CHAPTER 1

Logic and Proofs

1.1 THE LANGUAGE OF MATHEMATICS

Mathematics makes precise use of language in stating and proving its results. Mathematicians use the English (or other) language to express their ideas and arguments, though they give some common English words a more precise meaning, so as to make them unambiguous.

Your aim in writing mathematics should be to convince the reader (and yourself) that your ideas are correct. Good mathematical writing consists of complete sentences, allowing for the fact that symbols stand for words. For example, "$A = B$." is a sentence in which the subject is "A", the verb is *equals* and the object is "B".

Symbols are supposed to make the mathematics easier to comprehend, not to confuse the reader, so do not go overboard in using a multitude of nonstandard symbols. The standard symbols that we use in this book are listed in the List of Symbols on page 293. Nonmathematical readers may be baffled by pages of mathematics full of symbols, but writing it out without symbols would not make it any clearer to them.

Mathematicians use a variety of terms to label their results. We shall use the terms **theorem**, **proposition**, and **lemma** to describe results, in decreasing order of importance. These will be general statements that usually apply to a large number of cases. A *theorem* will be a major landmark in the mathematical theory, a *proposition* a lesser result, while a *lemma* will usually be a result that is needed to prove a theorem or proposition but is not very interesting on its own. A **corollary** is a result that follows almost immediately from a theorem. An **example** is not normally a general result, but often a particular case of a theorem or proposition. An **algorithm** is an explicit procedure for solving a problem in a finite number of steps.

A **definition** gives a precise meaning to a mathematical term so that the reader knows what the author intends. A given definition may not be the one you would use, but you have to accept it to make sense of the following mathematics. For example, some people would define the natural numbers as the positive integers 1, 2, 3,..., while others think that zero is natural, and would define the natural numbers as the nonnegative integers 0, 1, 2, 3,....

A **proof** is a mathematical argument intended to convince us that a result is correct. A proof of a theorem, or other result, is a series of logical deductions, using the assumptions of the theorem, the definitions of the terms involved, and previous

results that have been proven. You have to use your judgment when writing a proof on how much detail to include, and this will depend on your audience. If you put in too much detail, the overall argument will be cluttered. On the other hand, if you do not put in enough detail, your readers may not understand all your argument and, more important, you may omit some technicality that invalidates your proof. In this chapter, we introduce the more common types of mathematical reasoning used in proofs and the standard strategies for attacking proofs.

In mathematics, we tend to use more complicated, and more compound expressions than we do in everyday language, so the next section explains some methods for dealing with these expressions.

1.2 LOGIC

Logic is the study of correct reasoning. The rules of logic give precise meaning to mathematical statements and allow us to make correct arguments about these statements.

Definition. In mathematics, a **statement** or **proposition** is a sentence that is either TRUE or FALSE.

For example,

- The year 2000 is a leap year.
- $3 + 2 = 6$.
- $\pi^2 < 10$.
- The decimal expansion of π contains one hundred consecutive 3's.

They are sentences that are either TRUE or FALSE, though you most probably do not know the truth value of the last statement.

However, the following sentences are not statements.

- Let $x = 4$.
- Find the nearest integer to $\sqrt{5}^{13}$.
- Is it Friday today?

Questions are never statements. If we changed the last sentence to "It is Friday today" it would be a statement.

Propositional logic is the part of logic that deals with combining statements using connectives such as AND, OR, NOT, or implies. We use these connectives in everyday language, but in mathematics and computer science we tend to use them in more complex combinations. We (and the computers) need to know precisely what these combinations mean.

We can always combine any two statements using AND or OR to form a third statement. For example,

- Ottawa is the capital of Canada and New York is the capital of the United States.

If P denotes the statement "Ottawa is the capital of Canada" and Q denotes the statement "New York is the capital of the United States" then the preceding statement could be denoted by P AND Q.

Every statement has a negation. For example, if P is the statement "$3+2=6$" then its negation is "It is not true that $3+2=6$" or more simply "$3+2 \neq 6$."

Definition. Let P and Q be statements. The statement P **AND** Q is called the **conjunction** of P and Q. The statement P AND Q will be TRUE if P is TRUE and Q is TRUE but will be FALSE otherwise.

The statement P **OR** Q is called the **disjunction** of P and Q. The statement P OR Q will be TRUE if either P is TRUE, or Q is TRUE, or both are TRUE.

The **negation** of the statement P is denoted by **NOT** P. Another very common notation is $\sim P$.

We can define these connectives by the following truth tables, in which T stands for TRUE and F stands for FALSE.

P	Q	P AND Q
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	P OR Q
T	T	T
T	F	T
F	T	T
F	F	F

P	NOT P
T	F
F	T

A *truth table* for a statement containing unknowns lists the truth values of the statement for all possible truth values of the unknowns. Since each statement has two possible values, T or F, the number of possibilities for n independent unknown statements is 2^n, and this will be the number of rows (not counting the headings) in the truth table of a statement with n unknowns. The statement P AND Q has the two unknowns P and Q, so the truth table will have four rows, while the truth table for NOT P has two rows.

