTS: $(-a)b$ is the additive inverse of ab. That is, WTS: $(-a)b + ab = 0$.

Notice that

$$\begin{aligned}(-a)b + ab &= ((-a) + a)b && [\textit{distributivity}] \\ &= 0 \cdot b && [\textit{additive inverse}] \\ &= 0 && [\text{From Claim 5.1.2}]\end{aligned}$$

So, $(-a)b$ is the additive inverse of ab. That is,

$$(-a)b = -ab.$$

■

Claim 5.1.4. If $a, b \in \mathbb{Z}$, then $(-a)(-b) = ab$.

Remark. We leave the proof of this claim as an exercise.

`Let` $x \in \mathbb{Z}$ `and` $x \neq 0$. `Then` $x^2 = x \cdot x \in \mathbb{Z}^+$.

***Proof* (4).**

Suppose $x \in \mathbb{Z}$ and $x \neq 0$. Since $x \neq 0$, by *trichotomy*, $x \in \mathbb{Z}^+$ or $-x \in \mathbb{Z}^+$

Case 1 Suppose $x \in \mathbb{Z}^+$. Then, $x^2 = x \cdot x \in \mathbb{Z}^+$ by *closure for* $\mathbb{Z}^+$.

Case 2 Suppose $-x \in \mathbb{Z}^+$. Then, $(-x)(-x) \in \mathbb{Z}^+$ by *closure for* $\mathbb{Z}^+$.

But $(-x)(-x) = x \cdot x = x^2$ by Claim 5.1.4. So, $x^2 \in \mathbb{Z}^+$.

■

Notation 5.1.

$$a - b = a + (-b)$$

$$ab = (a) \cdot (b)$$

Definition 5.1.2. Let $x, y \in \mathbb{Z}$. We say $x < y$ if $y - x \in \mathbb{Z}^+$.

Remark. We can use the axioms of closure and trichotomy to establish some well-known facts about inequalities.

Claim 5.1.5. Let $a, b, c \in \mathbb{Z}$. Then, exactly one of the following holds: $a = b$, $a < b$, or $b < a$.

***Proof* (5).**

Let $a, b \in \mathbb{Z}$

As before, by *additive inverse*, $\exists(-b) \in \mathbb{Z}$ *s.t.* $b + (-b) = 0$. Then $a - b \in \mathbb{Z}$.

By *trichotomy*, there are 3 cases to consider:

Case 1 $a - b = 0$, so then adding b on both sides, we get $a = b$.

Case 2 $a - b \in \mathbb{Z}^+$, then by Definition 5.1.2, $a > b$.

Case 3 $-(a - b) \in \mathbb{Z}^+$. But

$$\begin{aligned} -(a-b) &= -a - (-b) && [\textit{distributivity}] \\ &= -a + b \\ &= b - a. \end{aligned}$$

So, by Definition 5.1.2, $b > a$.

■

Claim 5.1.6. Let $a \in \mathbb{Z}$. If $a > 0$, then $-a < 0$, and if $a < 0$, then $-a > 0$.

Claim 5.1.7. Let $a, b \in \mathbb{Z}$. If $a > 0$ and $b > 0$, then $ab > 0$.

Claim 5.1.8. Let $a, b, c \in \mathbb{Z}$. If $a < b$ and $b < c$, then $a < c$.

Claim 5.1.9. Let $a, b, c \in \mathbb{Z}$. If $a < b$, then $a + c < b + c$.

Theorem 5.1.1 (Well-Ordering Principle). Every non-empty subset of the positive integers has a smallest element. (If $X \subseteq \mathbb{Z}^+$ and $X \neq \varnothing$, then $\exists x_0 \in X$ *s.t.* $\forall a \in X$ with $a \neq x_0$, we have $a - x_0 \in \mathbb{Z}^+$.)

Theorem 5.1.2. There is no integer x such that $0 < x < 1$.

***Proof* (6).**
Assume for the sake of contradiction that $\exists x \in \mathbb{Z}$ *s.t.* $0 < x < 1$.
Let $S = \{n \in \mathbb{Z} \mid 0 < n < 1\}$.
By our assumption, $x \in S$, so $S \neq$.
Note that, by definition, $S \subseteq \mathbb{Z}^+$.
By the Well-Ordering Principle (Theorem 5.1.1), S has a smallest element, say s_0.
We know that $0 < s_0 < 1$. Then $1 - s_0 \in \mathbb{Z}^+$.
Since $s_0, 1 - s_0 \in \mathbb{Z}^+$, there product $s_0(1 - s_0) \in \mathbb{Z}^+$ [*closure for* $\mathbb{Z}^+$]
That is, $s_0 - s_0^2 \in \mathbb{Z}^+$.
By Definition 5.1.2, we have $s_0 > S_0^2$.
As $x_0 \neq 0, s_0^2 \in \mathbb{Z}^+$ [Problem 5.1]
So, $0 < s_0^2 < s_0 < 1$.

