MA1100 Discrete Math Notes

Nawwaf Sudi **2025 | Y2S1**

Preface This is my notes for MA1100 Discrete Math that i took in my second year in NUS. This note is non-comprehensive, meaning that it discusses surface level course materials and common problem solving techniques wherever appropriate. One should use this note as a supplement to the course material, serving as a quick-referencefor both those taking the course or planning to in the future. This note follows the flow of the online lectures and textbook of the time, and as such might not be the best option for future curriculum, but the content should be the same. This is the reason why you might notice that this note doesn't contain much exercises and examples: The textbook already has them.

1 Mathematical Language and Proofs

This chapter's content has most likely been discussed quite extensively before university, and most of you most likely have a good sense of familiarity with it. As such, I'll focus more on the problems for this one.

In Mathematics, any claims that you make requires a set of logical reasoning that back it up. This chapter is concerned with this mathematical language and the fundamental theory of proofs.We define the following:

Definition

Proposition, sometimes referred to as statement, is a statement that has exactly one truth value, either true or false, but not both.

For example, take $2 + 2 = 5$ as a statement Q. As such, we can say that:

$$Q \implies 2 + 2 = 5$$

is false.

Definition

Predicate is a form of a statement that has free variable(s) such that they can be either true or false, depending on the variable. Predicate is denoted by $P(x)$, where x is a free variable.

Together, these two makes up the basic 'building blocks' of the first half of this course.

1.1 Connectives

To put it simply, connectives are a logical connection between two statement. It forms a 'compound statement' tha behaves the same way as any other statement. There are a couple of such connectives: disjunction($\vee$), conjunction($\wedge$), negation($\neg$), implication($\implies$) and bi-implication($\iff$). I'll leave implication

and bi-implication towards the end of the chapter, as it is comparatively more complex than the first three.

1.1.1 Negation ($\neg$)

The negation of a statement can be thought of as the opposite of the statement. That is to say, if we were to have a statement P that was true, $\neg P$ (read not p) is false. The opposite is also true: if P were false, $\neg P$ would also be true. In a truth table:

Tabel 1: Truth table for $\neg$

P	$\neg P$
T	F
F	T

1.1.2 Conjunction ($\wedge$)

A good way to understand Conjunction is to think of it as an 'and'. Let P and Q be two statements. P $\wedge$ Q is true if both P and Q is true. If this is not ssatisfied, then P $\wedge$ Q is false.

Tabel 2: Truth table for $\wedge$

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

1.1.3 Disjunction ($\vee$)

In a similar manner to a conjunction, disjunction can be thought of as an 'or'. If we were to have two statements P and Q, P $\vee$ Q would be true if atleast one of P and Q are true. Otherwise, P $\vee$ Q is false.

Tabel 3: Truth table for $\vee$

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

1.1.4 Implication ($\implies$)

Let P and Q be two statements. P $\implies$ Q (read P implies Q) can be described as this: If P is true, then Q is also true. I'd like to think of it in a sense that P

is tied to Q: If we assume P $\implies$ Q is true, then whenever P is true, Q is also true. The reverse might not be true, however: Whenever Q is true, P might not also be true. The value of P is wholy dependent on Q.

Tabel 4: Truth table for $\wedge$

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

Implication can also be turned into a disjunction ($\vee$).

For statements P and Q,

$$P \implies Q \equiv (\neg P) \vee Q.$$

The equal sign ($\equiv$) is an equivalence sign, which denotes that two statments are logically equivalent. I'll go through it shortly. Which could be proven by comparing the truth tables.

1.1.5 Biconditional ($\iff$)

Bi-implication ($\iff$, read ïf and only if) is much easier to understand than implication. One can think of Bi-implication between two statement P and Q as stating that P and Q must have the same truth values.

Tabel 5: Truth table for $\wedge$

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

Given a biconditional statement, the following applies.

For statements P and Q,

$$P \iff Q \equiv (P \implies Q) \wedge (Q \implies P)$$

When using english sentences, these logical connectives tend to be interpreted in a different way. here are some of the most common:

Tabel 6: Interpretation in English

P $\implies$ Q	If P then Q, P only if Q, Q if P, P is sufficient for Q Q is neccesary for P
P $\iff$ Q	P if and only if Q, P iff Q, P is equivalent to Q, P exactly when Q, P is neccesary and equivalent to Q

1.2 Logical Equivalence

Definition

If two compound statement produce the same truth table, then we can say that the statements are logically equivalent.

