Contents

1 The language of mathematics  
2 Implications  
3 Proofs  
4 Proof by contradiction  
5 The induction principle  
6 The language of set theory  
7 Quantifies  
8 Functions


1 The language of mathematics

1.1 Mathematical statements

Mathematical statements is a broad concepts. It includes proposition and predicates.

A proposition is a sentence which is either true or false. A predicate is a sentence which depends on some free variables and it can be both true or false depending on the values of the free variables.

Example of two propositions:

(i) $1 + 1 = 2$.

(ii) $\pi = 2$.

Here (i) is true while (ii) is false.

Example 1.1.1. "Every even integer greater than 2 may be written as the sum of two prime numbers" is a proposition. But we don’t know it is true or false. We often call a proposition like this as an open problem.

This is the Goldbach’s Conjecture. This conjecture is raised by Christian Goldbach in 1742. The Chinese famous mathematician Jingrun Chen proved a "close" proposition to the Goldbach’s Conjecture in 1966: every even integer greater than 2 can be written as the sum of a prime and a semiprime (the product of two primes).

Then let us look at two examples which are not propositions.

Example 1.1.2.

(i) $m < n$; (ii) $x$ is a special number; (iii) $n - m$.

Here (i) is a sentence but it is not a proposition. Because we don’t know whether it is true or not until the values of $n, m$ are given. Sentences like this are called predicates. The symbols like $n, m$ are called free variables.

(ii) is a sentence but it is meaningless in mathematics because we don’t know what "special" means. (ii) can be a predicates if we define, for example, “special” to be prime numbers’ square.

(iii) $n - m$ is not a sentence.

Definition 1.1. The word statement will be used to denote a sentence which is either a proposition or a predicate.

1.2 Logical connectives

In mathematics, we often need to consider a large number of statements. We need logical connectives to connect them or to tell the logical relations of them.

We introduce three of the logical connectives: “or”, “and”, “not”.

Suppose we have two statements: $P, Q$. If one of $P$ and $Q$ is true, then $P$ or $Q$ is true.
Example 1.2.1. (1) If $P = \text{“} n < m \text{”}$ and $Q = \text{“} n \geq m \text{”}$, then $P$ or $Q$ is true.
(2) A true proposition: $ab = 0$ if $a = 0$ or $b = 0$.

The connective “or” is sometimes hidden in other notations:

- $a \leq b$ : means $a < b$ or $a = b$
- $a = \pm b$ : means $a = b$ or $a = -b$

Now we consider “and”. We use “and” when we want to assert that two things are both true.

Example 1.2.2. (1) If $P = \text{“} n < m \text{”}$ and $Q = \text{“} n \geq m \text{”}$, then $P$ and $Q$ has to be false.
(2) $3 < \pi < 4$ means $\pi > 3$ and $\pi < 4$.

Now we discuss “not”. A statement $P$ is true is and only if not $P$ is false.

Example 1.2.3. Let $f(x)$ be a polynomial and $a$ be a real number. Write the negation of the following statement: if $f(a) = 0$ then $a$ is positive.

Solution. Consider $P$ to be a statement that $f(a) = 0$ and $Q$ to be a statement that $a$ is positive. Then the assertion (or statement) here is “$P$ implies $Q$”. The negation of this is “not ($P$ implies $Q$)”. The negation is the same as “$P$ does not implies $Q$”. And so it is “($P$) and (not $Q$) can happen at the same time”.

Thus the correct negation is: it is possible that $f(a) = 0$ and $a$ is non-positive i.e. there exists $a \leq 0$ such that $f(a) = 0$.

We will discuss this more in Theorem 2.2.

Example 1.2.4. Read the tables 1.2.1, 1.2.2 in the textbook.

2 Implications

Mathematics is primarily concerned with establishing the truth of statements. This is achieved by giving a proof of the statement. Implication is one of the key in proofs.

2.1 Implications

The definition of implications is the following: given two statements $P$ and $Q$, we say $P$ implies $Q$ if whenever $P$ is true then we must have that $Q$ is true. We use the notation $P \implies Q$.

Example 2.1.1. Suppose that $P$ is the statement that “$x^2 - x - 2 > 0$”, $Q_1$ is the statement that “$x > 2$ or $x < -1$” and $Q_2$ is the statement that “$x \neq 0$”. Then we have

$$P \implies Q_1 \implies Q_2.$$
Actually here we also have

\[ Q_1 \implies P. \]

But \( Q_2 \) does not imply \( Q_1 \) written as

\[ Q_2 \nRightarrow Q_1. \]

**Definition 2.1.** In an implication \( P \implies Q \), \( P \) is called the *hypothesis* or *antecedent* and \( Q \) is called the *conclusion* or *consequent*.

