Emory University

MATH 250 - Foundations of Mathematics Learning Notes

Jiuru Lyu

February 1, 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**.

Solution. This is the *answer* part of an **example**. $\square$

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

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

$\blacksquare$

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.

Definition 1.1.2 (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 $x = \dfrac{a}{b}$.

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

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 $\exists n \in \mathbb{Z}\ s.t.\ \forall m \in \mathbb{Z},\ m = n^2$.

Solution.

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 $m \in \mathbb{Z}$.

$\square$

Definition 1.1.3 (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 $\neg P$.

Solution. $\neg P$: 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."

Solution. $\neg P$: 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: $P \vee \neg Q$.

Solution.

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

   Solution.

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

□

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

   Solution.

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

$\square$

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

   Solution.

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

$\square$

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

   Solution.

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

$\square$

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 ($\neg Q$)

Definition 1.2.4 (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 1.2.5 (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 1.2.6 (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:

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

Solution.

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

□

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 $x > M$.”

Solution.

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

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

□

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 $x \in \mathbb{Z}$

$\boxed{\text{Case 1}}$ 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.

$\boxed{\text{Case 2}}$ 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 $3 \nmid n$.

$\boxed{\text{Case 1}}$ 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, $3 \mid n^2 - 1$.

$\boxed{\text{Case 2}}$ 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 $x \in \mathbb{Z}$.

$\boxed{\text{Case 1}}$ 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.

$\boxed{\text{Case 2}}$ 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` $4k+4$ `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 $x \in \mathbb{Z}$.

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

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

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

$\boxed{\text{Case 2}}$ 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.* $\sqrt{2} = \dfrac{p}{q}$. 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 $\alpha \geq 1 \quad \text{or} \alpha \leq 0$.

⋇ 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.* $x = 2k$.

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

$\boxed{\text{Method 1}}$

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.

$\divideontimes$ This contradicts with the fact that even numbers cannot equal to an odd number.

$\boxed{\text{Method 2}}$

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

$\divideontimes$ 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 $q = \underbrace{p_1 p_2 p_3 \cdots p_n}_{\text{product}} + 1$. 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,

$$c = \frac{q}{p_k} = \frac{p_1 p_2 p_3 \cdots p_n + 1}{p_k} = \frac{p_1 p_2 p_3 \cdots p_n}{p_k} + \frac{1}{p_k}$$

Then,

$$\frac{1}{p_k} = c - \frac{p_1 p_2 p_3 \cdots p_n}{p_k}$$

Note that since p_k is one prime among $p_1, \cdots p_n$, $\dfrac{p_1 p_2 p_3 \cdots p_n}{p_k} \in \mathbb{Z}$.

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 $n \in \mathbb{Z}$.

$\boxed{\text{Case 1}}$ 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.

$\boxed{\text{Case 2}}$ 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 $y = 0$
($\Leftarrow$): 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, $(x+y)^2 = x^2 + y^2$.

$\blacksquare$

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.)
- $\emptyset$ the **empty set**
- $M = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$
- $\{\text{Ludacris}, \text{T.I.}, \text{Killer Mike}, \text{Big Boi}, \text{Andre 3000}, \text{Latto}\}$

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 ($\{1, 2\} = \{2, 1\}$).

Definition 2.1.4 (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 2.1.5 (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. $\emptyset$ 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 2.1.6. 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 2.1.7 (Universal Set). A **universal set** of A is a set within which A exists.

Definition 2.1.8 (Complement). The **complement** of A in its universal set U is $\overline{A} = A^C = U - A$.

Theorem 2.1.3.

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

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

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 2.1.9 (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).**
($\Rightarrow$): $(A \cap B) - C \subseteq (A - C) \cap (B - C)$
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, $x \in (A - C) \cap (B - C)$
($\Leftarrow$): $(A - C) \cap (B - C) \subseteq (A \cap B) - C$
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 $x \in \overline{A}$.
($\Leftarrow$): $\overline{B} \subseteq \overline{A} \implies A \subseteq B$.
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, $x \in B$.

■