As an example, say we have statements P and Q. We can produce the above truth table.

Tabel 7: Truth table of P and Q

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

Notice that $\neg (P \wedge Q)$ has the same truth table as $\neg P \vee \neg Q$. From the definition, we can say that $\neg (P \wedge Q)$ and $\neg P \vee \neg Q$ are logically equivalent, which we can write as:

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

1.2.1 Equivalence Laws

The following are laws that will be used to analyze compound statements. ld For any statement P, Q and R:

Definition

Negation Law

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

Idempotent Law

$$P \wedge P \equiv P.$$

$$P \vee P \equiv P.$$

Commutative Law

$$P \wedge Q \equiv Q \wedge P.$$

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

Associative Law

$$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)\,.$$

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

Distributive Laws

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

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

DeMorgan's Law

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

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

When determining the equivalence between two statements, one could always use a truth table to check both of their truth values. Infact, you could verify all the above laws by doing so. However, this is excrutiatingly slow, especially if the statements in questions contain more that three sub-statements. As such, being proficient with applying these laws are quite crucial.

Whenever you use DeMorgan's Laws to express a negation of a conjunction or disjuction, we can say that you've made a useful denial.

Example Assume n is a fixed positive integer. We are trying to find a usefull denial for the sentence

$$n = 2 \text{ or n is odd.}$$

To do this, we'll write out the statement in mathmatical notation. We'll take statement P and Q as the LHS and RHS, respectively. This would give use $P \vee Q$. Negating it,

$$\begin{aligned}\neg\,(P \vee Q) &\equiv \neg P \wedge \neg Q \\ &\equiv (n \neq 2) \wedge (\text{n is even})\,.\end{aligned}$$

We call $\equiv (n \neq 2) \wedge (\text{n is even})$ a useful denial.

Another tool that you might use when dealing statements involving real numbers is the Trichotomy Axiom.

Trichotomy Axiom

Given a fixed real number a and b, exactly one of these is true: $a < b$, $a = b$, $b < a$.

Say we want to find a negation of the statement $1 < x < 2$. We could split the statement into two: $x > 1$ and $x < 2$. Using DeMorgan's Laws:

$$\begin{aligned}\neg\,(P \wedge Q) &\equiv \neg P \vee \neg Q \\ &\equiv (x \leq 1) \vee (x \geq 2)\,.\end{aligned}$$

Notice the inequality signs. Since we are seeking a negation of the initial sign, we'll switch them to a $\geq$ and $\leq$ respectively.

1.3 Tautologies and Contradictions

I'll start of by defining the two terms:

Definition

Tautology is a statement form that is always true, no matter the value assignments to it's constituent statement variables.

Contradiction is a statement form that is always false, no matter the value assignemnts to it's constituent statement variables.

To demonstrate, take a statement P. From a truth table, we can see that

- $P \vee \neg P$ is a tautology.
- $P \wedge \neg P$ is a contradiction.

Tabel 8: Comparison

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

As you can see, both of the collumns are always true and false, respectively. When dealing with tautologies and contradiction in a statement, it is useful to keep in mind the following laws:

Let P be a statement. If T is a Tautology and C is a contradiction, then the following applies:

Identity Laws:

$$P \wedge T \equiv P.$$

$$P \vee C \equiv P.$$

Universal Bound Laws:

$$P \vee T \equiv T.$$

$$P \wedge C \equiv C.$$

Which should be intuitive

1.4 Converse, Inverse and Contrapositive

I'll start by defining the following: Let P and Q be statements. Then,

i. The *converse* of $P \implies Q$ is the statement $Q \implies P$.

ii. The *inverse* of $P \implies Q$ is the statement $\neg P \implies \neg Q$.

iii. The *contrapositive* og $P \implies Q$ is the statement $\neg Q \implies \neg P$.

When dealing with equivalence, the following also applies.

