Contents

Chapter 1: Logic.
   Section 1: Introduction.
   Section 2: Propositional Calculus.
   Section 3: Quantifiers.

Chapter 2: Mathematical Proofs.
   Section 4: First Examples of Mathematical Proofs.
   Section 5: Induction.
   Section 6: Insight versus Induction.
   Section 7: Complete Induction.
   Section 8: Order Properties of the System of Real Numbers.
   Section 9: Absolute Value.

Chapter 3: Sets, Functions, and Relations.
   Section 10: Sets.
   Section 11: Functions.
   Section 12: More About Functions
   Section 14: Applications of the Principles of Counting.
   Section 15: Infinite Sets.
   Section 16: More About Infinite Sets.
   Section 17: Relations.
   Section 18: Well-Ordered Sets and the Magic Words “And So On.”
Chapter 1

Logic

Section 1. Introduction

Logic is the art of reasoning. In some form it is as old as human thought. Legal arguments were probably among the earliest instances of intricate reasoning. The Babylonian king Hammurabi (1728–1686 B.C.) promulgated the oldest surviving code of laws. Mathematics as practised by the Egyptians and Babylonians as early as the nineteenth century B.C. seems to have consisted of recipes developed by trial and error. In the sixth century B.C., the Greeks (Thales, Pythagoras, and others) began to establish mathematics as a deductive science in which truths that are not obvious were explained in terms of obvious ones. Of course logic was an essential tool for this. Greek philosophers of the fifth and fourth centuries B.C. delighted in trying to trick their listeners with fallacious arguments. These developments in mathematics and in rhetoric focused interest on logic. Aristotle (384–322 B.C.) is credited with establishing logic as a subject to be studied in its own right. By about 300 B.C., with the publication of Euclid’s Elements, the Greek development of mathematics as a deductive science had achieved a highly polished form.

Aristotle’s formulation of logic remained the standard for over two thousand years. Leibniz (1646–1716), Euler (1707–1783), and Bolzano (1781–1848) made some of the first tentative efforts to improve on the logic of Aristotle. Then in 1847, Augustus De Morgan’s Formal Logic and George Boole’s Mathematical Analysis of Logic were published. These works initiated a revolution in logic which culminated in the development of modern symbolic logic, a vast improvement on the cumbersome logical system of Aristotle. Some other important contributors to this revolution in logic during the second half of the nineteenth century and the early years of the twentieth century were Gottlob Frege, Charles Sanders Peirce, Giuseppe Peano, Bertrand Russell and Alfred North Whitehead. During about the same period, a revolution in mathematics was also taking place. We shall discuss some aspects of this revolution in mathematics in later chapters. In this chapter, we shall present the fundamentals of modern symbolic logic.

In logic, one seeks to determine which sentences are true and which are false. Under the usual interpretation of the words and symbols in them, the following sentences are true:

Paris is the capital of France.
1 + 3 = 4.
5 < 7.

Under the usual interpretation of the words and symbols in them, the following sentences are false:

The moon is made of green cheese.
2 + 3 = 4.
7 < 5.

By the way, perhaps you are not used to thinking of formulas such as 1 + 3 = 4 or 5 < 7 as sentences, but they are. For instance, the formula 1 + 3 = 4 has a subject, “1 plus 3”, and a predicate, “is equal to 4.”

It is sometimes convenient to speak of the truth value of a sentence. When a sentence is true, its truth value is “true.” When a sentence is false, its truth value is “false.”

If there are variables in a sentence, the truth value of the sentence may depend on what the variables in it stand for. For instance, the sentence $x + 3 = 4$ is true when $x$ stands for 1, but false otherwise. To take another example, the truth value of the sentence $x < y$ depends on what the variables $x$ and $y$ stand
for. If \( x \) stands for 5 and \( y \) stands for 7, then \( x < y \) is true. If \( x \) stands for 7 and \( y \) stands for 5, then \( x < y \) is false. If \( x \) stands for a two-by-two matrix and \( y \) stands for an apple, then \( x < y \) is false.

Some sentences, such as “Shut the door!” or “Do you like Mozart?” cannot properly be said to have truth values. (Your answer to a question such as “Do you like Mozart?” would have a truth value, but the question itself does not.) Logic does not deal with such sentences. Logic deals only with sentences that, at least in principle, may be said to have a truth value, though this truth value may depend on what the variables (if any) in the sentence stand for, as well as on how the words and symbols in the sentence are interpreted.

It seems appropriate to conclude this introduction with some remarks on the role of logic in mathematics. Logic can help to discover mathematical truths but logic alone is not usually sufficient for this. Insight and intuition are also needed. With the help of these, one can hope to formulate intelligent guesses about what may be true. Then one must check these guesses to make sure that one has not overlooked anything. Logic is the tool that mathematicians use to do this.

Section 2. Propositional Calculus

In logic, words and phrases such as “not”, “and”, “or”, “implies”, and “if and only if” serve as logical connectives to build compound sentences out of simpler sentences. Propositional calculus (which is also called sentential calculus) is the branch of logic that is concerned with analysing the truth values of such compound sentences in terms of the truth values of the simpler sentences from which they are built. In propositional calculus, it is often convenient to denote sentences by letters such as \( P \), \( Q \), \( R \), and so on. When so used, these letters are called propositional variables. It is also convenient to abbreviate “not”, “and”, “or”, “implies”, and “if and only if” by \( \neg \), \( \land \), \( \lor \), \( \Rightarrow \), and \( \Leftrightarrow \) respectively. For example, suppose \( P \) stands for the sentence “Jill likes Jack” and \( Q \) stands for the sentence “Mary had a little lamb”. Then the expression \( \neg P \) stands for the sentence “Jill does not like Jack” (which may also be rendered as “It is not the case that Jill likes Jack”). The expression \( P \land Q \) stands for the sentence “Jill likes Jack and Mary had a little lamb.” The expression \( P \lor Q \) stands for the sentence “Jill likes Jack or Mary had a little lamb.” The expression \( P \Rightarrow Q \) stands for the sentence “If Jill likes Jack implies Mary had a little lamb” (which more often would be rendered as “If Jill likes Jack, then Mary had a little lamb”). Finally, the expression \( P \Leftrightarrow Q \) stands for the sentence “Jill likes Jack if and only if Mary had a little lamb.” These whimsical examples have been chosen just for the sake of illustrating how the notation is supposed to be interpreted. If \( P \) and \( Q \) stand for other sentences, then the sentences that \( \neg P \), \( P \land Q \), \( P \lor Q \), \( P \Rightarrow Q \), and \( P \Leftrightarrow Q \) stand for change accordingly.

It should be understood that the meanings of the symbols \( \neg \), \( \land \), \( \lor \), and \( \Rightarrow \) are not exactly the same as the meanings of the English words “not”, “and”, “or”, and “implies”. In fact, each of these English words has many different meanings. For example, the definition of the word “and” in the Oxford English Dictionary is more than a page long. In logic, each of the symbols \( \neg \), \( \land \), \( \lor \), \( \Rightarrow \), and \( \Leftrightarrow \) has a single precise meaning that will be explained below. Thus in logic, we are not concerned with the analysis of the meaning of sentences in a natural language such as ordinary English. Rather, we are interested in constructing an artificial language in which the ambiguities of ordinary English are eliminated and which is therefore more suitable than ordinary English in situations in which precise reasoning is called for. However, you should not interpret the last sentence as an exhortation to avoid the use of English words and use only symbols. When talking about logic, it is convenient to use the symbols \( \neg \), \( \land \), \( \lor \), \( \Rightarrow \), and \( \Leftrightarrow \). However, when applying logic, it is usually better to use the corresponding words, with the understanding that they are to be interpreted in their logical sense, rather than in one of their other ordinary language senses.

Let us now turn to an explanation of the meanings of the symbols \( \neg \), \( \land \), \( \lor \), \( \Rightarrow \), and \( \Leftrightarrow \) in logic.