In everyday language, the word *or* can be used in two different ways. Consider the meaning of *or* in the following two sentences.

- The prerequisite for this course is algebra or trigonometry.
- You will be served tea or coffee.

In the first sentence, the *or* is used in an inclusive way, which means that you can still take the course if you have both algebra and trigonometry. However, in the second sentence, *or* is used in an exclusive way; you should not expect tea *and* coffee. Mathematics always uses the *inclusive* OR, which means that P OR Q is true even if both P and Q are true.

Example 1.21. Show that the statement NOT (P AND Q) has the same truth table as the statement (NOT P) OR (NOT Q).

Solution.

P	Q	P AND Q	NOT (P AND Q)
T	T	T	F
T	F	F	T
F	T	F	T
F	F	F	T

P	Q	NOT P	NOT Q	(NOT P) OR (NOT Q)
T	T	F	F	F
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

The two final columns are the same, so the two statements have the same truth table. □

The symbol □ denotes the end of a proof or solution.

The negation of a conjunction in the previous example can be illustrated in everyday language. Consider the statement "It is not true that it is raining and windy." This means that "Either it is not raining or it is not windy." Notice that we are using the mathematical *inclusive or* here; it could be sunny and calm.

In a similar way, you are asked to show in Exercise 22 that NOT (P OR Q) and (NOT P) AND (NOT Q) have the same truth tables.

In mathematics, we often use statements of the form "If P, then Q" such as "If an angle bisector of a triangle is also a median, then the triangle is isosceles." This is called a conditional statement or implication, where P is the *hypothesis* and Q is the *conclusion*.

If P is a true statement, then clearly the truth value of "If P then Q" should be the same as the truth value of Q. However, if P is false, it is not obvious what the truth value of the statement should be. For example, if pigs can fly then I will eat my hat. If P is false, then the statement "If P then Q" normally imparts no meaning in everyday language, though you would certainly not say that it is false. Since we would like "If P then Q" to be a mathematical statement that is either true or false, we define it to be true, whenever P is false. This yields the following definition.

Definition. Given two statements P and Q, the **conditional statement** "If P, then Q" is denoted by $P \Longrightarrow Q$ (pronounced "P implies Q") and is defined by the following truth table.

P	Q	$P \Longrightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

The conditional in mathematics is an extension of everyday usage, but it has some unusual consequences because $P \Longrightarrow Q$ is always true if P is false. For example, "If $5 > 7$, then $2+2 = 3$" is a true statement. When we use the conditional "If P, then Q" in everyday language we are usually suggesting that the truth of P *causes* Q to be true. In mathematics, there does not have to be any relation whatsoever between P and Q. However, this leads to logically correct but pretty useless statements, such as "If $2 < 4$, then $2+2 = 4$." One reason for not considering causality in the definition is that it would be very hard to make precise. "If you take this pill, you will get better." Is there a cause and effect here? Maybe, maybe not.

An implication in which the hypothesis is false is sometimes called **vacuously true**, because there is nothing to check. For example, "If x is an integer between 2.2 and 2.8, then x is even" is vacuously true, as there are no integers in that range.

The following are all alternative ways of expressing a conditional statement.

- $P \Longrightarrow Q$.
- P implies Q.
- If P, then Q.
- If P, Q.
- Q if P.
- P only if Q.
- P is sufficient for Q.
- Q is necessary for P.

The **converse** of the conditional statement "If P, then Q" is "If Q, then P." Of course, even if a statement is true, its converse does not have to be true. For example, "If a quadrilateral has its four sides equal, then it is a parallelogram" is true, but the converse "If a quadrilateral is a parallelogram, then it has its four sides equal" is false.

If the conditional statement "If P, then Q" and its converse "If Q, then P" are both true, then we say that "P if and only if Q." For example, if $xy = 0$ then $x = 0$ or $y = 0$. Also, if $x = 0$ or $y = 0$, then $xy = 0$. Hence

$$xy = 0 \quad \text{if and only if} \quad x = 0 \text{ or } y = 0.$$

The statement "$xy = 0$" is true if and only if the statement "$x = 0$ or $y = 0$" is true. The statements express the same idea in different words.

Example 1.22. Find the truth table for the statement

$$(P \Longrightarrow Q) \text{ AND } (Q \Longrightarrow P).$$

Solution.

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$(P \Rightarrow Q)$ AND $(Q \Rightarrow P)$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

We shall now use this for the truth table for the statement "P if and only if Q." □

Definition. Given two statements P and Q, we denote the statement "P **if and only if** Q" by $P \iff Q$, and define it by $(P \Rightarrow Q)$ AND $(Q \Rightarrow P)$. The truth table is given below.

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

The statement $P \iff Q$ is true precisely when P and Q have the same truth values, in which case we say that P and Q are **equivalent statements**. Hence equivalent statements have the same truth tables.

The expression "if and only if" is used so often in mathematics that it is often abbreviated as *iff*. The following are alternative ways of expressing an "if and only if" statement.