Let P and Q be statements.

i. *$P \implies Q$ is logically equivalent to $\neg Q \implies \neg P$ (it's contrapositive).*

ii. *$P \implies Q$ is not logically equivalent to $Q \implies P$ (its converse).*

iii. *The converse of the statement $P \implies Q$ is logically equivalent to it's inverse.*

While the lecture does not go into the greater significance of these definitions, I do still think that it is worth knowing. In general, these are usually used to proof conditional statements (implication and biconditional). Let's say I want to prove the statement $P \implies Q$. In many cases, the direct proof is very hard to do. As such, converting it into it's contrapositive $\neg Q \implies \neg P$ and proving that statement instead could be much easier. I encourage you to read it in your own time.

1.5 Quantifers ($\forall$, $\exists$)

I'll start of with an example. Let $P(n)$ be the predicate $n + 1 > 3$. Let $\mathbb{U}$ also be a the set of natural number $\mathbb{N}$. We could always assign a value to n from $\mathbb{N}$,, thus turning it into a statement. Another way to do this is by using quantifiers. There are two quantifiers discussed in this note: universal and existential quantifiers.

For the same predicate $P(n)$, we can derive both it's universal and existential statement from. For the universal statement, the from would be

$$\text{"for all x in } \mathbb{U},\ P(x)\text{"} \qquad \text{Notation: } (\forall\, x \,\epsilon\, \mathbb{U})\, P(x)\,.$$

$\forall$ here is called a universal quantifier. In a similar manner, we can derive the existential form of the statement:

$$\text{"there exist x in } \mathbb{U},\ P(x)\text{"} \qquad \text{Notation: } (\exists\, x\, \epsilon x \mathbb{U})\,.$$

We call $\exists$ an existential quantifier.

When negating a quantified statement, we may use the following:

Let $\mathbb{U}$ be the universe under consideration. For a predicate $P(x)$ whose only free variable is x,

$\neg[(\forall\, x\ \mathbb{U})\, P(x)]$ *is logically equivalent to* $(\exists\, x \,\epsilon\, \mathbb{U})\, \neg P(x)\,.$

$\neg[(\exists\, x\ \mathbb{U})\, P(x)]$ *is logically equivalent to* $(\forall\, x \,\epsilon\, \mathbb{U})\, \neg P(x)\,.$

For statements with multiple quantifier, we begin with the first quantifier, and work our way in. This is due to the fact that the order of the quantifier applied to a predicate changes its results. *You should give it a try.*

2 Techniques of Proof

2.1 Proof

Proof in Mathematics are only considered complete when it demonstrates an arguement that holds for all cases. Let's explore an example to demonstrate:

Example. We observe that:

- 31 is a prime number.
- 331 is a prime number.
- 3331 is a prime number.
- 33331 is a prime number.

From this observation, one would be tempted to assume that any number of the form $3333\ldots33331$ is a prime number.
We call this assumption a **conjecture**. More formally:

Definition

Conjecture is a mathematical statement that is taken to be true based on supporting evidence, yet it's validity has not been fully established.

To test this conjecture, we could try to come up with a number of the form $3333\ldots33331$ that is not a prime number. Note that:

$$333333331 = 17 \times 19607843.$$

by the definition of prime numbers, makes 333333331 not a prime. Therefore, we can say that the conjecture is false. This method of disproving a conjecture is called a **counterexample**.

Let's now define the definition of proof, more formally:

Definition

Proof is a logical arguement that extablishes a truth of a mathematical statement.

There are three kinds of proof:

- direct proof
- indirect proof
- mathematical induction

We will discuss the first two in this chapter, while mathmatical induction will be left for the next one.
In addition to proof, I'll also define the following:

Theorem as a mathematical statement that has been proven. It's sometime's referred to as a proposition

Lemma as a 'side-effect' or 'stepping stone' that appears at the proccess of proving a theorem.

Claim as a result that must be achieved in proving a theorem.

2.2 Inference

Inference is the proccess of deducing a result of a theorem in such as way that the theorem is fundamentally preserved. I'll demonstrate it with the following: Suppose we have a fixed integer n, and we know the following:

- If and integer is even, then it's square is also even.
- n is even.

The answer is n is even, which seems obvious. However, let's use the rule of inference. Let P and Q be the statement n *is even* and n^2 *is even*, respectively. We know that $P \implies Q$ is true. Here's I'll follow a inference rule called *modus ponens*. It's represented by the following diagram:

$$\frac{P \implies Q \quad P}{\therefore Q}.$$

From the diagram, we can conclude that Q is true. The symbol $\therefore$ stands for therefore.