**Negation.** Recall that the symbol \( \neg \) is supposed to correspond to the word “not.” Given a sentence \( P \), the sentence \( \neg P \) is called the negation of \( P \). Given a sentence \( Q \), we say that \( Q \) is a negative sentence when \( Q \) is of the form \( \neg P \) where \( P \) is some other sentence. The meaning of \( \neg \) in logic is defined by the following rule: If \( P \) is a true sentence, then the sentence \( \neg P \) is considered to be false, whereas if \( P \) is a false sentence, then the sentence \( \neg P \) is considered to be true. It is customary to summarize this definition...
in a truth table, as follows:

<table>
<thead>
<tr>
<th>P</th>
<th>¬P</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

Of course in such a truth table, “T” is an abbreviation for “true” and “F” is an abbreviation for “false.”

**Logical Equivalence.** Notice that if \( P \) is true, then \( ¬P \) is false, so \( ¬¬P \) is true, whereas if \( P \) is false, then \( ¬P \) is true, so \( ¬¬P \) is false. Thus whatever the truth value of \( P \) may be, the truth value of \( ¬¬P \) is the same. We describe this situation by saying that \( ¬¬P \) is logically equivalent to \( P \). (The order is not important. One may equally well say that \( P \) is logically equivalent to \( ¬¬P \).) We shall see many other examples of logical equivalence below.

**An Abbreviation for Logical Equivalence.** The phrase “is logically equivalent to” is rather long and is cumbersome to use in handwritten work, so it is convenient to have an abbreviation for it. You may write \( A \equiv B \) as an abbreviation for the statement that the sentence \( A \) is logically equivalent to the sentence \( B \). For instance, \( P \equiv ¬P \). It is good to keep in mind that while the symbols \( ¬, \land, \lor, ⇒, \) and \( ⇔ \) are symbols of propositional calculus, the symbol \( \equiv \) is not one of the symbols of propositional calculus. Rather, it is just an abbreviation for the English phrase “is logically equivalent to.” So for instance \( A \land B \) is a sentence in propositional calculus but \( A \equiv B \) is not. Rather \( A \equiv B \) is an abbreviation for a statement in ordinary language about two sentences in propositional calculus. Without going into a full explanation, we may say that in our current discussion, propositional calculus is the object language, or in other words, the language that we are studying and ordinary language is the metalanguage, or in other words, the language in which we conduct our discussion of the object language. The symbol \( \equiv \) belongs to the metalanguage, not the object language.

**Negation (Continued).** Given sentences \( P \) and \( Q \), when \( Q \) is logically equivalent to \( ¬P \), we say that \( Q \) is a denial of \( P \). The negation of a sentence is a denial of that sentence, but a denial of a sentence need not be the negation of that sentence. For instance, \( P \) is a denial of \( ¬P \), because \( P \) is logically equivalent to \( ¬¬P \), which is the negation of \( ¬P \). However \( P \) is not the negation of \( ¬P \).

Here is an example to illustrate the difference between the logical meaning of \( ¬ \) and the meaning of “not” in ordinary English. To say that something is “unimportant” means that it is not important. But to say that something is “not unimportant” does not exactly mean that it is important. It may mean that it just somewhat important, rather than highly important. Such subtle shades of meaning are not captured by the definition of \( ¬ \) in logic. Nevertheless, the logical definition of \( ¬ \) does correspond to the way the word “not” is generally used in mathematics.

**Conjunction.** Recall that the symbol \( \land \) is supposed to correspond to the word “and.” Given sentences \( P \) and \( Q \), the sentence \( P \land Q \) is called the conjunction of \( P \) and \( Q \). Given a sentence \( R \), we say that \( R \) is a conjunctive sentence when \( R \) is of the form \( P \land Q \), where \( P \) and \( Q \) are some other sentences, and we call the sentences \( P \) and \( Q \) the conjuncts in the sentence \( R \). The meaning of \( \land \) in logic is defined by the following rule: Given sentences \( P \) and \( Q \), the sentence \( P \land Q \) is considered to be true just when both of \( P \) and \( Q \) are true. If at least one of them is false, then \( P \land Q \) is considered to be false. Once again, we summarize the logical definition of \( \land \) in a truth table:

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>P \land Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

By the way, to remember the order in which the lines are written in such a truth table, notice that the truth values of the basic propositional variables \( P \) and \( Q \) together are listed in reverse alphabetical order: TT,
Notice that whatever the truth values of \( P \) and \( Q \) may be, the sentence \( Q \land P \) has the same truth value as the sentence \( P \land Q \), because each of the latter two sentences is true just when both of \( P \) and \( Q \) are true. Thus \( Q \land P \) is logically equivalent to \( P \land Q \). Sometimes one describes this situation by saying that \( \land \) is commutative. This means that \( P \land (Q \land R) \) is logically equivalent to \( (P \land Q) \land R \). (To see this, notice that \( P \land (Q \land R) \) is true just when all three of \( P, Q, R \) are true, and that the same holds for \( (P \land Q) \land R \).) Since \( \land \) is associative, we may omit parentheses in \( P \land Q \land R \).

In ordinary English, “and” is not always commutative. For instance, the sentence “Judith caught a plane and went to New York” conveys quite a different meaning than the sentence “Judith went to New York and caught a plane.” This illustrates one of the differences between the logical meaning of \( \land \) and the meaning of “and” in ordinary English. Another common use of “and” in ordinary English is to join the terms of a list, as in “Bob and Carol and Ted and Alice.” Another such example, which is particularly relevant here, occurs in the phrase “both of \( P \) and \( Q \)” Here “and” connects nouns. (In the latter example, \( P \) and \( Q \) stand for sentences but grammatically, in the phrase in question, the letters \( P \) and \( Q \) play the role of nouns since the sentences they stand for are being considered as objects.) In logic, \( \land \) connects only sentences. This is another difference between the logical meaning of \( \land \) and the meaning of “and” in ordinary English.

**Disjunction.** Recall that the symbol \( \lor \) is supposed to correspond to the word “or.” Given sentences \( P \) and \( Q \), the sentence \( P \lor Q \) is called the disjunction of \( P \) and \( Q \). Given a sentence \( R \), we say that \( R \) is a disjunctive sentence when \( R \) is of the form \( P \lor Q \), where \( P \) and \( Q \) are some other sentences, and we call the sentences \( P \) and \( Q \) the disjuncts in the sentence \( R \). The meaning of \( \lor \) in logic is defined by the following rule: Given sentences \( P \) and \( Q \), the sentence \( P \lor Q \) is considered to be true just when at least one of \( P \) and \( Q \) is true. As usual, we can summarize the logical definition of \( \lor \) in a truth table:

\[
\begin{array}{ccc}
P & Q & P \lor Q \\
T & T & T \\
T & F & T \\
F & T & T \\
F & F & F \\
\end{array}
\]

Thus \( P \lor Q \) is false just when both of \( P \) and \( Q \) are false. In particular, if \( P \) and \( Q \) are both true, then \( P \lor Q \) is considered to be true. Thus \( \lor \) corresponds to the so-called inclusive sense of “or,” as in the sentence “You must be at least 18 years old or accompanied by an adult to be admitted to this movie.” (If you are at least 18 years old and you are also accompanied by an adult, you will still be able to get in.) In ordinary English, “or” may also have an exclusive sense, as in the question “Would you like tea or coffee?” (You are not expected to answer “Both.”) Even less are you expected to answer simply “Yes,” although that would be consistent with the meaning of “or” in logic.) In Latin, there were two words for “or”: “aut” for “exclusive or” and “vel” for “inclusive or.” As a matter of fact, the symbol \( \lor \) for “or” in logic is derived from the first letter of “vel.” (And the symbol \( \land \) for “and” in logic is simply an upside down \( \lor \).)

It is easy to check that \( \lor \) is commutative and associative. In other words, \( Q \lor P \) is logically equivalent to \( P \lor Q \), and \( P \lor (Q \lor R) \) is logically equivalent to \( (P \lor Q) \lor R \).

**Connections between Negation, Conjunction, and Disjunction.** In algebra, there are a number of rules that relate the operations of addition, subtraction, multiplication, and division. For instance, \( a(b + c) = ab + ac \). Analogously, in logic, there are rules that relate the different logical connectives. We shall now discuss some of the rules that relate the logical connectives \( \neg \), \( \land \), and \( \lor \). The main ones are called De Morgan’s laws and the distributive laws.