- $P \iff Q$.
- P if and only if Q.
- P iff Q.
- P is equivalent to Q.
- P is necessary and sufficient for Q.

Example 1.23. Show that the statement $P \Longrightarrow Q$ is equivalent to the statement Q OR NOT P.

Solution. Compare their truth tables.

P	Q	$P \Rightarrow Q$	NOT P	Q OR NOT P
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Since the statements $P \Longrightarrow Q$ and Q OR NOT P have the same truth tables, they are equivalent.

As an example, the statement "If I am late, then I am running" is equivalent to "Either I am running or I am not late." □

Example 1.24. Is the statement $R \Longrightarrow (P$ OR $Q)$ equivalent to the statement P OR (Q AND NOT R)?

Solution. Compare their truth tables.

P	Q	R	P OR Q	$R \Longrightarrow (P$ OR $Q)$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	T	T
F	T	T	T	T
F	T	F	T	T
F	F	T	F	F
F	F	F	F	T

P	Q	R	Q AND NOT R	P OR (Q AND NOT R)
T	T	T	F	T
T	T	F	T	T
T	F	T	F	T
T	F	F	F	T
F	T	T	F	F
F	T	F	T	T
F	F	T	F	F
F	F	F	F	F

Since the truth tables differ in two positions, the statements are not equivalent. They differ when P is false and both Q and R are true and also when all the variables are false. □

Alternative Notations for Connectives		
Connective	Propositional Logic	C and Java syntax
AND	$\wedge$	&&
OR	$\vee$	||
NOT	$\neg$ or $\sim$	!
$\Longrightarrow$	$\longrightarrow$	
$\Longleftrightarrow$	$\longleftrightarrow$	

1.3 SETS

Mathematics not only deals with individual objects, such as the integer 2007 or the number $\sqrt{3}$, but also with collections of objects, such as all the real numbers, or all the solutions to an equation. In mathematics, such a collection is called a set. We shall not give a rigorous definition of set, but we shall describe it.

A *set* is any well-defined collection of objects; the objects are called the *elements* or *members* of the set. If x is an element of the set S, we say x belongs to S and write

$$x \in S.$$

If y is not an element of S, we write $y \notin S$. The set of *real numbers* is denoted by the blackboard bold symbol $\mathbb{R}$, so "$\sqrt{3} \in \mathbb{R}$" is a true statement.

There are two basic ways of describing a set. One method is to list all its elements. For example, a set S whose elements are 2, 4, 6 and 8 can be written as

$$S = \{2,4,6,8\}.$$

In mathematics, a set is considered as an unordered collection, so this same set S could be written as $\{4,8,6,2\}$, or even $\{2,2,8,6,4\}$. We might write the set of letters of the alphabet as $\{A,B,C,\ldots,X,Y,Z\}$, where the three dots indicate that all the letters between C and X are also to be included. By abusing this notation, we write the set of *positive integers* (or *natural numbers*) as

$$\mathbb{P} = \{1,2,3,4,\ldots\}$$

and also the set of all *integers* as

$$\mathbb{Z} = \{\ldots,-2,-1,0,1,2,3,\ldots\}.$$

The set $\mathbb{Z}$ consists of the positive integers, zero, and the negative integers.

The other basic method of describing a set is by means of a rule. For example,

$$S = \{x \in \mathbb{R} \mid 1 < x < 2\}$$

is read as "S is the set of all real numbers x, such that x is greater than 1 and less than 2"; in other words, S is the set of real numbers lying between 1 and 2. Other variants of this notation for the same set are $\{x \in \mathbb{R} : 1 < x < 2\}$ and $\{x \mid x \in \mathbb{R} \text{ AND } 1 < x < 2\}$.

The set with no elements is called the *empty set* or *null set* and is denoted by the symbol $\emptyset$. There is only one empty set; for example, the set $\{x \in \mathbb{R} \mid x^2 < 0\}$ and the empty set of oranges are the same set.

If S and T are sets such that every element of S is also an element of T, then we say that S is *contained* in T or that S is a *subset* of T and write $S \subseteq T$ or $T \supseteq S$. For example, $\{2,7,5\} \subseteq \mathbb{P}$ but $\{-1,5,8\}$ is not a subset of $\mathbb{P}$ because $-1 \notin \mathbb{P}$. Two sets S and T are *equal* if $S \subseteq T$ and $T \subseteq S$.

The *intersection* of two sets S and T is the set $S \cap T$, consisting of all elements that are in both S and T; hence

$$S \cap T = \{x \mid x \in S \text{ AND } x \in T\}.$$

If $S \cap T = \emptyset$, then S and T are said to be *disjoint*. The *union* of the sets S and T is the set $S \cup T$, of all elements that are in either S or T (or both S and T). Hence

$$S \cup T = \{x \mid x \in S \text{ OR } x \in T\}.$$

The *Cartesian product*, or just the *product*, of two sets S and T is the set $S \times T$, of all ordered pairs (x,y), where $x \in S$ and $y \in T$; hence

$$S \times T = \{(x,y) \mid x \in S \text{ AND } y \in T\}.$$

For example, $\{a,b,c\} \times \{1,2\}$ is the six-element set

$$\{(a,1),\ (b,1),\ (c,1),\ (a,2),\ (b,2),\ (c,2)\}.$$

The product $\mathbb{R} \times \mathbb{R} = \{(x,y) \mid x,y \in \mathbb{R}\}$ consists of all the points in the plane.