The following are some rules of inference:

Rules of Inference

Modus Ponens

$$\frac{P \implies Q \quad P}{\therefore Q}$$

Modus Tollens

$$\frac{P \implies Q \quad \neg Q}{\therefore \neg Q}$$

Generalization

$$\frac{P}{\therefore P \implies Q}$$

Transitivity

$$\frac{P \implies Q \quad Q \implies R}{\therefore P \implies R}$$

Specialization

$$\frac{P \wedge Q}{\therefore P}$$

Division into Cases

$$\frac{P \wedge Q \quad P \implies R \quad Q \implies R}{\therefore R}$$

Elimination

$$\frac{P \vee Q \quad \neg Q}{\therefore P}$$

2.3 Properties of Real Numbers

The properties of real numbers can largely be divided into three catagories: algebraic properties, ordered properties and completeness properties.

The algrebaic properties of real numbers

There are two binary operations, ($+$ and $\times$) that is defined for real numbers. For all real numbers, we have:

Closure under $+$ and $\times$	$a+b$ and ab are real numbers.
Commutative laws	$a+b=b+a$, $ab=ba$.
Associative laws	$(a+b)+c=a+(b+c)$, $(ab)\,c=a\,(bc)$.
Distributive laws	$a\,(b+c)=ab+ac$.
Identities	$0\neq 0$, $a+0=a$, $a\cdot 1=a$.
Additive inverses	There is a unique real number $-a$ such that $a+(-a)=0$.
Subtraction	$a-b$ is defined to equal $a+(-b)$.

The ordered property of real numbers

The order relation $<$ has the following properties: For all real numbers a, b, c, we have:

Trichotomy	Exactly one of the following holds: $a<b$, $a>b$ or $a=b$.
Transitivity	If $a<b$ and $b<c$, then $a<c$.
Order Property 1	If $a<b$, then $a+c<b+c$.
Order Property 2	If $a<b$, and $c>0$, then $ac<bc$.
Order Property 3	If $a<b$ and $c<0$, then $ac>bc$.

The completeness property

If a nonempty subset of $\mathbb{R}$ has an upper bound, then it has a leat upper bound.

Most of these properties are intuitive, maybe even obvious. However, I do want to remark on the completeness property. It's something that's only really studied in real analysis, and most likely won't come up in any test of thie module. However, this property implies the result of the Archimedian Property and the theorem on the existence of nth root. If you are familiar with the property, the following proof might be much easier to understand.

Archimidean Property

For every real number x, there is a positive integer n such that $n>x$.

In mathematical notation, this can be written as $(\forall x\epsilon\mathbb{R})\,(\exists n\epsilon\mathbb{Z}^{+})\,[n>x]$.

The existence of nth root

Let $n \in \mathbb{Z}^+$:

i. Assume that n is even. The every $x \in \mathbb{R}$ with $x \geq 0$ has a real "*nth root*"; i.e., there is a unique nonnegative real number denoted by $x^{\frac{1}{n}} = \sqrt[n]{x}$ which satisfies

$$\left(x^{\frac{1}{n}}\right)^n = x.$$

ii. Assume that n is even. The every $x \in \mathbb{R}$ has a real "*nth root*"; i.e., there is a unique nonnegative real number denoted by $x^{\frac{1}{n}} = \sqrt[n]{x}$ which satisfies

$$\left(x^{\frac{1}{n}}\right)^n = x.$$

One way to think about this theorem that helped me understand this intuitively is by analyzing the criterion $\left(x^{\frac{1}{n}}\right)^n = x$. We could rewrite the root $x^{\frac{1}{n}}$ as $x^n = a$, where a is an arbitrary number from subset $\mathbb{R}$. Notice that in this new expression for the root, the LHS matches the RHS in exactly one x, since the function x^n hae exactly one value for every x.

Something to also note here is that, since integers $\mathbb{Z}$ is a subset of $\mathbb{R}$, they have all the properties of $\mathbb{R}$. In addition, they also have the following property:

Closure property of real numbers

If a and b are integers, then $a + b$ and ab are also integers.

2.4 Direct Proof

Direct proof is a method of proofing that tackles the statement head-on. I'll start with proofing the statement $P \implies Q$.