**Example 2.1.2.** Consider the following statements:

(i) \((\pi < 4) \implies (1 + 1 = 2)\);
(ii) \((\pi < 4) \implies (1 + 1 = 3)\);
(iii) \((\pi < 3) \implies (1 + 1 = 2)\);
(iv) \((\pi < 3) \implies (1 + 1 = 3)\).

(i)(iii)(iv) is OK. For (i), both the assumption and the conclusion are true. For (iii)(iv), the assumption can never be true, so we do not care what the conclusion is in this case. For (ii), even under the assumption, the conclusion is false.

**Theorem 2.2.** The followings are equivalent (have the same meaning)

- \( P \nLeftrightarrow Q \);
- “\( P \implies Q \)” is false;
- “\( P \) and (not \( Q \))” is true.

**Reading implications.** \( P \implies Q \) is the same as

- \( P \) implies \( Q \);
- \( Q \) if \( P \);
- \( P \) only if \( Q \);
- \( P \) is sufficient for \( Q \);
- \( Q \) is necessary for \( P \).

**Definition 2.3.** We define *equivalence* of two statements \( P, Q \) (written as \( P \Leftrightarrow Q \)) as

\[(P \implies Q) \quad \text{and} \quad (Q \implies P).\]

We read \( P \Leftrightarrow Q \) as
• \( P \) is equivalent to \( Q \).

• \( P \) is necessary and sufficient for \( Q \).

• \( P \) if and only if \( Q \) (sometimes written \( P \) iff \( Q \)).

• \( P \) precisely when \( Q \).

**Definition 2.4.** By *universal* statement we mean the statement is always true for all values of variables in the statement. For example “\( a^2 + b^2 \geq 0 \) for all real numbers \( a, b \)”.

### 3 Proofs

A proof of a mathematical statement is a logical argument which establishes the truth of the statement. The steps of the logical argument are usually provided by implications.

#### 3.1 Direct proofs

**Example 3.1.1.** *For positive real numbers \( a \) and \( b \), prove \( a < b \Rightarrow a^2 < b^2 \).*

Before the proof, we need to list the assumptions that people take for granted. The following basic properties of real numbers are often referred to as *Axioms*. Let \( a, b, c \) be any real numbers.

(i) Trichotomy law. For each pair of real numbers \( a, b \), one of the following holds: \( a < b, a = b, a > b \).

(ii) Addition law.

\[
 a < b \iff a + c < b + c. 
\]

(ii) Multiplication law.

\[
 a < b \iff ac < bc \quad \text{if } c > 0, \\
 a < b \iff ac > bc \quad \text{if } c < 0. 
\]

(ii) Transitive law.

\[
 a < b \text{ and } b < c \Rightarrow a < c. 
\]

Now we are able to write a formal proof of example 3.1.1.

**Proof.** Given positive real numbers \( a, b \) and suppose \( a < b \). Then by the multiplication law \( a^2 < ab \) (multiplying through by \( a > 0 \)) and \( ab < b^2 \) (multiplying through by \( b > 0 \)). By the transitive law \( a^2 < ab < b^2 \). Hence \( a < b \Rightarrow a^2 < b^2 \). \( \square \)
3.2 Constructing proofs backwards

Sometimes the problem would be much easier if we start with the conclusions instead of the assumptions.

Example 3.2.1. For real numbers \(a\) and \(b\) such that \(a < b\), show \(4ab < (a + b)^2\).

Actually the conclusion holds for all real \(a, b\) that are not equal.
Let us construct a proof backwards:

\[
4ab < (a + b)^2 \iff 4ab < a^2 + 2ab + b^2 \\
\iff 0 < a^2 - 2ab + b^2 \\
\iff 0 < (a - b)^2 \\
\iff a \neq b \quad \text{(think about why?)} \\
\iff a < b.
\]

Hence \(a < b \implies 4ab < (a + b)^2\). With this backwards proof, if we write it backward, we get a direct proof:

Proof. \(a < b \implies a \neq b \implies (a - b)^2 > 0 \implies 0 < a^2 - 2ab + b^2 \implies 4ab < a^2 + 2ab + b^2 \implies 4ab < (a + b)^2\). \(\square\)

4 Proof by contradiction

In the previous section we construct some simple direct proofs. Here we introduce a different idea of proof: proof by contradiction.