1.4 QUANTIFIERS

In mathematics we constantly use sentences involving variables, such as "$x > 5$." However, until the value of x is specified, this sentence has no truth value. If we let $P(x)$ denote the sentence "$x > 5$" then $P(7)$ is a true statement while $P(0)$ is a false statement.

If $P(x)$ is a sentence depending on the variable x, we often want to say that $P(x)$ is true for all values of x or that $P(x)$ is true for at least one value of x. This can be done by adding quantifiers, which convert the sentence $P(x)$ into a statement that is either true or false.

Definition. The *universal quantification* of $P(x)$ is the statement

- $P(x)$ is true for all values of x

and is denoted by

- $\forall x, \quad P(x)$

where the symbol $\forall$ is called the **universal quantifier** and is pronounced "for all."

This statement $\forall x, \ P(x)$ can also be expressed in any of the following ways.

- For all x, $P(x)$.
- For every x, $P(x)$.
- For each x, $P(x)$.
- $P(x)$, for all x.

The values of x are assumed to lie in a particular set called the *universe of discourse*. For example, the universe of discourse may be the integers, or the real numbers, or the set of all people.

If we are dealing with the real numbers, the statement "$\forall x, \ x^2 > 0$" means that "For all real numbers x, $x^2 > 0$" which is a false statement. However the statement "$\forall x, x^2 \geq 0$" is true.

Definition. The *existential quantification* of $P(x)$ is the statement

- There exists an x for which $P(x)$ is true

and is denoted by

- $\exists x, \quad P(x)$

where the symbol $\exists$ is called the **existential quantifier** and is pronounced "there exists."

Again this is interpreted to mean that "There exists an x in the universe of discourse for which $P(x)$ is true." This statement $\exists x, \ P(x)$ could also be expressed in any of the following ways.

- There is an x for which $P(x)$.
- For some x, $P(x)$.
- $P(x)$, for some x.

For example, if the universe of discourse is the set of real numbers, then the factorization $x^3 - 1 = (x-1)(x^2+x+1)$ is true for all x. So

$$\forall x, \quad x^3 - 1 \;=\; (x-1)(x^2+x+1)$$

is a true statement. However the equation $x^2 + x - 6 = 0$ is true for only certain values of x, namely $x = 2$ and $x = -3$. Hence $\forall x,\ x^2 + x - 6 = 0$ is false, but $\exists x,\ x^2 + x - 6 = 0$ is true.

Example 1.41. Express the statement "Every real number has a real square root" as a logical expression using quantifiers.

Solution. If we assume that the universe of discourse is the set of real numbers, we can express this statement as

$$\forall a\, \exists x, \quad x^2 \;=\; a.$$

Note that this is just a statement. It does not have to be true; in fact it is not. □

Example 1.42. Express the statement "There is a real number between any two real numbers" as a logical expression using quantifiers.

Solution. Assume that the universe of discourse is the set of real numbers. Before we start to convert the statement to a logical expression, we have to decide how to interpret the English. Does *between* mean *strictly between* and does *two real numbers* mean *two distinct real numbers*?

If we assume that *between* means *strictly between* and we require the statement to be true, then we have to take distinct real numbers. We could write it in either of the following ways.

$$\forall y\, \forall z, \quad (y \neq z \Longrightarrow (\exists x,\ (y < x < z \text{ OR } z < x < y))).$$
$$\forall y\, \forall z, \quad (y < z \Longrightarrow (\exists x,\ y < x < z)).$$

If we assume that *between* could include equals, then we could write

$$\forall y\, \forall z, \quad \exists x,\ (y \leq x \leq z \text{ OR } z \leq x \leq y).$$ □

Proposition 1.43. *If S is any set and $\emptyset$ denotes the empty set, then $S \subseteq S$ and $\emptyset \subseteq S$. If A and B are sets, the inclusion relation $A \subseteq B$ can be expressed using a quantifier as*

$$\forall x, \quad (x \in A \Longrightarrow x \in B).$$

Proof. The statement $S \subseteq S$ is equivalent to $\forall x, (x \in S \implies x \in S)$. If $P(x)$ is the statement $x \in S$, then $P(x) \implies P(x)$ is true for all x. Hence $S \subseteq S$ is true.

The statement $\emptyset \subseteq S$ is equivalent to $\forall x, (x \in \emptyset \implies x \in S)$. Now $x \in \emptyset$ is false for all x. However, $P \implies Q$ is always true if P is false, so that the statement $\emptyset \subseteq S$ is true. □

Example 1.44. The *divisibility* relation $a|b$, which will be discussed in detail in Chapter 2, can be defined symbolically as

$$\exists q, \quad b = qa,$$

where the universe of discourse is the set of integers. Using this definition, determine whether (i) $0|3$ and (ii) $0|0$.