**2.1 Theorem.** (De Morgan’s Laws.) Let \( P \) and \( Q \) be sentences. Then:

(a) \( \neg(P \land Q) \) is logically equivalent to \( \neg P \lor \neg Q \).

(b) \( \neg(P \lor Q) \) is logically equivalent to \( \neg P \land \neg Q \).
Proof. First we should point out that \(¬P \lor ¬Q \) means \((¬P) \lor (¬Q)\). Similarly, \(¬P \land ¬Q\) means \((¬P) \land (¬Q)\). Now we can see (a) by inspecting the following truth table:

<table>
<thead>
<tr>
<th>(P)</th>
<th>(Q)</th>
<th>(P \land Q)</th>
<th>(¬(P \land Q))</th>
<th>(¬P)</th>
<th>(¬Q)</th>
<th>(¬P \lor ¬Q)</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

The point is that the column of truth values headed by \(¬(P \land Q)\) is the same as the column of truth values headed by \(¬P \lor ¬Q\).

While a proof based on such a truth table is convincing, a proof by means of an explanation in words is often more enlightening. Moreover, the exercise of writing explanations in words for such basic facts of logic is a good way to prepare for writing more advanced mathematical proofs. Accordingly, let us also prove (a) by means of an explanation in words.

Suppose the sentence \(¬(P \land Q)\) is true. Then the sentence \(P \land Q\) is false, so at least one of the sentences \(P\) and \(Q\) is false, so at least one the sentences \(¬P\) and \(¬Q\) is true, so the sentence \(¬P \lor ¬Q\) is true. This shows that if the sentence \(¬(P \land Q)\) is true, then the sentence \(¬P \lor ¬Q\) is true.

Conversely, suppose the sentence \(¬P \lor ¬Q\) is true. Then at least one of the sentences \(¬P\) and \(¬Q\) is true, so at least one the sentences \(P\) and \(Q\) is false, so the sentence \(P \land Q\) is false, so the sentence \(¬(P \land Q)\) is true. This shows that if the sentence \(¬P \lor ¬Q\) is true, then the sentence \(¬(P \land Q)\) is true.

It follows that the sentence \(¬(P \land Q)\) is true exactly when the sentence \(¬P \lor ¬Q\) is true. (Then by elimination, the sentence \(¬(P \land Q)\) is false exactly when the sentence \(¬P \lor ¬Q\) is false.) Therefore the sentence \(¬(P \land Q)\) is logically equivalent to the sentence \(¬P \lor ¬Q\).

Notice that the explanation in words may be thought of as consisting in analysing the truth table without actually writing it out. The first paragraph of the explanation in words shows that in each line of the truth table \(¬(P \land Q)\) is true, \(¬P \lor ¬Q\) is also true. The second paragraph of the explanation in words shows that in each line of the truth table \(¬P \lor ¬Q\) is true, \(¬(P \land Q)\) is also true. It follows that \(¬(P \land Q)\) is true in exactly the same lines of the truth table where \(¬P \lor ¬Q\) is true. (Then by elimination, \(¬(P \land Q)\) is false in exactly the same lines of the truth table where \(¬P \lor ¬Q\) is false.) Hence in every line of the truth table, \(¬(P \land Q)\) has the same truth value as \(¬P \lor ¬Q\). Therefore \(¬(P \land Q)\) is logically equivalent to \(¬P \lor ¬Q\).

The proof of (b) is left as an exercise. ■

Exercise 1. Prove Theorem 2.1(b) in two ways:
(a) By means of a truth table;
(b) By means of an explanation in words.

2.2 Example.
(a) Let \(R\) stand for the sentence “The murder occurred between midnight and sunrise, and the butler did it.” Then \(¬R\), the negation of \(R\), is logically equivalent to the sentence “The murder did not occur between midnight and sunrise, or the butler did not do it.” This follows from the first of De Morgan’s laws.

(b) Let \(R\) stand for the sentence “The butler did it or the maid did it.” Then \(¬R\), the negation of \(R\), is logically equivalent to the sentence “The butler did not do it and the maid did not do it.” This follows from the second of De Morgan’s laws.

2.3 Example. Let \(x\) be a real number. The sentence \(1 \leq x < 3\) means \((1 \leq x) \land (x < 3)\). Hence, by De Morgan’s first law, the sentence \(¬(1 \leq x < 3)\) is logically equivalent to the sentence \(¬(1 \leq x) \lor ¬(x < 3)\). But since \(x\) is a real number, the sentence \(¬(1 \leq x)\) is logically equivalent to the sentence \(x < 1\), and the sentence \(¬(x < 3)\) is logically equivalent to the sentence \(x \geq 3\). Hence the sentence \(¬(1 \leq x < 3)\) is logically equivalent to the sentence \((x < 1) \lor (x \geq 3)\). With the help of our abbreviation “≡” for the phrase
“is logically equivalent to,” we may summarize this argument as follows:
\[
\neg(1 \leq x < 3) \equiv \neg[(1 \leq x) \land (x < 3)] \\
\equiv \neg(1 \leq x) \lor \neg(x < 3) \\
\equiv (x < 1) \lor (x \geq 3).
\]

In other words, to say that it is not the case that \(1 \leq x < 3\) is logically equivalent to saying that either \(x < 1\) or \(x \geq 3\). Another way to see this is to think in terms of the real number line. To say that \(1 \leq x < 3\) means that \(x\) lies between 1 and 3 (and \(x \neq 3\) but maybe \(x = 1\). Hence to say that \(\neg(1 \leq x < 3)\) means that either \(x\) lies to the left of 1, or \(x\) lies to the right of 3 (but maybe \(x = 3\). This way has the advantage that we can illustrate it by a drawing, but you should understand the other way too.

2.4 Theorem. (The Distributive Laws.) Let \(P, Q,\) and \(R\) be sentences. Then:

(a) \(P \land (Q \lor R)\) is logically equivalent to \((P \land Q) \lor (P \land R)\).

(b) \(P \lor (Q \land R)\) is logically equivalent to \((P \lor Q) \land (P \lor R)\).

Proof. This time the proof of (a) will be left as an exercise. Let us prove (b). For the sake of illustration, we shall do this in two ways: first by means of a truth table, and then by means of an explanation in words. Here is the truth table:

\[
\begin{array}{cccccccc}
P & Q & R & Q \land R & P \land (Q \land R) & P \lor (Q \land R) & P \lor Q & P \lor R & (P \lor Q) \land (P \lor R) \\
T & T & T & T & T & T & T & T & T \\
T & T & F & F & T & T & T & T & T \\
T & F & T & F & T & T & T & T & T \\
T & F & F & F & T & T & T & T & T \\
F & T & T & T & T & T & T & T & T \\
F & T & F & F & T & T & T & T & T \\
F & F & T & F & F & T & F & F & F \\
F & F & F & F & F & F & F & F & F \\
\end{array}
\]

Thus \(P \lor (Q \land R)\) is logically equivalent to \((P \lor Q) \land (P \lor R)\), because the column of truth values headed by \(P \lor (Q \land R)\) is the same as the column of truth values headed by \((P \lor Q) \land (P \lor R)\).

Notice that this time the truth table has eight lines. The reason for this is as follows. \(P\) may be either true or false. For each of these 2 possibilities, \(Q\) may be either true or false, which makes \(2 \times 2 = 4\) possible combinations of truth values for \(P\) and \(Q\). But for each of these 4 possibilities, \(R\) may be either true or false, which makes \(4 \times 2 = 8\) possible combinations of truth values for \(P, Q,\) and \(R\).

Now let us give the explanation in words. Suppose the sentence \(P \lor (Q \land R)\) is true. Then at least one of the two sentences \(P\) and \(Q \land R\) is true.\(^1\)

Case 1. Suppose the sentence \(P\) is true. Then both of the sentences \(P \lor Q\) and \(P \lor R\) are true, so the sentence \((P \lor Q) \land (P \lor R)\) is true.

Case 2. Suppose the sentence \(Q \land R\) is true. Then both of the sentences \(Q\) and \(R\) are true, so both of the sentences \(P \lor Q\) and \(P \lor R\) are true, so the sentence \((P \lor Q) \land (P \lor R)\) is true.

Thus in either case, the sentence \((P \lor Q) \land (P \lor R)\) is true.\(^2\) We have shown that if the sentence \(P \lor (Q \land R)\) is true, then the sentence \((P \lor Q) \land (P \lor R)\) is true.