2.4.1 Proof for $P \implies Q$

First let's analyze the statement. By the truth table,

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

we can see that the truth value for $P \implies Q$ depends heavily on P. If P is false, then no matter the value of Q, $P \implies Q$ is true. If P is true, Q would need to be true as well in order for the statement to be true. Given an arbitrary statement P and Q, we can follow the following procedure of proving $P \implies Q$.

1. Begin by *assuming* that P is true.
2. Apply rule of inference to get new statements.

3. Repeat step 2 until we can see that Q is true.

This proof is said to be sufficient, as in, it is enought to proof the statement. To understand this better, let's take a look at an example.
Let n be an integer. Proof that if n is even, then n^2 is even. I'll give the definition of odd and even integers for this example

Definition

$$n \text{ is even if } (\exists k \epsilon \mathbb{Z})\,[n = 2k]$$
$$n \text{ is odd if } (\exists k \epsilon \mathbb{Z})\,[n = 2k + 1].$$

I'll also introduce the division algorithm

Division Algorithm

Let a, $b \epsilon \mathbb{Z}$with $b > 0$. Then, there exist unique q,r $\epsilon \mathbb{Z}$ such that

$$a = bq + r \qquad \textit{where } 0 \leq r < b..$$

This algorithm would be proven in chapter 6, where we delve into number theory. For the time being, we would use it to solve problem without scrutinizing it. In the division theorem, if we take b = 2, we can write every integers as

$$a = 2q,$$

$$a = 2q + 1.$$

Continuing with our example, if we take $n = 2k$, which is even,

$$n^2 = (2k)^2 = 4k^2 = 2\left(2k^2\right).$$

Since $2(2k^2)$ is an integer, we can see that it is also even. As such the original statement can be said to be proven.

2.4.2 Proving $(\forall x \epsilon \mathbb{U})\, P(x)$

Now, we'll intend to proof the statement $(\forall x \epsilon \mathbb{U})\, P(x)$. To make a direct proof of $(\forall x \epsilon \mathbb{U})\, P(x)$, we'll let $x \epsilon \mathbb{U}$. Then, we'll demonstrate that $P(x)$ is true. Consider the following example:
Prove that the sum of an even and odd integer is odd.
In mathematical notation:

$$(\forall m \epsilon \mathbb{Z})\,(\forall n \epsilon \mathbb{Z})\,[(\text{m is even}) \vee (\text{n is odd}) \implies m + n \text{ is odd}]..$$

We'll start by assuming that m and n is even and odd, respectively. Since m is even, there is an integer i such that $m = 2i$. Similarly, there is an integer j such that $n = 2j + 1$. As such,

$$m + n = 2i + (2j + 1) = (2j + 2i) + 1 = 2\,(i + J) + 1.$$

Since $i + j$ is an integer, $m + n$ is odd.

2.5 Additional properties of real numbers

It is now time to delve deeper into some properties of real numbers that might seems obvious, but would nontheless prove useful when solving proof problems.

For all real numbers a, $a \cdot 0 = 0$.

Since $a \epsilon \mathbb{R}$ and $0 = 0 + 0$, by the distributive law,

$$\begin{aligned} a \cdot 0 &= a\,(0 + 0) = a \cdot 0 + a \cdot 0 \\ a \cdot 0 + (-a \cdot 0) &= (a \cdot 0 + a \cdot 0) + (-a \cdot 0) \\ 0 &= a \cdot 0 + (a \cdot 0 - a \cdot 0) \\ a \cdot 0 &= 0 \end{aligned}$$

For all real numbers a, we have

$$-a = (-1)\,a, .$$

that is, the additive inverse of a is equal to the product of -1 and a.

I'll leave the proof of this one to the reader.

Recall that a real number r is defined as a rational number $\mathbb{Q}$ if there are integers a and b, with $b \neq 0$ such that r a/b.

The Closure Property of Rational Numbers

If r and s are rational numbers, then $r + s$ *are also real numbers.*

2.5.1 Divisibility of Integers

Recall that $\mathbb{Z}$ denotes the set of all integers, and $\mathbb{Z}^+$ denotes the set of all positive integers(in some textbook, it is sometimes denoted as $\mathbb{N}$, but here we denote it as such to avoid the ambiguity of the number 0.) Let's define the divisibility of an integers:

Definition

Let a and b be integers. We would say that a **divides** b if there exists $n \epsilon \mathbb{Z}$ such that $b = an$. In other words, $(\exists n \epsilon \mathbb{Z})\,(b = an)$.