Solution. ***(i)*** $0|3$ is equivalent to $\exists q,\ 3 = q0$; that is, $\exists q,\ 3 = 0$. Since $3 = 0$ is always false, $0|3$ is not true.

(ii) $0|0$ is equivalent to $\exists q\ 0 = q0$; that is, $\exists q,\ 0 = 0$. Since $0 = 0$ is always true, we can choose q as any integer, and so $0|0$ is true. □

How do we negate quantifiers? For example, the statement "All Canadians speak French" is not true. However, we do not have to show that "All Canadians do not speak French" to show that the statement is false. We only have to show that "There exists a Canadian who does not speak French." Also, the statement "There exists a real solution to the equation $x^2 = -1$." is false. However, to show this, we have to show that "For all real x, $x^2 \neq -1$."

Consider the negation of the statement "Everyone has a calculator." It is "Not everyone has a calculator," which has the same meaning as "Someone does not have a calculator." On the other hand, the negation of the statement "Someone has a calculator" is "No one has a calculator," which has the same meaning as "Everyone does not have a calculator." These are examples of the following rules for negating quantifiers.

Quantifier Negation Rules 1.45.

$$\begin{array}{lll} \text{NOT } (\forall x,\ P(x)) & \textit{is equivalent to} & (\exists x,\ \text{NOT } P(x)). \\ \text{NOT } (\exists x,\ P(x)) & \textit{is equivalent to} & (\forall x,\ \text{NOT } P(x)). \end{array}$$

In general, two statements involving quantifiers will be *equivalent* if they have the same meaning. We cannot always use truth tables to check for equivalence or implications involving quantifiers, so at this stage we have to reason informally to check the equivalence or implication.

Example 1.46. If the universe of discourse is the integers, what does the following statement mean in English? How would you prove it true or false?

$$\exists x \, \forall y, \ \ (x \geq y).$$

Solution. The statement says that there is an integer that is greater than or equal to all integers. That is, the statement says that there is a largest integer.

This is false. To show that it is false, we have to prove that

$$\text{NOT } (\exists x \, \forall y, \ \ (x \geq y))$$

is true. This is equivalent to the following statements.

$$\forall x, \ \ \text{NOT } (\forall y, \ \ (x \geq y)).$$
$$\forall x \, \exists y, \ \ \text{NOT } (x \geq y).$$
$$\forall x \, \exists y, \ \ (x < y).$$

This last statement is true because, for every x, we can take $y = x + 1$. □

Mathematicians would not normally write out the proof in the above example this way, using logical symbols. They would write it out as in the example following the Proof by Contradiction Method 1.55 in the next section, where it is proved that there is no largest integer. This illustrates the fact that mathematics is normally easier to understand if words are used for quantifiers rather than symbols. Compare the following two ways of saying the same thing.

- $\exists x \, \forall y, \ \ (x \geq y)$.
- There is an integer that is greater than or equal to all integers.

The symbolic form is certainly more concise, but that does not necessarily make it easier to understand. Therefore, in later chapters, we shall not normally use quantifier symbols, but we shall write them out in English. However, some complicated manipulations of logical statements, such as finding the negation, may be easier to do using symbols.

Example 1.47. Determine whether each pair of statements are equivalent.

(i) $\forall x$, $(P(x)$ AND $Q(x))$. $(\forall x, \ P(x))$ AND $(\forall x, \ Q(x))$.

(ii) $\forall x$, $(P(x)$ OR $Q(x))$. $(\forall x, \ P(x))$ OR $(\forall x, \ Q(x))$.

Solution. (i) These statements are equivalent. Suppose $\forall x$, $(P(x)$ AND $Q(x))$ is true. Hence $\forall x$, $P(x)$ is true and $Q(x)$ is true. In particular, $(\forall x, \ P(x))$ is true. Similarly, $(\forall x, \ Q(x))$ is true. Therefore, $(\forall x, \ P(x))$ AND $(\forall x, \ Q(x))$ is true.

Now suppose $(\forall x, \ P(x))$ AND $(\forall x, \ Q(x))$ is true. If x is any element in the universe of discourse, then $P(x)$ is true and $Q(x)$ is true. Hence the statement $\forall x$, $(P(x)$ AND $Q(x))$ is true. We have shown that whenever one of the statements is true, then the other one is also true.

(ii) These statements are not always equivalent. We shall give a particular example in which they do not have the same meaning.

Let the universe of discourse be the set of real numbers. Let $P(x)$ be the expression $x \geq 0$ and $Q(x)$ be the expression $x < 0$. Then, for all real numbers x, ($P(x)$ OR $Q(x)$) is true. However, ($\forall x$, $P(x)$) is not true, and ($\forall x$, $Q(x)$) is not true, so ($\forall x$, $P(x)$) OR ($\forall x$, $Q(x)$) is not true. □

1.5 PROOFS

Why are mathematicians so fussy about proving their results? Besides wanting to be correct, mathematicians want to be able to rely on a result, so that they can build on it and use it for further theorems. It is not good enough if the result is correct 99.9% of the time. Mathematics is most probably the most cumulative of subjects; later work nearly always relies on previous theorems. If an earlier theorem was found to be incorrect, it may put any subsequent work in jeopardy.