Conversely, suppose the sentence \((P \lor Q) \land (P \lor R)\) is true. Then both of the sentences \(P \lor Q\) and \(P \lor R\) are true. Now either \(P\) is true or \(P\) is false.\(^3\)

\(^1\) We consider two cases. First, the case where \(P\) is true. Second, the case where \(Q \land R\) is true. It is possible that both are true, but there is no need to consider this as a third case, because either of the two cases we consider already covers this possibility.

\(^2\) To repeat, it is not necessary to consider the case where both of the sentences \(P\) and \(Q \land R\) are true, because this case is subsumed under Case 1 and also under Case 2. The argument in Case 1 works if both of \(P\) and \(Q \land R\) are true. So does the argument in Case 2.

\(^3\) Here we appeal to the so-called law of the excluded middle: a logical sentence is either true or false. Our use of this principle in this example just makes the proof shorter. There are other examples where the use of the law of the excluded middle or one of its equivalents is essential, not just convenient.
Case 1. Suppose $P$ is true. Then the sentence $P \lor (Q \land R)$ is true.

Case 2. Suppose $P$ is false. Then since the sentence $P \lor Q$ is true, $Q$ must be true. Similarly, since the sentence $P \lor R$ is true, $R$ must be true. Thus both of the sentences $Q$ and $R$ are true, so the sentence $Q \land R$ is true, so the sentence $P \lor (Q \land R)$ is true.

Thus in either case, the sentence $P \lor (Q \land R)$ is true. Therefore if the sentence $(P \lor Q) \land (P \lor R)$ is true, then the sentence $P \lor (Q \land R)$ is true.

From the previous two paragraphs, it follows that the sentence $P \lor (Q \land R)$ is true exactly when the sentence $(P \lor Q) \land (P \lor R)$ is true. Hence the sentence $P \lor (Q \land R)$ is logically equivalent to the sentence $(P \lor Q) \land (P \lor R)$.

2.5 Remark. In the preceding proof, we saw our first example of a truth table involving 3 basic propositional variables. Such a truth table has 8 lines. As is customary, we listed these lines so that the truth values of the 3 basic propositional variables $P$, $Q$, and $R$ together would be in reverse alphabetical order: TTT, TTF, TFT, TFF, FTT, FTF, FFT, FFF.

Exercise 2. Prove Theorem 2.4(a) in two ways:

(a) By means of a truth table;
(b) By means of an explanation in words.

Exercise 3. Show by means of a truth table that the sentence $P \land (Q \lor R)$ is not logically equivalent to the sentence $(P \land Q) \lor R$. Then explain how the truth value of the sentence “Bob likes Sally, and Sally likes Bob or Sally likes Joe” could be different from the truth value of the sentence “Bob likes Sally and Sally likes Bob, or Sally likes Joe.” (The placement of the comma determines where the parentheses should go in the symbolic representations of these sentences.)

Exercise 4. Suppose that $P \lor Q$ is true and $\neg Q$ is true. Explain why it follows that $P$ must be true.4

Conditional Sentences. A sentence of the form $P \Rightarrow Q$ is called a conditional sentence. In such a conditional sentence, $P$ is called the antecedent and $Q$ is called the consequent. Recall that $P \Rightarrow Q$ is supposed to mean “$P$ implies $Q$”. In other words, $P \Rightarrow Q$ is supposed to mean “If $P$, then $Q$.” Just as was the case with “not”, “and”, and “or”, when we define $\Rightarrow$ in logic, we do not wish to try to capture all the various meanings that the word “implies” has in ordinary English. Rather, we wish to settle on a single precise meaning that will be useful in logic. To define the precise meaning of $\Rightarrow$ in logic, we must explain what the truth value of $P \Rightarrow Q$ is in terms of the truth values of $P$ and $Q$. The following truth table does this:

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$P \Rightarrow Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

The first two lines of this truth table are not surprising: When $P$ and and $Q$ are both true, $P \Rightarrow Q$ is considered to be true, and when $P$ is true and $Q$ is false, $P \Rightarrow Q$ is considered to be false. However the last two lines of the truth table for $\Rightarrow$ are apt to seem a little strange at first, for they tell us that whenever $P$ is false, $P \Rightarrow Q$ is considered to be true. Remember though that the appropriate question is not “How do we know that $\Rightarrow$ is defined this way?” Rather, the appropriate question is “Why do we choose to define $\Rightarrow$ this way?” One answer to this question is that we want $P \Rightarrow Q$ to mean that $Q$ is at least as true as $P$. Now if $P$ is false, then whether $Q$ is true or false, $Q$ will be at least as true as $P$, so $P \Rightarrow Q$ should be true. Notice that this way of looking at $P \Rightarrow Q$ also makes it easy to remember that whenever $Q$ is true, $P \Rightarrow Q$ is true. We shall have more to say later about the reasons why $\Rightarrow$ is defined as it is in logic.

Let us emphasize again that $P \Rightarrow Q$ stands for “If $P$, then $Q$.” You should avoid the mistake of writing “If $P \Rightarrow Q$” when you mean “If $P$, then $Q$.” Remember, the symbol “$\Rightarrow$” does not mean “then.”

4 This rule of inference is called disjunctive syllogism.
2.6 Example. Let \( x \) be any real number. Then the sentence “If \( x < 1 \), then \( x < 3 \)” is true. This should seem intuitively correct. Let us explain how it accords with the definition of \( \Rightarrow \) given above. Let \( P \) stand for the sentence “\( x < 1 \)” and let \( Q \) stand for the sentence “\( x < 3 \)” Then \( P \Rightarrow Q \) stands for the sentence “If \( x < 1 \), then \( x < 3 \).” Whatever \( x \) stands for, it must satisfy one of the mutually exclusive conditions shown in the left column of the following truth table:

<table>
<thead>
<tr>
<th>( x )</th>
<th>( P )</th>
<th>( Q )</th>
<th>( P \Rightarrow Q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x &lt; 1 )</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>( 1 \leq x &lt; 3 )</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>( x \geq 3 )</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

Since there is no value for \( x \) that would make \( P \) true and \( Q \) false at the same time, there is no line in this truth table where \( P \) is true and \( Q \) is false, so \( P \Rightarrow Q \) is always true. Notice in particular that if \( x \geq 1 \), then \( P \) is false, so \( P \Rightarrow Q \) is true.

There are a number of other phrases that are considered to be synonymous with “If \( P \), then \( Q \)” in logic. The main ones are:

- \( P \) is sufficient for \( Q \)
- \( Q \) is necessary for \( P \)
- \( Q \) if \( P \)

Thus, for instance, in logic the following sentences are all considered to be different ways of saying the same thing:

- If \( x < 1 \), then \( x < 3 \).
- \( x < 1 \) is sufficient for \( x < 3 \).
- \( x < 3 \) is necessary for \( x < 1 \).
- \( x < 3 \) if \( x < 1 \).

You should make sure that you understand these different ways of expressing a conditional sentence in words well enough so that you will not have difficulty remembering them.

Exercise 5.

(a) Joe, Sandra, Peter, and Cathy are sitting at a table in a restaurant. Each of them has a glass of some beverage in front of them. Your job is to check whether or not they are legally entitled to be consuming the beverages that you see on the table in front of them. The drinking age is 21. Joe is drinking beer. Sandra is clearly over 21. Peter is drinking milk. Cathy is obviously under 21. Whose ages or beverages would you have to check? Explain your answer.

(b) Four cards are lying on a table. Each card has a single letter on one side and a single number on the other side. The sides that are up show the following letters and numbers.

\[
\begin{array}{ccc}
A & 2 & X & 3 \\
\end{array}
\]

Your job is to check whether or not the following rule holds: Whenever there is a vowel on one side of a card, then there must be an even number on the other side. Which cards would you have to turn over to be sure that the rule holds? Explain your answer.

(c) Most people find part (a) easier than part (b). Explain how part (b) is really just a disguised form of part (a).

2.7 Remark. Each of parts (a) and (b) in Exercise 5 is an example of what is called a Wason selection task. These types of tasks, which are famous in the psychology of reasoning, were devised in 1966 by Peter Cathcart Wason. Studies consistently show\(^5\) that about 65% of people get the right answer in examples like part (a) but only about 25% of people get the right answer in examples like part (b).