4.1 Proving negative statements by contradiction

Let us explain the idea through the following example:

Example 4.1.1. There do not exist integers \(m, n\) such that

\[
14m + 20n = 101. \quad (1)
\]

Idea: The problem is: known that \(m, n\) are integers, and the goal is to show that \(14m + 20n \neq 101\).

The proof by contradiction method is, instead of starting from what is known, we start with assuming that the goal is incorrect. So in this example, we assume that \(14m + 20n = 101\) and \(m, n\) are integers. And the goal is to show that this is impossible i.e. contraction.

This would be easier to argue. Because, when \(m, n\) are integers, \(14m + 20n\) is an integer and furthermore it equals \(2(7m + 10n)\) which is an even number. While 101 is odd, we obtain a contraction. This contraction indicates that the original statement (1) is true. \(\square\)

Now we consider a harder problem:
Example 4.1.2. Let $n$ be a positive integer. Then $4n + 3$ cannot be one positive integer’s square.

Proof. Suppose for contradiction that there exist a positive integer $n$ such that $4n + 3 = m^2$ for some positive integer $m$.

Since $m$ is a positive integer, it is either odd or even. If it is even, we can suppose $m = 2k$ for some positive integer $k$. Then $m^2 = 4k^2$ is even. However $4n + 3$ is odd, $m^2 = 4n + 3$ is not possible.

Now if $m$ is odd, suppose $m = 2k + 1$. Then $m^2 = (2k + 1)^2 = 4k^2 + 4k + 1$ and thus the remainder of dividing $m^2$ by 4 equals 1. However the remainder of dividing $4n + 3$ by 4 equals 3. Therefore $m^2$ cannot equal $4n + 3$. We get a contradiction.

In all $4n + 3$ cannot be one positive integer’s square.

A template for proofs by contradiction. To show $P \implies Q$.

Proof. Suppose, for contradiction, that the statement $Q$ is false. Then [present argument which leads to a contradiction]. Hence our assumption that $Q$ is false must be false. Thus $Q$ is true as required.

4.2 Proving implications by contradiction

Example 4.2.1. If $a, b, c$ are integers such that $a > b$, then

$$ac \leq bc \implies c \leq 0.$$ 

We are going to use the Multiplication law:

$$a < b \iff ac < bc \quad \text{if } c > 0,$$

However it is difficult to make use of the multiplicative law of inequalities in a direct proof. The easiest thing to do in this case is again a proof by contradiction.

Proof. For integers $a, b, c$ with $a > b$, suppose that $ac \leq bc$ but, for contradiction, that $c > 0$. Then the given statement $a > b$ implies that $ac > bc$ by the multiplicative law. However this contradicts with the statement that $ac \leq bc$. Hence the assumption that $c > 0$ must be false. Thus $ac \leq bc \implies c \leq 0$.

4.3 Proof by contrapositive

Theorem 4.1. Let $P, Q$ be two statements. Then $P \implies Q$ is equivalent to $(\neg Q) \implies (\neg P)$.

Can you prove the theorem?

A proof by contrapositive is to use the theorem and so that we show $(\neg Q) \implies (\neg P)$ to conclude with $P \implies Q$.

Let us again consider Example (4.2.1).
Proof. (of Example (4.2.1)) The contrapositive of the statement
\[ ac \leq bc \implies c \leq 0 \]
is the statement
\[ c > 0 \implies ac > bc \]
which is exactly the multiplicative law. Thus the proposition of Example (4.2.1) is true.

### 4.4 Proving “or” statements

In this subsection we constructing a proof for composite statements involving “or”.

**Example 4.4.1.** If \( a \) and \( b \) are real numbers, then

\[ ab = 0 \iff a = 0 \text{ or } b = 0. \]

Before the proof, let us analyze the statement. We are asked to prove a statement of the form \( P \iff Q \). Then we are required to give two parts of proofs: \( P \implies Q \) and \( P \iff Q \).

**Proof.** “ \( \implies \)”: Known \( ab = 0 \) and the goal is to show that \( a \) or \( b \) equals 0. If \( a = 0 \), the conclusion holds. Otherwise suppose \( a \neq 0 \). Then dividing \( ab = 0 \) through by \( a \) gives \( b = 0 \), as required. Hence \( ab = 0 \implies a = 0 \text{ or } b = 0. \)

“\( \iff \)”: If one of \( a, b \) equals 0, then it is a basic property of 0 that \( ab = 0 \). The conclusion holds.