We denote this divisibility by the symbol $|$. Divisibilty also has a trasitive relation:

For all integers a, b, c, if $a|b$ *and* $b|c$, *then* $a|c$.

As a consequence of this, we also have the following:

For all integers a, b, c, if $a|b$ *and* $a|c$, *then* $a|\,(bm+cn)$ for some integers m, n.

and

If $a, b \epsilon \mathbb{Z}^+$, *and* $a|b$, then $a \leq n$.

2.5.2 Counterexample

I've already defined informally in the first chapter, so I'll delve into it deeper here.Recall that a counterexample is a way to prove that a statement is false, or proving it's negation true, by naming single condition that would contradict the statement.

2.5.3 Proof by cases

While one sometimes find it difficult to come up with some single general arguement to prove a statement, one could divide the arguement into multiple cases. Take the following example:

$$\text{For all integers} a, a\,(a+1) \text{ is even..}$$

When proving a statemnt such as this, it is often useful to divide it into multiple cases. In this case, we could divide the proof into two cases: a is even and a is odd. We would then proceed to proof that this statement holds for all the cases.

2.5.4 Working Backwards

This is another method of proving a conditional statement. Suppose we have the statement $P \implies Q$. Instead of assuming P is true, as is the case for the usual method of proving conditional statements, we *know* that P is true. We would then start by assuming that Q is true, then *work our way backwards* from Q to P. In other words, we would check the reversibilty of the intermediate arguements that leads to Q, then reverse those arguements and obtain a valid proof of $P \implies Q$.

2.5.5 Proving biconditional statements

Recall that $P \iff Q$ is equivalent to the statement $(P \implies Q) \wedge (Q \implies P)$. As such, when proving a biconditional statement, we have to proof the following:

- the forward direction $P \implies Q$
- The backwards direction $Q \implies P$

2.5.6 Uniqueness of Proof

Sometimes, we not only want to proof that an object exists, but also that proof that there is exactly one instance of that object. Take the statement there is a unique x such that $P(x)$. This can be written as

$$(\exists x \, \epsilon \mathbb{U}) \left((P(x) \wedge (\forall y \, \epsilon \mathbb{U}) (P(y) \wedge P(z) \implies y = z)) \right).$$

2.6 Indirect Proof

Unlike direct proof, which proofs the statement itself, indirect proof uses contradiction and contrapositives and proving them that way. We'll start of with contradictions.

2.6.1 Proof by Contradiction

Proof of contradiction is made by assuming a condition other than the one laid out by the statement and finding a contradiciton in the arguement, thus indirectly proofing the statement. In general, we follow the following procedure:

- Begin by assunming $\neg P$ is true.
- We then come up with a contradiction.
- Conclude that P is true.

2.6.2 Proof by contrapositive

Suppose we want to prove $P \implies Q$, Sometimes, proving the statement directly might be a bit challenging. So we rewrite the statement into it's contrapositive $\neg Q \implies \neg P$.

2.6.3 Proving or statements

We now formulate a method to prove some aritrary statement $P \vee Q$. Recall that $P \implies Q$ is equivalent to $\neg P \vee Q$. We could, then, manipulate the or statement in such a way that would allow us to turn it into a conditional statement, which could be proven by the already laid out methods.

By and large, there are two ways to turn $P \vee Q$ into a conditional statement. We could convert it into either a $\neg P \implies Q$ or a $\neg Q \implies P$, a product of the commutative property. Either way, proving it would require us to assume the first composite statement is true, then prooving the second composite statement.

2.7 Important Theorem

These are some important theorem that is incredibly useful when approaching proving problems. We would leave the proof of the theorem for later chapters.