---

\(^5\) See http://blogs.discovermagazine.com/loom/2005/05/02/cheating-on-the-brain/
2.8 Remark. The Symbol “⇒” Does Not Mean “Therefore.” The symbol “⇒” is frequently misused by students and even by professional mathematicians, when they use it as an abbreviation for ‘therefore’ or for ‘so.’ On the one hand, “P ⇒ Q” means “If P, then Q.” In other words, it means that if P were true, then Q would be true too. It makes no claim about the truth value of P and without knowledge of this truth value, it permits no conclusion about the truth value of Q. For instance, from the sentence “(x > 2) ⇒ (x² > 4),” we may not infer that x² > 4. On the other hand, “P, therefore Q,” or more briefly “P, so Q,” means “P is true and consequently Q is true.” It would be more accurate to symbolize it by “P ∧ (P ⇒ Q),” rather than by “P ⇒ Q.” For instance, if we write “x > 2, so x² > 4,” we mean that x > 2 and therefore x² > 4.

In this chapter, we are concerned more with studying logic than with applying logic. When we are applying logic as opposed to talking about logic, there is seldom any reason to use the symbol “⇒.” It is just as easy to write “P, so Q” and most often this is what is meant, rather than “P ⇒ Q.”

2.9 Remark. “If” versus “Suppose.” Here is a point that is related to what we just said about the common misuse of the symbol “⇒.” The following is an example of bad mathematical writing:

If x > 2, then x² > 4. Therefore x⁴ > 16. (1)

Now here is a good way to write it:

Suppose x > 2. Then x² > 4. Therefore x⁴ > 16. (2)

The difference is that in (2), the assumption “x > 2” remains in effect throughout the argument, whereas in (1), the assumption “x > 2” is no longer in effect after the end of the sentence “If x > 2, then x² > 4,” so the conclusion “x⁴ > 16” is justified in (2) but is not justified in (1). Of course, since the argument in (2) is quite short, it is practical to express it in a single sentence such as

If x > 2, then x² > 4, so x⁴ > 16.

But if you want to use an assumption throughout an argument that is several sentences long, it will probably be better to state that assumption in a sentence by itself, as we did in (2).

The Negation of a Conditional Sentence. We have seen that De Morgan’s laws help us to analyze negations of conjunctive and disjunctive sentences. Now we shall consider a similar analysis of the negation of a conditional sentence.

2.10 Theorem. Let P and Q be sentences. Then ¬(P ⇒ Q) is logically equivalent to P ∧ ¬Q.

Proof. Suppose ¬(P ⇒ Q) is true. Then P ⇒ Q is false, so P is true and Q is false. Since Q is false, ¬Q is true. Thus both of the sentences P and ¬Q are true, so the sentence P ∧ ¬Q is true.

Conversely, suppose the sentence P ∧ ¬Q is true. Then both of the sentences P and ¬Q are true. Since ¬Q is true, Q is false. Thus P is true and Q is false, so P ⇒ Q is false, so ¬(P ⇒ Q) is true.

Exercise 6. Use a truth table to give an alternative proof of Theorem 2.10.

Exercise 7. Let x and y be real numbers.

(a) Let A be the sentence “If x + y > 0, then x > 0 or y > 0.” Use Theorem 2.10 and one of De Morgan’s laws to show that ¬A is logically equivalent to “x + y > 0 and x ≤ 0 and y ≤ 0.” Be careful not to skip any steps. (Hint: To save writing, feel free to use the abbreviation “≡” for the phrase “is logically equivalent to.” It may help you to review Example 2.3.)

(b) Is the sentence A in part (a) true, or is ¬A true? Explain why.

(c) Let B be the sentence “If x + y > 2, then x > 2 or y > 2.” Is B true, or is ¬B true, or is it impossible to say without further information about the specific values of x and y? (Hint: Can you find specific values for x and y for which B is true? If so, give an example of such values. Can you find other specific values for x and y for which ¬B is true? If so, give an example of such values.)

2.11 Remark. In solving Exercise 7, you might find it even more enlightening to sketch the set of all points (x, y) in the plane, for which the sentence B is true. You should find that this set of points is not empty but is also not the whole plane.
The Converse of a Conditional Sentence. Given a conditional sentence \( P \rightarrow Q \), the sentence \( Q \rightarrow P \) is called the converse of \( P \rightarrow Q \). It is important to realize that \( Q \rightarrow P \) is not logically equivalent to \( P \rightarrow Q \). For instance, when \( P \) is false and \( Q \) is true, \( P \rightarrow Q \) is true but \( Q \rightarrow P \) is false.

2.12 Example. Let \( P \) stand for the sentence “It is raining” and let \( Q \) stand for the sentence “The streets are wet.” Then \( P \rightarrow Q \) stands for the sentence “If it is raining, then the streets are wet.” This sentence is true. On the other hand, \( Q \rightarrow P \) stands for the sentence “If the streets are wet, then it is raining.” This sentence need not be true. For instance, it might have stopped raining five minutes ago. (We are not saying that \( Q \rightarrow P \) is false. We are just saying that it need not be true. It can be true in certain circumstances. If \( P \) is true, then \( Q \rightarrow P \) is true. Thus if it happens to be raining, then the sentence “If the streets are wet, then it is raining” is considered to be true.)

2.13 Example. Let \( x \) be a real number. Whatever the value of \( x \) may be, the sentence \( x > 3 \Rightarrow x^2 > 9 \) is true. (Proof: If the sentence \( x > 3 \) is true, then so is the sentence \( x^2 > 9 \), so the sentence \( x > 3 \Rightarrow x^2 > 9 \) is true. If \( x \leq 3 \), then the sentence \( x > 3 \) is false, so the sentence \( x > 3 \Rightarrow x^2 > 9 \) is false.)

However, the converse sentence \( x^2 > 9 \Rightarrow x > 3 \) is not always true. For instance, if \( x = -4 \), then \( x^2 = 16 \), so the sentence \( x^2 > 9 \) is true but the sentence \( x > 3 \) is false, so the sentence \( x^2 > 9 \Rightarrow x > 3 \) is false. More generally, if \( x < -3 \), then the sentence \( x^2 > 9 \) is true but the sentence \( x > 3 \) is false, so the sentence \( x^2 > 9 \Rightarrow x > 3 \) is false. Thus if \( x < -3 \), then the sentence \( x > 3 \Rightarrow x^2 > 9 \) is true but the sentence \( x^2 > 9 \Rightarrow x > 3 \) is false, so for such values of \( x \), these two sentences have different truth values. (By the way, sometimes the sentence \( x^2 > 9 \Rightarrow x > 3 \) is true. It is true if \( x > 3 \). It is also true if \(-3 \leq x \leq 3 \), because then the sentence \( x^2 > 9 \) is false.)

2.14 Example. If you have studied infinite series in calculus, then you will know that if an infinite series

\[
a_1 + a_2 + a_3 + \cdots
\]

converges, then its \( n \)-th term \( a_n \) tends to zero as \( n \) tends to infinity. But you will also know that the converse of this statement is not true in general. For instance, if \( a_n = 1/n \) for all natural numbers \( n \), then \( a_n \) tends to zero as \( n \) tends to infinity but in this case the series (3) diverges. In fact,

\[
\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots = \infty,
\]

as is shown in any calculus textbook that treats infinite series.

2.15 Remark. Sometimes one writes \( P \Leftrightarrow Q \) instead of \( Q \Rightarrow P \). Here are three synonymous ways to read \( P \Leftrightarrow Q \):

- \( P \) is implied by \( Q \).
- \( P \) is necessary for \( Q \).
- \( P \) if \( Q \).