Actually we can discuss by cases for \( a, b \). There are three possibility for \( a \) (\( b \)): \( a < 0 \) or \( a = 0 \) or \( a > 0 \) (\( b < 0 \) or \( b = 0 \) or \( b > 0 \)). Discussing by cases leads to nine possibilities in all.

<table>
<thead>
<tr>
<th>a&lt;0</th>
<th>a=0</th>
<th>a&gt;0</th>
</tr>
</thead>
<tbody>
<tr>
<td>b&lt;0</td>
<td>ab&gt;0</td>
<td>ab&lt;0</td>
</tr>
<tr>
<td>b=0</td>
<td>ab=0</td>
<td>ab=0</td>
</tr>
<tr>
<td>b&gt;0</td>
<td>ab&lt;0</td>
<td>ab=0</td>
</tr>
</tbody>
</table>

### 5 The induction principle

The induction principle is a special proof technique which is particularly useful when proving statements about the positive integers.

Suppose we wish to prove some property for all the positive integers: 1, 2, 3, 4... That is we want to prove infinitely many statements labeled by \( n \). Suppose the statement involving positive integer \( n \) is \( P(n) \).

**Axiom 5.1. (The induction principle)** \( P(n) \) is true for all \( n = 1, 2, 3, \ldots \) if

(i) \( P(1) \) is true, and
(ii) $P(k) \implies P(k + 1)$ for all positive integers $k$.

**Remark 5.1.** (i) is often referred to as the base case. In (ii), we assume $P(k)$ and the goal is to prove $P(k + 1)$. The assumption $P(k)$ is called the inductive hypothesis.

**Example 5.0.1.** For all positive integers $n$ we have $n \leq 2^n$.

**Proof.** We use induction on $n$ using the Axiom 5.1.

Base case: For $n = 1$, since $n = 1 \leq 2 = 2^n$, then $n \leq 2^n$.

Inductive step: Suppose now as inductive hypothesis that $k \leq 2^k$ for a positive integer $k$. Then

$$2^{k+1} = 2 \times 2^k \geq 2k \geq k + 1.$$ 

So $k + 1 \leq 2^{k+1}$ as required.

Conclusion: Hence, by induction, $n \leq 2^n$ holds for all positive integer $n$. □

**Example 5.0.2.** For all positive integers $n$, the number $n^2 + n$ is even.

**Proof.** We use induction on $n$. (Base case) For $n = 1$, $n^2 + n = 1 + 1 = 2$ which is even as required. (Inductive step) Now suppose $n^2 + n$ is even for $n = k$ for some positive integer $k$. Then we have

$$k^2 + k = 2q \quad \text{for some positive integer } q.$$ 

For $n = k + 1$,

$$(k + 1)^2 + (k + 1) = k^2 + 2k + 1 + k + 1 = (k^2 + k) + 2(k + 1) = 2q + 2(k + 1)$$

which is again even. (Conclusion) Hence, by induction, $n^2 + n$ is even for all positive integers $n$. □

### 5.1 Changing the base case

**Example 5.1.1.** For all integers $n$ such that $n \geq 4$, we have the inequality $n^2 \leq 2^n$.

**Solution.** We use induction on $n$ starting with $n = 4$. (Base case) For $n = 4$, $n^2 = 16 = 2^4$ and so $n^2 \leq 2^n$.

(Inductive step) Suppose now as inductive hypothesis that $k^2 \leq 2^k$ for some $k \geq 4$. Then

$$2^{k+1} \geq 2k^2.$$ 

So we will have proved that $2^{k+1} \geq (k + 1)^2$ if we can show that $2k^2 \geq (k + 1)^2$. Notice

$$2k^2 - (k + 1)^2 = 2k^2 - k^2 - 2k - 1 = k^2 - 2k - 1 = k(k - 2) - 1 \geq 0$$

when $k \geq 4$. Therefore we proved $2^{k+1} \geq (k + 1)^2$ to complete the inductive step.

(Conclusion) Hence, by induction, $n^2 \leq 2^n$ for all $n \geq 4$. □
5.2 Definition by induction

Suppose given a sequence of numbers $a_1, a_2, \ldots$, recall the summation notation: $\sum_{i=1}^{n} a_i$ for positive integers $n$. We can interpret the summation notation as a definition by induction:

(i) For $n = 1$, $\sum_{i=1}^{1} a_i$ is defined as $a_1$;

(ii) (Suppose $\sum_{i=1}^{k} a_i$ is defined.) For $n = k + 1$, $\sum_{i=1}^{k+1} a_i = (\sum_{i=1}^{k} a_i) + a_{k+1}$.