There are many methods for proving theorems, propositions, and lemmas, but there is no procedure that will apply to all proofs. It is extremely difficult to get a computer to write a good proof. Proof writing is an art that requires much practice. There is a delicate balance between writing down too many details and leaving out logical steps that cannot easily be filled by the reader. Remember that a proof is designed to be read and understood by a human!

There are some standard strategies for attacking proofs, and we now introduce the most important of these. These methods of proof are not only important in mathematics but also in computer science, where for example they are used in software specification for verifying programs.

Many mathematical theorems can be expressed symbolically in the form

$$P \Longrightarrow Q.$$

The statement P is called the *assumption* or *hypothesis* of the theorem, and the statement Q is the *conclusion*. The assumption will consist of one or more statements, normally involving some variables. The theorem says that if the assumption is true, then the conclusion is true.

How do you go about thinking up ways to prove a result? In general, it takes time and practice before you are comfortable in being able to write out a proof. You should start out with simple proofs and build up to multistage proofs. If you cannot immediately see how to prove a result, here are some steps you should go though in tackling a proof.

- **Understand the definitions.** You should know the technical terms involved in the result; this may mean looking up the definition of some terminology with which you are not familiar.

- **Try examples.** Look at various concrete examples that satisfy the hypothesis in order to get a feel for the problem. These examples should convince you

that the result is true and may suggest a method of attack for the proof. If the problem involves sets, like the first proposition below, you might draw an appropriate Venn diagram, and if the problem involves functions, you might sketch some suitable graphs.

If you find an example that satisfies the hypothesis but does not satisfy the conclusion, then you have found a counterexample, and the result is false. We discuss counterexamples in the next section.

- **Try standard proof methods.** Try the various techniques in this section that are appropriate for the result you are trying to prove.

Direct Proof Method 1.51. *Proving* $P \Longrightarrow Q$

The direct method of proving $P \Longrightarrow Q$ is to assume that the hypothesis P is true, and use this to prove that the conclusion Q is true.

PROPOSITION. *If* $S \cap T = S$, *then* $S \subseteq T$.

Proof. Suppose that $S \cap T = S$. To prove that S is a subset of T, we need to prove that if $x \in S$, then $x \in T$.

Let $x \in S$, so that $x \in S \cap T$, since $S \cap T = S$. It follows from the definition of the intersection of sets that $x \in T$. It now follows from the definition of inclusion that $S \subseteq T$. □

If and Only If Proof Method 1.52. *Proving* $P \Longleftrightarrow Q$

This type of result can usually be recognized by the phrase "if and only if" or the phrase "necessary and sufficient." The result "P if and only if Q" can be split up into the two cases, the "only if" part $P \Longrightarrow Q$, and the "if" part $Q \Longrightarrow P$, and then each case can be proved separately.

PROPOSITION. $S \cap T = S \cup T$ *if and only if* $S = T$.

Proof. To prove $(S \cap T = S \cup T) \Longrightarrow (S = T)$, suppose $S \cap T = S \cup T$. If $x \in S$ then $x \in S \cup T$. Since $S \cap T = S \cup T$, $x \in S \cap T$, and hence $x \in T$. This proves that $S \subseteq T$. The problem is symmetric in S and T, since interchanging S and T leaves the problem unchanged. Hence a similar proof, with S and T interchanged, will show that $T \subseteq S$. Combining $S \subseteq T$ with $T \subseteq S$ shows that $S = T$.

The proof in the other direction of $(S = T) \Longrightarrow (S \cap T = S \cup T)$ is very easy. Is is often the case that one direction of an "if and only if" proof is simple. Suppose that $S = T$. Then $S \cap T = S \cap S = S$ and $S \cup T = S \cup S = S$, so $S \cap T = S \cup T$. □

The **contrapositive** of the general implication "If P, then Q" is the statement "If not Q, then not P." The Contrapositive Law will show that these statements are equivalent. For example, the contrapositive of the statement "If it rains, then I get wet." is the statement "If I am not wet, then it is not raining." These statements mean the same thing.

Contrapositive Law 1.53. *$P \Longrightarrow Q$ is equivalent to* NOT $Q \Longrightarrow$ NOT P.

Proof. Consider the truth tables.

P	Q	$P \Rightarrow Q$	NOT Q	NOT P	NOT $Q \Rightarrow$ NOT P
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

We see from the truth table that $P \Longrightarrow Q$ is equivalent to NOT $Q \Longrightarrow$ NOT P. □

Contrapositive Proof Method 1.54. *Proving $P \Longrightarrow Q$*

In this method, we prove the statement $P \Longrightarrow Q$ by proving its contrapositive NOT $Q \Longrightarrow$ NOT P.