Biconditional Sentences. A sentence of the form \( P \iff Q \) is called a biconditional sentence. Recall that \( P \iff Q \) is supposed to mean “\( P \) if and only if \( Q \)” (The phrase “if and only if” is often abbreviated by “iff.”) The precise meaning of \( \iff \) in logic is defined by the following rule: Given two sentences \( P \) and \( Q \), the sentence \( P \iff Q \) is considered to be true just when both of the sentences \( P \) and \( Q \) have the same truth value. As usual, we can summarize the logical definition of \( \iff \) in a truth table:

<table>
<thead>
<tr>
<th>( P )</th>
<th>( Q )</th>
<th>( P \iff Q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

Notice that the sentence \( P \iff Q \) is true when the two sentences \( P \) and \( Q \) are both true or both false. When one of the sentences \( P \) and \( Q \) is true and the other is false, the sentence \( P \iff Q \) is false.
2.16 Example. Let $x$ be a real number. Then $x^2 = 1$ if and only if $x = 1$ or $x = -1$. This may be shown by the following chain of biconditionals:

\[
\begin{align*}
x^2 &= 1 \\
\text{iff} &
\quad x^2 - 1 = 0 \\
\text{iff} &
\quad (x - 1)(x + 1) = 0 \\
\text{iff} &
\quad x - 1 = 0 \text{ or } x + 1 = 0 \\
\text{iff} &
\quad x = 1 \text{ or } x = -1.
\end{align*}
\]

Sometimes one says that the solutions of $x^2 = 1$ are $x = 1$ and $x = -1$. Here the word “and” is not used in its logical sense but is used simply to join the terms of a list. This is not wrong, but it is more logical to say “$x^2 = 1$ if and only if $x = 1$ or $x = -1$.” (Note the “or.” It could not be right to say “$x^2 = 1$ if and only if $x = 1$ and $x = -1.” The reason why this could not be right is that whatever $x$ stands for, the sentence “$x = 1$ and $x = -1$” is false.)

Exercise 8. Solve the equation $x^2 = x + 6$. Write your answer in a logical form. Justify your answer by a suitable chain of biconditionals.

2.17 Theorem. Let $P$ and $Q$ be sentences. Then $P \iff Q$ is logically equivalent to $(P \Rightarrow Q) \land (Q \Rightarrow P)$.

Proof. Consider the following truth table:

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$P \iff Q$</th>
<th>$P \Rightarrow Q$</th>
<th>$Q \Rightarrow P$</th>
<th>$(P \Rightarrow Q) \land (Q \Rightarrow P)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

Notice that the the column of truth values headed by $P \iff Q$ is the same as the column of truth values headed by $(P \Rightarrow Q) \land (Q \Rightarrow P)$. It follows that $P \iff Q$ is logically equivalent to $(P \Rightarrow Q) \land (Q \Rightarrow P)$. $\blacksquare$

Recall that $P \iff Q$ is another way to write $Q \Rightarrow P$. Thus we see that $P \iff Q$ is logically equivalent to $(P \Rightarrow Q) \land (P \Leftarrow Q)$. Since $\land$ is commutative, it is also true that $P \iff Q$ is logically equivalent to $(P \Leftarrow Q) \land (P \Rightarrow Q)$.

Since $P \iff Q$ is logically equivalent to $(P \Leftarrow Q) \land (P \Rightarrow Q)$, we see that $P \iff Q$ is also logically equivalent to “$(P$ is necessary for $Q) \land (P$ is sufficient for $Q)$.” Consequently the sentence “$P$ is necessary and sufficient for $Q$” is considered to mean the same thing as the sentence “$P$ if and only if $Q$”.

Since a biconditional sentence $P \iff Q$ is logically equivalent to $(P \Rightarrow Q) \land (Q \Rightarrow P)$, we may prove that such a biconditional sentence is true by first proving that $P \Rightarrow Q$ is true and then proving that $Q \Rightarrow P$ is true. In such a proof of a biconditional sentence $P \iff Q$, the proof of $P \Rightarrow Q$ is called the proof of the forward implication and the proof of $Q \Rightarrow P$ is called the proof of the reverse implication.

The Negation of a Biconditional Sentence. We have seen how to analyze negations of conjunctive and disjunctive sentences (by means of De Morgan’s laws) and we have also seen how to analyze negations of conditional sentences. In the following exercise, one of the things you are asked to do is to analyze the negation of a biconditional sentence. Such a negation turns out to be related to the notion of “exclusive or.”

Exercise 9. Let $P$ xor $Q$ mean “$P$ exclusive or $Q$.” In other words, $P$ xor $Q$ should be true just when exactly one of $P$ and $Q$ is true.

(a) Write out the truth table table for $P$ xor $Q$.
(b) Show by a truth table that $P$ xor $Q$ is logically equivalent to $(P \land \lnot Q) \lor (Q \land \lnot P)$.
(c) Show by truth tables that the following four sentences are logically equivalent:

\[ P \text{ xor } Q, \quad \lnot (P \iff Q), \quad (\lnot P) \iff Q, \quad P \iff (\lnot Q). \]

(d) Show by a truth table that $(\lnot P) \iff (\lnot Q)$ is logically equivalent to $P \iff Q$. 

Copyright Neil Falkner, December 17, 2021
Don’t Ignore the Words. Mathematical prose does not just consist of formulas. In fact, it mostly consists of words. One purpose of the next exercise is to illustrate how important it is to pay attention to the words, not just the formulas.

Exercise 10. For each of the following sentences, draw a real number line and show on the number line the set of values of \( x \) for which the sentence is true. (You should get a different set for each sentence. This illustrates the fact that all of the sentences have different meanings.)

(a) \( x > 2 \) and \( x^2 > 4 \).
(b) \( x > 2 \) or \( x^2 > 4 \).
(c) If \( x > 2 \), then \( x^2 > 4 \).
(d) \( x > 2 \) iff \( x^2 > 4 \).

(Suggestion: In each part, it may help you to construct a suitable truth table. See Example 2.6.)

Parentheses. As we have seen, the placement of parentheses can make a difference in the meaning of a sentence. For instance, by Exercise 3, the sentence \( P \land (Q \lor R) \) is not logically equivalent to the sentence \( (P \land Q) \lor R \). In algebra, there are rules for interpreting expressions in which parentheses have been omitted. Multiplication is given priority over addition, so that \( a + b \cdot c + d \) means \( a + (b \cdot (c + d)) \), not \( (a + b) \cdot (c + d) \).

In logic, there are similar rules. The order of priority of the logical connectives is the same as the order in which we have introduced them, namely \( \neg, \land, \lor, \Rightarrow, \Leftrightarrow \). Thus for instance, \( \neg P \land \neg Q \) means \( (\neg P) \land (\neg Q) \).

We already used this in our discussion of De Morgan’s laws (Theorem 2.1). Here are some more examples:

\[
\begin{align*}
P \land Q \lor R \quad & \text{means} \quad (P \land Q) \lor R \\
P \land Q \Rightarrow P \lor Q \quad & \text{means} \quad (P \land Q) \Rightarrow (P \lor Q) \\
P \Rightarrow (Q \Rightarrow R) \iff P \land Q \Rightarrow R \quad & \text{means} \quad [P \Rightarrow (Q \Rightarrow R)] \iff [(P \land Q) \Rightarrow R]
\end{align*}
\]

These rules of priority for the logical connectives make it possible to save writing by omitting some parentheses. However this does not mean that parentheses should always be omitted when they are not essential. Judicious inclusion of some dispensable parentheses can often make a sentence easier to read.

Exercise 11. Show that each two of the following three sentences are logically inequivalent:

(a) \( P \Rightarrow (Q \Rightarrow R) \);
(b) \( (P \Rightarrow Q) \Rightarrow R \);
(c) \( (P \Rightarrow Q) \land (Q \Rightarrow R) \).

(Hint: To show that two sentences are logically inequivalent, it suffices to find one choice of truth values for the propositional variables in them which makes the two sentences have different truth values. Usually, with a little thought, we can accomplish this without writing out an entire truth table. For instance, suppose we wish to show that the sentence \( P \Rightarrow (Q \Rightarrow R) \) is not logically equivalent to the sentence \( (P \Rightarrow Q) \Rightarrow R \). If \( P \) is false, then \( P \Rightarrow (Q \Rightarrow R) \) is true and \( P \Rightarrow Q \) is true, so it should be easy for you to find a truth value for \( R \) which makes the truth value for \( P \Rightarrow (Q \Rightarrow R) \) different from the truth value for \( (P \Rightarrow Q) \Rightarrow R \). In this particular example, the truth value of \( Q \) turned out not even to matter but in general we should not expect to be so lucky.)