Example 5.2.1. For positive integers $n$, show

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

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

Proof. Let me only prove the first equality here.

We use induction on $n$. (Base case) For $n = 1$, $\sum_{i=1}^{1} i = 1$ and $\frac{1}{2} n(n + 1) = \frac{1}{2} \times 1 \times 2 = 1$ and therefore the equality holds for $n = 1$.

(Inductive step) Suppose as inductive hypothesis that $\sum_{i=1}^{k} i = \frac{1}{2} k(k + 1)$ for some positive integer $k$. Then

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k + 1) \quad \text{(by definition of summation notation)}$$

$$= \frac{1}{2} k(k + 1) \quad \text{(by inductive hypothesis)}$$

$$= \frac{1}{2} (k + 1)(k + 2) \quad \text{(by direct computations)}$$

and so

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

as required.

(Conclusion) Hence, by induction, $\sum_{i=1}^{n} i = \frac{1}{2} n(n + 1)$ holds for all positive integer $n$. 

Another example is the factorial $n$.

Definition 5.2. For non-negative integers $n$, the number factorial $n$ written $n!$, are defined inductively by

(i) $0! = 1$; and

(ii) $(k + 1)! = k! \times (k + 1)$ for all non-negative integer $k$. 


5.3 The strong induction principle

Axiom 5.2. (The strong induction principle) Suppose that \( P(n) \) is a statement involving a general positive integer \( n \). Then \( P(n) \) is true for all positive integers \( n \) if

1. \( P(1) \) is true, and
2. \[ P(n) \] holds for all positive integers \( n \leq k \) \( \implies P(k+1), \) for all positive integers \( k \).

In this case, the basic template is as follows.

Proof. We use (strong) induction on \( n \).

(Base case) \[ \text{Prove the statement } P(1). \]

(Inductive step) Suppose now as inductive hypothesis that \( P(n) \) is true for all positive integers \( n \leq k \) for some positive integer \( k \). Then \[ \text{deduce that } P(k+1) \text{ is true}. \] This proves the inductive step.

(Conclusion) Hence, by induction, \[ P(n) \text{ is true for all positive integers } n. \]

As an illustration of the use of this form of induction we introduce the Fibonacci numbers.

Definition 5.3. For each positive integer \( n \) define the number \( F_n \) inductively as follows.

\[
F_1 = 1, \quad F_2 = 1, \\
F_{k+1} = F_k + F_{k-1} \quad \text{for } k \geq 2.
\]

In this way, we defined a sequence of numbers. The beginning of this sequence is

\[ 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots, \]

and the sequence is known as the Fibonacci sequence.

Proposition 5.4. The Fibonacci numbers are given by the following formula:

\[
F_n = (\alpha^n - \beta^n)/\sqrt{5}
\]

where \( \alpha, \beta = (1 \pm \sqrt{5})/2. \)

Remark 5.5. Here \( \alpha, \beta \) are the roots of

\[ x^2 - x - 1 = 0. \]

It is surprising here that these integers \( F_n \) involves \( \sqrt{5} \) which is not an integer (which is not even a rational number). Actually we will see later that there is a general procedure for finding a general formula for sequences defined inductively in this way.
Proof. (Base case) For \( n = 1 \), the formula gives \((\alpha - \beta)/\sqrt{5} = 1 = F_1\). Since the inductive formula does not apply until \( F_3 \), we have to calculate \( F_3 \). For \( n = 2 \), the formula gives \((\alpha^2 - \beta^2)/\sqrt{5}\). Using that \( \alpha^2 = \alpha + 1 \), \( \beta^2 = \beta + 1 \), we get
\[
(\alpha^2 - \beta^2)/\sqrt{5} = 1 = F_2.
\]

(Inductive step) Now suppose as inductive hypothesis that the formula holds for all positive integers \( n \) such that \( n \leq k \) for some positive integer \( k \geq 2 \). Then
\[
F_{k+1} = F_k + F_{k-1} \quad \text{(by definition of the sequence)}
\]
\[
= ((\alpha^k - \beta^k) + (\alpha^{k-1} - \beta^{k-1}))/\sqrt{5} \quad \text{(by inductive hypothesis)}
\]
\[
= ((\alpha^{k-1}(\alpha + 1) - \beta^{k-1}(\beta + 1))/\sqrt{5}
\]
\[
= (\alpha^{k+1} - \beta^{k+1}))/\sqrt{5} \quad \text{(using } \alpha^2 = \alpha + 1 \), \( \beta^2 = \beta + 1 \)
\]
as required to prove the formula for \( n = k + 1 \).