⁎ This is a contradiction because s_0 is assumed to be the smallest element of S.

So, $\nexists x \in \mathbb{Z}^+$ *s.t.* $0 < x < 1$, or there are no integers between 0 and 1.

■

5.2 Induction

Corollary 5.2.1 (Introduction to Mathematical Induction). The most powerful consequence of the well-ordering principle (Theorem 5.1.1) is the technique of mathematical induction. The central idea of mathematical induction is that

To prove a statement that depends on an integer n, denoted $P(n)$, it is enough to prove it about a smaller integer m, $P(m)$, and then show that since $m < n$, $P(m) \implies P(n)$.

Theorem 5.2.1 (First Principle of Mathematical Induction). Let $P(n)$ be a statement about the positive integer n. Suppose that

1. $P(1)$ is true; and
2. $\forall k \in \mathbb{Z}$ *s.t.* $k \geq 2$, $P(k-1) \implies P(k)$.

Then, $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Remark. Equivalently, we can write the Condition 2 as $\forall k \geq 1,\ P(k) \implies P(k+1)$.

The following is a prove of Theorem 5.2.1

`If` $P(1)$ `is true, and` $\forall k \geq 2,\ P(k-1) \Rightarrow P(k)$, `then` $P(n)$ `is true` $\forall n \in \mathbb{N}$.

***Proof* (1).**

Let $P(n)$ be a statement about positive integers.

Suppose $P(1)$ is true and $\forall k \geq 2,\ P(k-1) \implies P(k)$.

Assume for the sake of contradiction that $\exists a \in \mathbb{Z}^+$ *s.t.* $P(a)$ is false.

Let $F = \{x \in \mathbb{Z}^+ \mid P(x) \text{ is false}\}$. Note that $F \subseteq \mathbb{Z}^+$. Further by assumption, $a \in F$, and so $F \neq \varnothing$.

So, by WOP (Well-Ordering Principle, Theorem 5.1.1), $\exists f_0 \in F$ that is the smallest element of F. [WTS: $F = \varnothing$]

Note that since $P(1)$ is true, then $1 \notin F$. Consider numbers $f_0 - 1 \in \mathbb{Z}$.

Since 1 is the smallest positive integer (a corollary of Theorem 5.1.2), and $f_0 \in \mathbb{Z}^+$, we have $f_0 > 1$. So, $f_0 - 1 \in \mathbb{Z}^+$.

Since f_0 is the smallest element of F and $f_0 - 1 \in \mathbb{Z}^+$. Then $P(f_0 - 1)$ is true. (Because $f_0 - 1 < f$ cannot be in the set of F, by our assumption).

By assumption, $P(f_0)$ is true because $F(f_0 - 1) \implies P(f_0)$.

$$\lightning \text{ But } f_0 \in F \text{ so } P(f_0) \text{ is false.}$$

So, it must be that $\forall n \in \mathbb{Z}^+,\ P(n)$ is true.

■

Remark. This proof strategy is also called proof by **the smallest counterexample.**

`The sum of the first` n `natural numbers is` $\dfrac{n(n+1)}{2}$.

***Proof* (2).**

Let $P(n)$ be the statement

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Base Case Consider $P(1) : 1 = \dfrac{1(1+1)}{2}$.

The right side is $\dfrac{1(2)}{2} = 1$. So, the statement is clearly true.

Inductive Steps Assume that for some $k \geq 1,\ P(k)$ is true. That is,

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2} \qquad ①$$

WTS: $P(k+1)$ is true. That is, we WTS:

$$1+2+3+\cdots+k+(k+1)=\frac{(k+1)(k+1+1)}{2}=\frac{(k+1)(k+2)}{2}$$

Adding $(k+1)$ to both sides of equation ①:

$$\begin{aligned}(1+2+3+\cdots+k)+(k+1)&=\frac{k(k+1)}{2}+(k+1)\\&=(k+1)\left(\frac{k}{2}+1\right)\\&=(k+1)\left(\frac{k}{2}+\frac{2}{2}\right)\\&=(k+1)\frac{(k+2)}{2}\\&=\frac{(k+1)(k+2)}{2}\end{aligned}$$

So, $(k+1)$ is true.