2.18 Remark. From the inequivalence of the sentences (a) and (b) in Exercise 11, we see that \( \Rightarrow \) is not associative. For this reason, in the formal language of propositional calculus, there is no place for expressions such as

\[
P \Rightarrow Q \Rightarrow R.
\]

However, in colloquial mathematical writing, by analogy with the standard practice of writing “\( a \leq b \leq c \)” to mean “\( a \leq b \) and \( b \leq c \),” some people like to write an expression such as (4) when they really mean

\[
(P \Rightarrow Q) \land (Q \Rightarrow R).
\]

For instance, they might write

\[
x > 2 \Rightarrow x^2 > 4 \Rightarrow x^2 + 3 > 7.
\]
However, one should not write something like

\[ x > 2 \Rightarrow x^2 > 4 \Rightarrow x^2 + x > 6. \]  

(5)

The reason is that if \( x^2 > 4 \), it does not follow that \( x > 2 \), because it could be that instead \( x < -2 \). Hence the second implication in (5), namely

\[ x^2 > 4 \Rightarrow x^2 + x > 6, \]

is false for certain values of \( x \). For instance, if \( x = -3 \), then \( x^2 = 9 > 4 \), but \( x^2 + x = 6 \). A correct way to write what some erroneously try to express by (5) is

If \( x > 2 \), then \( x^2 > 4 \), so \( x^2 + x > 4 + 2 = 6. \)

What is wrong with trying to express this by (5) is that in the second implication in (5), the antecedent in the first implication, namely “\( x > 2 \),” can be false. A statement like \( P \Rightarrow Q \) does not mean “\( P \) is true, so \( Q \) is true.” It means “If \( P \) is true, then \( Q \) is true too.” It makes no assertion about the truth of \( P \). It only says that \( Q \) is at least as true as \( P \). Remember that when \( P \) is false, \( P \Rightarrow Q \) is true.

2.19 Remark. The comments about (4) in Remark 2.18 also apply to longer chains of conditionals. For instance, in the formal language of propositional calculus, there is no place for expressions such as

\[ P \Rightarrow Q \Rightarrow R \Rightarrow S. \]  

(6)

However, in colloquial mathematical writing, some people like to write an expression such as (6) to mean

\[ (P \Rightarrow Q) \land (Q \Rightarrow R) \land (R \Rightarrow S). \]

But it is important to remember that in each implication in (6), one must not assume the truth of the antecedent in the previous implication. For instance, it would be acceptable to write

\[ x > 2 \Rightarrow x^2 > 4 \Rightarrow x^2 + 3 > 7 \Rightarrow (x^2 + 3)^2 > 49. \]  

(7)

But it would be bad to write

\[ x > 2 \Rightarrow x^2 > 4 \Rightarrow x^2 + 3 > 7 \Rightarrow x^2 + x + 3 > 9, \]  

(8)

because if \( x = -3 \), then \( x^2 + 3 = 12 > 7 \), but \( x^2 + x + 3 = 9 \), so the last implication in (8) is false for this value of \( x \). A correct way to write what some erroneously try to express by (8) is

If \( x > 2 \), then \( x^2 > 4 \), so \( x^2 + 3 > 7 \), so \( x^2 + x + 3 > 9. \)

And a better way to write (7) is

If \( x > 2 \), then \( x^2 > 4 \), so \( x^2 + 3 > 7 \), so \( (x^2 + 3)^2 > 49. \)

This could be a good time for you to review Remark 2.8. As we already pointed out there, outside of the formal language of propositional calculus, there is usually no reason to use the symbol “\( \Rightarrow \)”. It is usually better to write appropriate words instead.

Exercise 12. Show that the sentence \( P \iff (Q \iff R) \) is logically equivalent to the sentence \( (P \iff Q) \iff R \), but that neither of these sentences is logically equivalent to the sentence \( (P \iff Q) \land (Q \iff R) \). (Note: The hint for Exercise 11 should help here too.)
2.20 Remark. From the equivalence of the first two sentences mentioned in Exercise 12, we see that $\iff$ is associative. Nevertheless, in colloquial mathematical writing (but not in the formal language of propositional calculus), by analogy with the standard practice of writing “$a = b = c$” to mean “$a = b$ and $b = c$,” when people write an expression such as

$$ P \iff Q \iff R \tag{9} $$

without parentheses, they usually mean

$$ (P \iff Q) \land (Q \iff R) \tag{10} $$

even though Exercise 12 shows that in the formal language of propositional calculus, (9) is not logically equivalent to (10). This usage also applies to longer chains of biconditionals. For instance, in colloquial mathematical writing, when people write an expression such as

$$ P \iff Q \iff R \iff S $$

they usually mean

$$ (P \iff Q) \land (Q \iff R) \land (R \iff S) $$

Indeed, we already introduced this usage, without comment, in Example 2.16 and in Exercise 8. (There, we wrote “iff” rather than “$\iff.$”)

Tautologies. Consider the sentence $P \lor \neg P$. If $P$ is true, then the sentence $P \lor \neg P$ is true. If $P$ is false, then $\neg P$ is true, so again the sentence $P \lor \neg P$ is true. Thus whether $P$ is true or false, the sentence $P \lor \neg P$ is true. We describe this situation by saying that the sentence $P \lor \neg P$ is a tautology. In general, a tautology is a sentence that is true simply because of the way it is built from more basic sentences by means of the connectives $\neg$, $\land$, $\lor$, $\Rightarrow$, and $\iff$, and not because of the truth values of these basic constituent sentences.

As we know, the sentence $\neg(P \land Q)$ is logically equivalent to the sentence $\neg P \lor \neg Q$. Another way to express this fact is to say that the sentence $[\neg(P \land Q)] \iff [\neg P \lor \neg Q]$ is a tautology. This means the same thing because a biconditional sentence $R \iff S$ is true exactly when the sentences $R$ and $S$ have the same truth values. Thus another example of a tautology is the sentence $[P \land (Q \lor R)] \iff [(P \land Q) \lor (P \land R)]$.

There are also a number of important examples of conditional sentences that are tautologies. We now turn to a discussion of some of these.

2.21 Example. Show that the sentence $(P \land Q) \Rightarrow P$ is a tautology.

Solution. We must show that $(P \land Q) \Rightarrow P$ is true no matter what truth values $P$ and $Q$ have. One way to do this is by means of a truth table. However, we prefer to give an explanation in words. Note that either $P \land Q$ is true or $P \land Q$ is false.

Case 1. Suppose $P \land Q$ is true. Then both of $P$ and $Q$ are true. In particular, $P$ is true. Hence $(P \land Q) \Rightarrow P$ is true.

Case 2. Suppose $P \land Q$ is false. Then by $(P \land Q) \Rightarrow P$ is true, by the definition of $\Rightarrow$. (Recall that a conditional sentence in which the antecedent is false is considered to be true.)

Thus in either case, $(P \land Q) \Rightarrow P$ is true. We have shown this under no assumptions on the truth values of $P$ and $Q$. Hence $(P \land Q) \Rightarrow P$ is a tautology.

In a similar way, one can show that the sentence $(P \land Q) \Rightarrow Q$ is a tautology.

6 By the way, the tautology $P \lor \neg P$ is often called the law of the excluded middle.
**Conditional Proof.** To show that a conditional sentence $A \Rightarrow B$ is true, it suffices to consider the case where $A$ is true and to show that in this case, $B$ must also be true. This approach is known as the method of conditional proof.

Let us discuss why the method of conditional proof is valid. Say we wish to prove that $A \Rightarrow B$ is true. We begin by supposing that $A$ is true. Under this assumption, we show that $B$ is true. From this we may conclude that $A \Rightarrow B$ is true whether or not $A$ is true. Here is why may we draw this conclusion. If $A$ happens to be true, then by what we showed, $B$ is true, so $A \Rightarrow B$ is true by the truth table for $\Rightarrow$. If $A$ happens to be false, then again $A \Rightarrow B$ is true by the truth table for $\Rightarrow$. Thus, as we claimed, we have shown that $A \Rightarrow B$ is true whether or not $A$ is true. In other words, we have shown that $A \Rightarrow B$ is true without the assumption that $A$ is true. At this point, the assumption that $A$ is true is said to have been discharged. (In other words, it is no longer assumed.) With the method of conditional proof, the solution of Example 2.21 can be shortened, as follows.