(Conclusion) Hence, by induction, the formula holds for all positive integers. \( \square \)

6 The language of set theory

The language of set theory is used throughout mathematics. For example, real numbers, integers etc. are sets of numbers.

We usually use the following symbols:

- \( \mathbb{Z} \) : the set of all integers;
- \( \mathbb{Z}^+ \) : the set of all positive integers;
- \( \mathbb{Z}^{\geq} \) : the set of all non-negative integers (same as \( \mathbb{N} \), the natural numbers);
- \( \mathbb{Q} \) : the set of all rational numbers;
- \( \mathbb{R} \) : the set of all real numbers;
- \( \mathbb{C} \) : the set of all complex numbers.

6.1 Sets

More generally, a set is defined as a collection of objects (not necessarily numbers). The objects in a set are called the elements, members or points of the set. We write
\[
x \in A
\]
to denote that \( x \) is an element of the set \( A \). Here \( x \) can be a number, a ball, a space or an apple etc. The negation of the statement \( x \in A \) is written \( x \notin A \). For example \( \sqrt{2} \notin \mathbb{Q} \).

If only talking about a set of elements, we DO NOT consider any order of elements in a set; we DO NOT repeat the same element for more than one times in one set.

There are three ways to specify a set:
- **List the elements.** E.g. \( A = \{1, 3, \pi, -14, "banana"\} \).
- **Conditional definition.** E.g. \( B = \{n \in \mathbb{Z} \mid 0 < n < 6\} \).
- **Constructive definition** by giving a formula of elements. E.g. \( \{n^2 \mid n \in \mathbb{Z}\}, \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\} \) (this is the same as \( \mathbb{Q} \)). The two set examples here contains infinitely many elements.

**Definition 6.1. Equality of sets.** Two set \( A, B \) are equal, written \( A = B \), if they have precisely the same elements, i.e. \( A = B \) means \( x \in A \iff x \in B \).

**Example 6.1.1.**

\[
\{x \in \mathbb{R} \mid x^2 - x - 2 = 0\} = \{-1, 2\} = \{2, -1\} = \{-1, -1, 2\}.
\]

**Definition 6.2.** The empty set is the unique set which has no element at all, denoted as \( \emptyset \).

**Definition 6.3.** Given sets \( A, B \), we say that \( A \) is a subset of \( B \), written \( A \subseteq B \), when every element of \( A \) is an element of \( B \), i.e. \( x \in A \implies x \in B \). If in addition \( A \neq B \), then we say that \( A \) is a proper subset of \( B \) and write \( A \subset B \).

**Remark 6.4.** It can be shown that

\[
A = B \iff A \subseteq B \text{ and } B \subseteq A.
\]

Next \( \in \) and \( \subseteq \) have very different meaning. For example \( a \in A \) means that \( a \) is an element of \( A \). While for \( B \subseteq A \), \( B \) is a set, but just smaller. We can write

\[
a \in A \iff \{a\} \subseteq A,
\]

here \( \{a\} \) is viewed as a set which contains a single element.

### 6.2 Operations on sets

Given two sets \( A, B \).

**Definition 6.5.** The intersection of \( A \) and \( B \) is denoted by \( A \cap B \). We have

\[
A \cap B = \{x \mid x \in A \text{ and } x \in B\}.
\]

\( A \) and \( B \) are said to be disjoint if \( A \cap B = \emptyset \).

The union of \( A \) and \( B \) is denoted by \( A \cup B \). We have

\[
A \cup B = \{x \mid x \in A \text{ or } B\}.
\]

We can also form a set of elements which lie in \( A \) but not \( B \). This is called the difference of \( A \) and \( B \), denoted as \( A - B \). Thus

\[
A - B = \{x \mid x \in A \text{ and } x \notin B\}.
\]

We call use Venn diagram to illustrate the above operations. See page 68 of the textbook.

**Example 6.2.1.** Given any two sets \( A \) and \( B \), the three sets \( A \cap B \), \( A - B \) and \( B - A \) are pairwise disjoint (i.e. each pair of these sets is disjoint) and

\[
A \cup B = (A \cap B) \cup (A - B) \cup (B - A).
\]
6.3 The power set

The power set is a more complected of constructing one set from one set.

**Definition 6.6.** The *power set* of a set $X$ is defined as the set of all subsets of the set $X$, denoted as $\mathcal{P}(X)$.