PROPOSITION. *If x is a real number such that $x^3 + 7x^2 < 9$, then $x < 1.1$.*

Proof. The contrapositive of the statement that we have to prove is "If $x \geq 1.1$, then $x^3 + 7x^2 \geq 9$." Hence suppose that $x \geq 1.1$. In particular, x is positive, and so

$$x^3 + 7x^2 \geq 1.1^3 + 7(1.1)^2 = 1.331 + 8.47 = 9.801.$$

Therefore, by the Contrapositive Proof Method, the original result must be true. □

Proof by Contradiction Method 1.55.

In the proof technique called proof by contradiction we assume that the statement we want to prove is false and then show that this implies a contradiction.

For example, suppose we wanted to prove the statement Q. If we can show that NOT Q leads to a contradiction, then NOT Q must be false; that is, Q must be true.

PROPOSITION. *There is no largest integer.*

Proof. Suppose that n is the largest integer. Then $n + 1$ is also an integer, and it is larger than n. This contradicts our assumption that n was the largest integer. Hence there is no largest integer. □

PROPOSITION. *There is no real solution to* $x^2 - 6x + 10 = 0$.

Proof. Assume that the result is false; that is, assume that there is a real number x with $x^2 - 6x + 10 = 0$. Then, by completing the square, we can write this as

$$(x-3)^2 + 1 = 0.$$

However $(x-3)^2 \geq 0$ for any real number x, so the left side of this equation is greater than or equal to 1. This gives a contradiction. Hence the original statement is true. □

We could prove, in a similar way, that there is no real square root of -1. These are examples of nonexistence results, which are normally proved by contradiction.

Other good examples of proof by contradiction are Euclid's Theorem 2.52 on the existence of an infinite number of primes, and Theorem 5.21 on the irrationality of $\sqrt{2}$.

Proof Method 1.56. *Proving* $P \Longrightarrow (Q \text{ OR } R)$

The statement Q is either true or false. If Q is true then $(Q \text{ OR } R)$ is true, and $P \Longrightarrow (Q \text{ OR } R)$ is always true, regardless of the truth values of P and R. We therefore only have to prove the result when Q is false. The method of proof therefore consists of assuming that P is true and NOT Q is true and using these to prove that R is true. The statement $P \Longrightarrow (Q \text{ OR } R)$ is therefore equivalent to the statement

$$(P \text{ AND NOT } Q) \Longrightarrow R.$$

You are asked to verify this equivalence using truth tables in Problem 76.

PROPOSITION. *Let m and n be integers. If $m^3 + n^3$ is odd, then m is odd or n is odd.*

Proof. Suppose that $m^3 + n^3$ is odd and that m is not odd. Therefore, m is even and so m^3 will also be even. Hence $m^3 + n^3 - m^3 = n^3$ will be odd. The contrapositive of the true statement "if n is even, then n^3 is even" is the true statement "if n^3 is odd, then n is odd." Hence we have shown

$$(m^3 + n^3 \text{ is odd }) \text{ AND NOT } (m \text{ is odd }) \Longrightarrow (n \text{ is odd }).$$

This is equivalent to the statement that was to be proved, namely $(m^3 + n^3 \text{ is odd }) \Longrightarrow (m \text{ is odd }) \text{ OR } (n \text{ is odd })$. □

Another good example of this type of proof, which we shall meet later, is in Theorem 2.53, which states that whenever p is a prime number

$$p \text{ divides } ab \Longrightarrow (p \text{ divides } a) \text{ OR } (p \text{ divides } b).$$

Proof Method 1.57. *Proving* $(P \text{ OR } Q) \Longrightarrow R$

We have to assume that P OR Q is true and then prove R. Whenever P is true, then $(P$ OR $Q)$ is true, and so we have to prove $P \Longrightarrow R$. Similarly, we have to prove $Q \Longrightarrow R$. These two results are sufficient, and this proof method is equivalent to proving

$$(P \Longrightarrow R) \text{ AND } (Q \Longrightarrow R).$$

Therefore, we have to prove both of the separate statements $P \Longrightarrow R$ and $Q \Longrightarrow R$. Problem 77 asks you to verify this equivalence using truth tables.

THEOREM. *If x is a real number, then $(x-a)(x-b) = 0$ if and only if $x = a$ or $x = b$.*

Proof. We shall first prove $(x-a)(x-b) = 0 \Longrightarrow (x = a)$ OR $(x = b)$, using Proof Method 1.56.

Suppose that $x \neq a$ and that $(x-a)(x-b) = 0$. Then $(x-a) \neq 0$ and we can divide by $(x-a)$ to obtain $(x-b) = 0$ and $x = b$.

Hence $(x-a)(x-b) = 0$ implies $x = a$ or $x = b$.

We shall now prove $(x = a)$ OR $(x = b) \Longrightarrow (x-a)(x-b) = 0$, using Proof Method 1.57.

Suppose $x = a$. Then $x - a = 0$ and so $(x-a)(x-b) = 0$. Similarly, if $x = b$ then $(x-a)(x-b) = 0$.