Fundamental Theorem of Arithmetic

Any positive integers greater than 1 can be written as a product of primes. More precisely, if $n \epsilon \mathbb{Z}$ and $n > 1$, then there exists primes $p_1, p_2, \ldots, p_m$ such that

$$n = p_1 p_2 \ldots p_m.$$

We call this expression the prime facotrization of n. ***This product of primes is unique, save for the order in which the primes appear.***

Euclid's Theorem

There are infinitely many prime numbers

3 Induction

This chapter picks off from the last chapter and discusses induction as a methdo of proving a statement. We'll first start by the definition of recursively defined functions.

3.1 Recursively Defined functions

Addition associates an ordered pair of real numbers by it's sum. Each time, however, we could only add two numbers. You could write $a_1 + a_2, a_3$, but the operator only adds them up two at a time. We call this sort of operation a **binary operation**.

Given real numbers $a_1, a_2, \ldots a_n$ for $n \epsilon \mathbb{R}$, we denote

$$\sum_{k=1}^{n} a_n = \text{ the sum of } a_1, a_2, \ldots, a_n.$$

3.2 Principle of Mathematical Induction

In general, the way one uses induction is by testing noth the base case of a statement and any other arbitrary values to see if it holds up. The principle can be defined as

The Principle of Mathematical Induction

Let $n \epsilon \mathbb{Z}^+$, *and* $P(n)$ *be a statement regarding* n. *If*

1. The statement $P(1)$ is true and
2. The statement $P(m) \implies P(m+1)$ is true for all $m \epsilon \mathbb{Z}^+$,

then, for all positive integers n, $P(n)$ *is true.*

In mathematical notation, we would write it as

$$\{P(1) \wedge (\forall m \in \mathbb{Z}^+)[P(m) \implies P(m+1)]\} \implies (\forall n \in \mathbb{Z}^+) P(n).$$

The principal of mathematical induction is a technique that could be used to proof statements of the form $(\forall n \in \mathbb{Z}^+)$.

Using the Principles of Mathematical Inductions, we can come up with some more theorem for the sum of real numbers:

For all $n \in \mathbb{Z}^+$, we have

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

and

$$\sum_{k=1}^{n} = \frac{n(n+1)(2n+2)}{6}.$$

We could also write a more general version of PMI, where the base case corresponds to an integer n_0 which can be 0 or negative.

The Principle of Mathematical Induction (Modified)

Let n be an integer. For each integer n such that $n \geq n_0$*, let P(n) be a statement on n.*

1. The statement $P(n_0)$ is true and
2. For all integers $m \geq n_0$,

   if P(m) is true, then P(m + 1) is true.

Then, for all positive integers n, $P(n)$ *is true.*

3.3 Strong Induction

For certain statements, PMI could not provide a good way to prove the statements. As such, we define the Principle of Strong Mathematical Induction.

The Principle of Strong Mathematical Induction

Let $n \in \mathbb{Z}^+$*, and* $P(n)$ *be a statement regarding n. If*

1. The statement $P(1)$ is true and
2. For all positive integers m,

   if $P(1), P(2), \ldots, P(m)$ *are true, then* $P(M+1)$ *is true.* .

Then, for all positive integers n, $P(n)$ *is true.*

Do note though that, despite the name, both PMI and PSMI are equivalent. You should decide which one you use based on the question, as PSMI tends to be too general to use in a concise manner, leading to longer proofs.

4 Sets

There are two types of set theories:

- **Naive set theory.** informal and intuitive, which this course will cover
- **Axiomatic Set theory.** Based on formal logic, which is discussed in MA1100T and MA3205

We'll start by the definition of a set.

> **A set** is a collection of objects, ech of which is is called an element of the set.

When dealing set problems, there are some general rule one must follow:

1) Fix a set of $\mathbb{U}$ which contains all the mathematical objects in consideration. In the previous chapters, we'd usually fix $\mathbb{U}$ to $\mathbb{R}$, but in the case of sets, one usually fix it to $\mathbb{Z}$.

2) Given set A and a given fixed object in $\mathbb{U}$, we can write that x is an element of A by these notations:

   - "x is an element of A", or $x \, \epsilon \, A$.
   - "x is not an element of A", or $x \;\; /\epsilon \, A$

- Two sets are equal if and only if they have the same elements. As such, a set is uniquely determined by its elements.

There are alos multiple ways of writing a set:

1 Explicitly writing the set.

2 Use the set builder notation.

3. Use constructive definition.

An empty set is a unique set that has zero elements inside it. It is denoted by $\emptyset$,