Thus $A \in \mathcal{P}(X)$ is an alternative way of writing $A \subseteq X$.

We have

$$\emptyset \in \mathcal{P}(X), \quad \text{and} \quad X \in \mathcal{P}(X).$$

**Example 6.3.1.** If $X = \{a, b\}$, then

$$\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$

It is often the case that all the sets we are considering are subsets of a fixed set. We refer to this largest set as the *universal set*.

**Definition 6.7.** Suppose $U$ is a universal set and $A \subseteq U$. Then the complement of $A$ in $U$ is defined as

$$A^c := U - A.$$

Here we can also write $A, A^c \in \mathcal{P}(U)$.

**Theorem 6.8.** Let $A, B, C$ be subsets of a set $U$. Then the following identities hold:

(i) **Associativity:**

$$A \cup (B \cup C) = (A \cup B) \cup C, \quad A \cap (B \cap C) = (A \cap B) \cap C.$$

(ii) **Commutativity:**

$$A \cup B = B \cup A, \quad A \cap B = B \cap A.$$

(iii) **Distributivity:**

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

(iv) **De Morgan laws:**

$$\left((A \cup B)^c\right) = A^c \cap B^c, \quad \left((A \cap B)^c\right) = A^c \cup B^c.$$

(v) **Complementation:**

$$A \cup A^c = U, \quad A \cap A^c = \emptyset.$$

(vi) **Double complement:**

$$\left((A^c)^c\right) = A.$$

14
Proof. (of \((A \cup B)^c = A^c \cap B^c\). In the textbook one of the distributive law is proved. Please read it.)

Proof of "\(\subseteq\)": Suppose \(x \in (A \cup B)^c\). Then \(x \notin (A \cup B)\) and so \(x \notin A\) and \(x \notin B\). \(x \notin A\) implies that \(x \in A^c\) and \(x \notin B\) implies that \(x \in B^c\). Therefore we get \(x \in A^c \cap B^c\).

Proof of "\(\supseteq\)": Suppose \(x \in A^c \cap B^c\). Then \(x \in A^c\) and \(x \in B^c\). We get \(x \notin A\) and \(x \notin B\), and so \(x \notin A \cup B\) which implies that \(x \in (A \cup B)^c\).

\[\square\]

Proposition 6.9. Show

\[(A \cup B) \cap (C \cup D) = (A \cap C) \cup (A \cap D) \cup (B \cap C) \cup (B \cap D).\]

Proof. Here we are asked to prove an equality. This is unlike the "equivalence \(\iff\)": we do not have to prove "\(=\)" from two directions.

First let us view \(A \cup B\) as one single set and apply the distributivity law:

\[(A \cup B) \cap (C \cup D) = ((A \cup B) \cap C) \cup ((A \cup B) \cap D).\]

By distributivity again

\[((A \cup B) \cap C) = (A \cap C) \cup (B \cap C),\]

\[((A \cup B) \cap D) = (A \cap D) \cup (B \cap D).\]

The associativity of the union operation implies that

\[(A \cup B) \cap (C \cup D) = (A \cap C) \cup (B \cap C) \cup (A \cap D) \cup (B \cap D)\]

\[= (A \cap C) \cup (A \cap D) \cup (B \cap C) \cup (B \cap D).\]

\[\square\]

7 Quantifies

In this section we consider a set of statements \(P(a)\) with a single free variable \(a\) taking values in a set \(A\). Recall that \(P(a)\) is called a predicate. The statement that all predicates \(P(a)\) for \(a \in A\) are true is called a universal statement.

Next we introduce two notations:

Definition 7.1. The notation \(\forall a \in A, P(a)\) means: for each (or for any, for all) \(a \in A\), \(P(a)\) is true. (\(\forall\) is called the universal quantifier symbol.)

The notation \(\exists a \in A, P(a)\) means there exists (at least) one \(a \in A\) such that \(P(a)\) is true. (\(\exists\) is called the existential quantifier symbol. It reads: “there exists”, “for some” etc.)
7.1 Proving statements involving quantifiers

Example 7.1.1. Prove \( \exists n \in \mathbb{Z}^+, 2n + 1 \) is a prime number.

Proof. Let \( n = 3 \) and then \( n \in \mathbb{Z}^+ \). We find that \( 2n + 1 = 7 \) is a prime number.

Example 7.1.2. For integers \( n \), if \( n \) is even then \( n^2 \) is even.