Hence $x = a$ or $x = b$ implies $(x-a)(x-b) = 0$. □

Proof Method 1.58. *Proving* $P \Longrightarrow (Q \text{ AND } R)$

The result can be split up into the two cases, $P \Longrightarrow Q$, and $P \Longrightarrow R$, and then each case can be proved separately.

You are asked to verify this common sense result using truth tables in Problem 78.

Proof Method 1.59. *Proving* $(P \text{ AND } Q) \Longrightarrow R$

In this case we assume that P and Q are true and use any of the previous techniques to prove R, such as the Direct Proof Method 1.51, the Contrapositive Method 1.54, or Proof by Contradiction 1.55.

PROPOSITION. *Let x be a real number. Then $x^2 + x < 0$ if and only if $-1 < x < 0$.*

Note that the statement "$-1 < x < 0$" means "$-1 < x$ AND $x < 0$."

Proof. We first prove $x^2 + x < 0 \Longrightarrow -1 < x$ AND $x < 0$.

Assume that $x^2 + x < 0$ so

$$x(x+1) < 0.$$

If the product of two numbers is negative, then one number is positive and the other is negative. There are two cases to consider.
Case (i) If $x > 0$ and $x + 1 < 0$, then $x > 0$ and $x < -1$. This case is impossible, since no real number is both positive and negative.
Case (ii) If $x < 0$ and $x + 1 > 0$, then $x < 0$ and $x > -1$. Hence $-1 < x < 0$.

We now prove $-1 < x$ AND $x < 0 \Longrightarrow x^2 + x < 0$.

If $-1 < x$ and $x < 0$, then $x + 1 > 0$ and $x < 0$. Since the product of a positive number and a negative number is negative, it follows that $x(x + 1) < 0$. That is, $x^2 + x < 0$. □

You may find it useful to refer back to the different types of proof methods in this section when you encounter specific examples of proofs in the remainder of the book.

1.6 COUNTEREXAMPLES

How do mathematicians think up their theorems? It is usually a combination of looking at many examples, mimicking a result in a related area, a hunch, and trial and error. However, the methods they use in formulating theorems are almost never disclosed or published; only the finished proof is presented. Before a result can be called a theorem or proposition, it has to be proved. A result that is thought to be true but has not been proven is called a *conjecture.*

Sometimes a conjectured result in mathematics is not true. In that case, we would not be able to prove it. However, we could try to disprove it; that is, try to prove that its negation is true. If the conjectured result is of the form

$$\forall x,\ P(x),$$

then its negation is NOT $(\forall x,\ P(x))$, which by the Quantifier Negation Rules 1.45, is equivalent to

$$\exists x,\ \text{NOT } P(x).$$

Hence to disprove the statement $\forall x,\ P(x)$ we only have to find *one value* of x, say c, such that $P(c)$ is false. This value c is called a **counterexample** to the conjecture $\forall x,\ P(x)$.

If the conjectured result is of the form

$$\forall x,\ P(x) \Longrightarrow Q(x),$$

then its negation is

$$\exists x,\ \text{NOT } (P(x) \Longrightarrow Q(x)),$$

which, by Example 1.23 and Exercise 22, is equivalent to the statement

$$\exists x,\ (P(x) \text{ AND NOT } Q(x)).$$

Hence $x = c$ is a counterexample to the conjecture if $P(c)$ is true, while $Q(c)$ is false.

A mathematician, when first tackling a proof of a conjecture, is not sure whether it is true and must always be on the lookout for counterexamples. You will be put in this situation when answering a question that asks whether a certain result is true or not.

Often the first attempt at stating a theorem is basically correct but fails in certain cases. If this happens, the hypotheses might be able to be changed to eliminate the bad cases and obtain a true result. When writing proofs, you should get in the habit of making sure that you have used all the hypotheses. If you have not used them all and your proof is correct, then you have proved a more general result, as the unused hypotheses could be removed from the statement of the theorem. However, at this stage in your mathematical development, it usually means that your proof is faulty, as most of the results you will be asked to prove have had any unnecessary hypotheses removed.

EXAMPLE. Let x be a real number. Disprove the statement

$$\text{If } x^2 > 9 \text{ then, } x > 3.$$

Solution. One counterexample to the statement is obtained by taking $x = c = -4$, since $c^2 = 16 > 9$ and $c \leq 3$. This counterexample disproves the statement. □

EXAMPLE. Let m and n be integers. If m or n is odd, is it necessarily true that $m^3 + n^3$ is odd?

Solution. This is a question about the converse of a result proved on page 16.

The answer to the question is no, since we can easily find a counterexample in which m or n is odd, and m^3+n^3 is even. One such counterexample is $m = 1$ and $n = 1$.

Notice that the mathematical inclusive OR is necessary here. Of course, there is an infinite number of counterexamples in this case; they occur when m and n are both odd. However, one counterexample is enough to disprove the result. □

If we wished to disprove an existence statement such as $\exists x,\ P(x)$, then its negation is NOT $(\exists x,\ P(x))$, which is equivalent to $\forall x,$ NOT $P(x)$. In this case we cannot use a counterexample because we have to show that $P(x)$ is false *for all* values of x.