We've shown that $P(1)$ is true and $\forall k\geq 1,\ P(k)\implies P(k+1)$.

So, by Principle of Mathematical Induction (Theorem 5.2.1), $P(n)$ is true $\forall n\in\mathbb{Z}^+$.

■

Remark (The Role of the Base Case). Mathematical induction only works if you can "get the ball rolling." However, our first step in mathematical induction **need not to be** $n=1$.

Definition 5.2.1 (Factorial). We define factorial of a positive integer n as

$$n!=1\cdot 2\cdot 3\cdot\cdots\cdot n$$

Notably, we define the factorial of 0 as 1. That is,

$$0!=1.$$

`Prove that if` $n\in\mathbb{Z}$ `and` $n>4$, `then` $n!>2^n$.

***Proof* (3).**

Let $P(n)$ be the statement that $n!>2^n$.

Base Case WTS: $P(4)$ is true.

$$4!=(1)(2)(3)(4)=24,\qquad 2^4=16.$$

Since $24>16$, $P(4)$ is true.

Inductive Step Suppose *f.s.* $k\geq 4$, $P(k)$ is true. That is, $k!>2^k$ ①

WTS: $P(k+1)$ is true. That is, $(k+1)!>2^{k+1}$.

Multiplying both sides of ① by $(k+1)$: $(k!)(k+1) > 2^k(k+1)$.
So, we have $(k+1)! > 2^k(k+1) > 2^k(2) = 2^{k+1}$ since $k \geq 4$.
That is, $(k+1)! > 2^{k+1}$.

Since $P(4)$ is true and $\forall k \geq 4,\ P(k) \implies P(k+1)$, by Mathematical Induction Principle (Theorem 5.2.1), $P(n)$ is true $\forall n \geq 4$.

■

Remark (Generalizing Theorem). Often the role of induction is to generalize theorems from cases with few elements to an arbitrary but finite number of elements.

Example 5.2.1. Let $n \in \mathbb{Z}^+$. The following theorems can be proven using the Mathematical Induction Principle (Theorem 5.2.1).:

1. Suppose $a_1, a_2, \cdots, a_n$ are all even integers. Then $\sum_{i=1}^{n} a_i$ is even.
2. Suppose A and $B_1, B_2, \cdots, B_n$ are all sets. Then
$$A \cap \left(\bigcup_{i=1}^{n} B_i \right) = \bigcup_{i=1}^{n} (A \cap B_i)$$
3. **Theorem 5.2.2.** Let A be a finite set with n elements. Then, $\mathcal{P}(A)$ has 2^n elements.

Definition 5.2.2. Fibonacci Numbers

$$F_1 = 1 \qquad F_2 = 1 \qquad F_n = F_{n-1} + F_{n-2} \texttt{ for } n \geq 3$$

Example 5.2.2. The *Fibonacci numbers* are described as follows:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \cdots$$

`Prove that the Fibonacci sequence satisfies:`

$$F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}$$

`for all` n`.`

***Proof* (4).**
Let $P(n)$ be the statement that $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}$
Base Case $P(1)$: $F_1 = 1,\ F_{2(1)} = F_2 = 1$, So, $P(1)$ is true.
Inductive Step Suppose *f.s.* $k \geq 1,\ P(k)$ is true. That is,

$$F_1 + F_3 + \cdots + F_{2k-1} = F_{2k} \qquad ①$$

WTS: $P(k+1)$ is true. That is, $F_1 + F_3 + \cdots + F_{2k-1} + F_{2k+1} = F_{2k+2}$.

Add F_{2k+1} to both sides of equation ①:

$$F_1 + F_3 + \cdots + F_{2k-1} + F_{2k+1} = F_{2k} + F_{2k+1} = F_{2k+2}$$

So, $P(k+1)$ is true.

Since $P(1)$ is true and $\forall k \geq 1,\ P(k) \implies P(k+1)$, by Mathematical Induction Principle (Theorem 5.2.1), $P(n)$ is true $\forall n \in \mathbb{Z}^+$.

■

`Prove that if` $n \in \mathbb{Z}$ `and` $n \geq 0$, `then` $6 \mid 7^n - 1$.

***Proof* (5).**

Let $P(n)$ be the statement "$6 \mid 7^n - 1$."

Base Case WTS: $P(0)$ is true. That is, $6 \mid 7^0 - 1$.

Since $7^0 - 1 = 1 - 1 = 0$ and $6 \mid 0$, then $6 \mid 7^0 - 1$.