This is a universal implication: \( \forall n \in \mathbb{Z} \) etc. The hypothesis that \( n \) is even is an existence statement, because \( n \) is even is the same as \( \exists q \in \mathbb{Z} \) such that \( n = 2q \).

Proof. Since \( n \) is even, \( \exists q \in \mathbb{Z} \) such that \( n = 2q \). Then \( n^2 = (2q)^2 = 2(2q^2) \) which is again even.

Example 7.1.3. To disprove the statement \( \forall x \in \mathbb{R}, x \leq 10^{10} \).

Proof. Let \( x = 10^{10} + 1 \). Then \( x \in \mathbb{R} \) and \( x > 10^{10} \).

Here in the example, we are asked to prove:

\[ \exists a \in A, \text{ not } P(a). \]

We gave a counterexample as a proof. This is often called disproof by counterexample to \( P(a) \).

7.2 Predicates involving more than one variable

Let \( P(a, b) \) be a predicate involving two free variables \( a \in A, b \in B \). Then there are several ways to form a proposition.

Example 7.2.1. \( \forall a, b \in \mathbb{R}^+, a < b \implies a^2 < b^2 \).

Example 7.2.2. It is not true that \( \exists m, n \in \mathbb{Z}, 14m + 20n = 9 \).

Here in the examples, “\( \forall a, b \in A \)” is a shorthand for “\( \forall a \in A, \forall b \in A \)” and similarly for “\( \exists \)”.

Statements might also involve both quantifiers:

Example 7.2.3. \( \forall \epsilon \in \mathbb{R}^+, \exists N \in \mathbb{R}^+ \) such that \( \frac{1}{N} < \epsilon \).

Proof. Given any \( \epsilon > 0 \), we can pick \( N = \frac{1}{\epsilon} + 1 \). Then

\[ \frac{1}{N} = \frac{1}{\frac{1}{\epsilon} + 1} = \frac{\epsilon}{1 + \epsilon} < \epsilon. \]

Example 7.2.4. \( \exists N > 0, \forall \epsilon \in \mathbb{R}^+, N > \frac{2 + \epsilon}{1 + \epsilon} \).
Proof. Let us pick \( N = 2 \). Then

\[
2 > \frac{2 + \epsilon}{1 + \epsilon}
\]

is true because it is equivalent to

\[
2(1 + \epsilon) > 2 + \epsilon \iff \epsilon > 0.
\]

Use quantifiers to define limit.

Definition 7.2. Let \( \{a_n, n \in \mathbb{Z}^+\} \) be a sequence of real numbers. Then \( \lim_{n \to \infty} a_n = c \) if and only if

\[
\forall \epsilon > 0, \exists N \in \mathbb{Z}^+ \text{ such that } \forall n \geq N, \quad |a_n - c| \leq \epsilon.
\]

7.3 Cartesian product of two sets

Cartesian is one way to construct a set from two set.

Definition 7.3. Given sets \( X, Y \), the Cartesian product of \( X, Y \), denoted by \( X \times Y \), is the set of all ordered pairs \( (x, y) \) where \( x \in X \) and \( y \in Y \). Thus

\[
X \times Y = \{(x, y) \mid x \in X \text{ and } y \in Y\}.
\]

We say that the ordered pair \( (x, y) \) has coordinates \( x \) and \( y \).

Example 7.3.1. \( \mathbb{R}^2 = \mathbb{R} \times \mathbb{R} \) is the familiar 2-dimensional Euclidean plane. 
\( \mathbb{R}^d = \mathbb{R} \times \mathbb{R} \times \ldots \times \mathbb{R} \) is the \( d \)-dimensional Euclidean plane.

Proposition 7.4. For all sets \( A, B, C \) and \( D \) the following hold:

(i) \( A \times (B \cup C) = (A \times C) \cup (A \times C) \);
(ii) \( A \times (B \cap C) = (A \times C) \cap (A \times C) \);
(iii) \( (A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D) \);
(iv) \( (A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D) \).

Proof. (of part (iii), the textbook proved (ii).) A proof that two sets are equal requires us to prove two inclusions. In this case we can do them together as follows.

\[
(x, y) \in (A \times B) \cap (C \times D) \iff (x, y) \in (A \times B) \text{ and } (x, y) \in (C \times D)
\]

\[
\iff x \in A, y \in B \text{ and } x \in C, y \in D
\]

\[
\iff x \in A \cap C \text{ and } y \in B \cap D
\]

\[
\iff (x, y) \in (A \cap C) \times (B \cap D).
\]
8 Functions