That is, $P(0)$ is true.

Inductive Step Suppose for some $k \geq 0$, $P(k)$ is true. That is, $6 \mid 7^k - 1$.

In other words, $\exists l \in \mathbb{Z}$ *s.t.* $7^k - 1 = 6l$ or $7^k = 6l + 1$.

WTS: $P(k+1)$ is true. That is, $6 \mid 7^{k+1} - 1$

Note that

$$\begin{aligned} 7^{k+1} - 1 = 7^k \cdot 7 - 1 &= 7(6l+1) - 1 \\ &= 42l + 7 - 1 \\ &= 42l + 6 \\ &= 6(7l+1). \end{aligned}$$

Since $7l + 1 \in \mathbb{Z}$, by definition of divides, $6 \mid 7^{k+1} - 1$.

Hence, $P(k) \implies P(k+1)$.

Since we've proven $P(0)$ is true and for $k \geq 0$ $P(k) \implies P(k+1)$, by Principle of Mathematical Induction (Theorem 5.2.1), for all $n \in \mathbb{Z}$ and $n \geq 0$, $P(n)$ is true.

■

Theorem 5.2.3 (Second Principle of Mathematical Induction). Let $P(n)$ be a statement about the positive integer n. Suppose that

1. $P(1)$ is true.
2. $\forall k \in \mathbb{Z}$ such that $k \geq 2$, if $P(i)$ is true for all $1 \leq i \leq k-1$, then $P(k)$ is true.

Then, $P(n)$ is true for all $n \in \mathbb{Z}^+$.

Remark. The phrasing "$P(i)$ is true for all $1 \leq i \leq k-1$, then $P(k)$ is true" can also be phrased as "$\forall k \geq 1$, $P(i)$ is true $\forall i \quad 1 \leq i \leq k$. Then, $P(k+1)$ is true.

Remark. The meaning of this phrasing, "$P(i)$ is true for all $1 \leq i \leq k-1$" is that $P(1)$ is true, $P(2)$ is true, $P(3)$ is true, $\cdots$, $P(k-2)$ is true, and $P(k-1)$ is true.

Remark. The Second Principle of Mathematical Induction (Theorem 5.2.3) is logically equivalent to the First Principle of Mathematical Induction (Theorem 5.2.1). However, in some cases, we have to use Theorem 5.2.3 in our proofs.

Remark. When using the Second Principle of Mathematical Induction, think about base cases! For example, if we need to show for $k-1 \geq 0$ $(k \geq 1)$ $P(k+1)$ is true, then our base cases are $P(0)$ and $P(1)$.

Given $n \in \mathbb{N}$, define a recursive function f as follows:

$$f(0) = 1 \qquad f(1) = 3 \qquad f(n) = 2f(n-1) - f(n-2) \quad \forall n \geq 2.$$

Prove that for all $n \geq 0$, $f(n) = 2n + 1$.

***Proof* (6).**

Let $P(n)$ be the statement "$f(n) = 2n + 1$."

Base Cases WTS: $P(0)$ and $P(1)$ are true.

$P(0)$ is true: [WTS: $f(0) = 2(0) + 1$]

Note that $2(0) + 1 = 0 + 1 = 1$ and $f(0) = 1$ by definition. That is, $P(0)$ is true.

$P(1)$ is true: [WTS:$f(1) = 2(1) + 1$]

Since $f(1) = 3$ by definition and $2(1) + 1 = 3$, $P(1)$ is true.

Inductive Steps Let $k \geq \mathbf{1}$ be *s.t.* $\forall i \quad 0 \leq i \leq k$, $P(i)$ is true. – *inductive hypothesis*

WTS: $P(k+1)$ is true.

Since $k \geq 1$, $k + 1 \geq 2$. So, by definition,

$$\begin{aligned} f(k+1) &= 2f(k+1-1) - f(k+1-2) \\ &= 2f(k) - f(k-1) \end{aligned}$$

Since $k - 1 \geq 0$, by inductive hypothesis, $P(k)$ and $P(k-1)$ are true.

So, $f(k-1) = 2(k-1) + 1$ and $f(k) = 2k + 1$.

Substituting, we have

$$\begin{aligned} f(k+1) &= 2(2k+1) - [2(k-1) + 1] \\ &= 4k + 2 - 2k + 2 - 1 \\ &= 2k + 3 \\ &= 2k + 2 + 1 \\ &= 2(k+1) + 1. \end{aligned}$$

Hence, by Mathematical Induction (Theorem 5.2.3), $P(n)$ is true $\forall n \geq 0$.

■