**2.22 Example.** Use the method of conditional proof to show that the sentence $(P \wedge Q) \Rightarrow P$ is a tautology.

*Solution.*

A1: Suppose $P \wedge Q$ is true.\(^8\)

Then both of $P$ and $Q$ are true.

In particular, $P$ is true.

We have shown that $P$ is true under the assumption A1 that $P \wedge Q$ is true.

Discharging A1, we see that $(P \wedge Q) \Rightarrow P$ is true under no assumptions.\(^9\)

Therefore $(P \wedge Q) \Rightarrow P$ is a tautology, because we have shown that it is true under no assumptions on the truth values of $P$ and $Q$. \(\blacksquare\)

In fact, the method of conditional proof is the standard way to show that such a conditional sentence is a tautology. Once again, in the example just considered, when we inferred that $(P \wedge Q) \Rightarrow P$ is true under no assumptions, the assumption that $P \wedge Q$ is true was discharged. This means that it ceased to be assumed. Whenever we use the method of conditional proof to prove a conditional sentence $A \Rightarrow B$, we show that $B$ is true under the assumption that $A$ is true. Then we may infer that $A \Rightarrow B$ is true, whether or not $A$ is true. At this point, the assumption that $A$ is true has been discharged. In normal mathematical prose, you need to read between the lines to realize when an assumption has been discharged. But until this is second nature to you, when you are writing proofs, it is a good idea for you to state explicitly when you have discharged an assumption.

**Exercise 13.** Show by means of an explanation in words that the sentence $P \Rightarrow (P \lor Q)$ is a tautology. (Do not use cases. Instead, use the method of conditional proof. Be explicit about discharging assumptions.)

In a similar way, one can show that the sentence $Q \Rightarrow (P \lor Q)$ is a tautology.

**Exercise 14.** Show by means of an explanation in words that the sentence $(P \land Q) \Rightarrow (P \lor Q)$ is a tautology. (As usual, you should use the method of conditional proof. You should not use cases. Also, you should be explicit about discharging assumptions.)

**2.23 Remark.** You will have noticed that the instructions in Exercise 13 and Exercise 14 specified that you should not use cases. Of course, if you know that a sentence $P \lor Q$ is true and you wish to draw conclusions from that fact, then it is natural and appropriate to consider cases, with Case 1 being the case where $P$ is true and with Case 2 being the case where $Q$ is true. But you should not overuse cases. If you give an argument in words in which you consider all possible combinations of truth values for the basic sentences

---

\(^7\) In fact, this is why we defined $A \Rightarrow B$ to be true when $A$ is false. In other words, the way we defined $\Rightarrow$ was chosen precisely to make the method of conditional proof work.

\(^8\) Notice that we have given this assumption a label, namely A1. This makes it easier to refer back to this assumption. Also, we have written the assumption A1 on a line by itself, we have indented the part of the proof where the assumption A1 is in force (we will unindent when this part is over), and we have written each step of this part of the proof on a line by itself. It is not required that we do these things. Moreover, in normal mathematical prose, it is not common to do them. However, they are good things for you to do until you are confident that you understand the method of conditional proof.

\(^9\) Once again, this is because in the case where $P \land Q$ is true, we have just shown that $P$ is true, so that $(P \land Q) \Rightarrow P$ is true, and because in the case where $P \land Q$ is false, $(P \land Q) \Rightarrow P$ is true by the definition of $\Rightarrow$, so that in either case, $(P \land Q) \Rightarrow P$ is true. Students often have trouble with this important point, so you should think about it until you are sure you understand it. If it continues to puzzle you, ask your teacher about it.
that are involved, then you are essentially working out a truth table. One of the purposes of this section is to help you learn more efficient and insightful methods of reasoning than the method of truth tables. The method of conditional proof is an example of such a more efficient method. Quite generally, most of the particular tautologies which are considered in this section are less important than the methods of reasoning that you are meant to learn by showing that these are tautologies. This is why you should solve the exercises in this section by the indicated methods, such as the method of conditional proof, rather than by some other method, such as exhaustive consideration of cases.

**Modus Ponens.** From the truth table for $\Rightarrow$, it is apparent that if $P \Rightarrow Q$ is true and $P$ is also true, then $Q$ must be true. This rule of inference is usually called *modus ponens.*

**Conditional Proof (Continued).**

2.24 Example. Use the method of conditional proof to explain in words why the sentence

$$\{(P \lor Q) \land [(P \Rightarrow R) \land (Q \Rightarrow R)]\} \Rightarrow R$$

is a tautology.11 Be explicit about discharging assumptions.

*Solution.*

A1: Suppose $(P \lor Q) \land [(P \Rightarrow R) \land (Q \Rightarrow R)]$ is true.

Then both of $P \lor Q$ and $(P \Rightarrow R) \land (Q \Rightarrow R)$ are true.

Since $P \lor Q$ is true, at least one of $P$ and $Q$ is true.

Case 1. Suppose $P$ is true.

Since $(P \Rightarrow R) \land (Q \Rightarrow R)$ is true, $P \Rightarrow R$ is true.

Thus $P \Rightarrow R$ is true and $P$ is true.

Hence, by modus ponens, $R$ is true.

Case 2. Suppose $Q$ is true.

Since $(P \Rightarrow R) \land (Q \Rightarrow R)$ is true, $Q \Rightarrow R$ is true.

Thus $Q \Rightarrow R$ is true and $Q$ is true.

Hence, by modus ponens, $R$ is true.

Thus in either case, $R$ is true.

We have shown that $R$ is true under the assumption A1 that the sentence $(P \lor Q) \land [(P \Rightarrow R) \land (Q \Rightarrow R)]$ is true.

Discharging A1, we see that $\{(P \lor Q) \land [(P \Rightarrow R) \land (Q \Rightarrow R)]\} \Rightarrow R$ is true under no assumptions, so it is a tautology. ■

**Exercise 15.** Use the method of conditional proof to explain in words why the sentence

$$\{(P \lor Q) \land [(P \Rightarrow R) \land (Q \Rightarrow S)]\} \Rightarrow (R \lor S)$$

is a tautology.12 Be explicit about discharging assumptions.

Note that it would be very tedious to do the preceding exercise by means of a truth table. Since 4 propositional variables are involved (namely $P$, $Q$, $R$, and $S$), the truth table would have $2^4 = 16$ rows. Also, it would have 11 columns. Thus there would be a total of $16 \times 11 = 176$ entries in the truth table! The explanation in words can be given in just a few lines and is much more enlightening than the truth table would be.

**Exercise 16.** Show by means of an explanation in words that the sentence $Q \Rightarrow (P \Rightarrow Q)$ is a tautology.

---

10 The full name for this rule is really *modus ponendo ponens*, which is Latin for “the way to affirm by affirming.”

11 By the way, this tautology is called *dilemma*, or more precisely *simple constructive dilemma*.

12 By the way, this tautology is called *complex constructive dilemma*. 
The method of conditional proof can be applied in a nested way in showing that a given sentence is a tautology. (The next example illustrates this.) When this is done, it helps to write each assumption on a line by itself, to make it stand out, and it helps to label each assumption, to make it easy to refer back to it. You may use labels such as $A_1$, $A_2$, $A_3$, and so on to label the successive assumptions. Also, to keep track of the nesting of assumptions, it helps to indent a bit more each time we introduce a new assumption, and to unindent each time we discharge an assumption. (We have used this format in the solution of the next example.)

2.25 Example. Use the method of conditional proof to explain in words why the sentence

$$[(P \Rightarrow Q) \land (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$$

(11)

is a tautology. Be explicit about discharging assumptions.

Solution.

A1: Suppose $(P \Rightarrow Q) \land (Q \Rightarrow R)$ is true.

We wish to show that $P \Rightarrow R$ is true.\(^{14}\)

A2: Suppose $P$ is true.

We wish to show that $R$ is true.\(^{15}\)

From A1, it follows that $P \Rightarrow Q$ is true.

From this and A2, we see that $Q$ is true, by modus ponens.

From A1, it also follows that $Q \Rightarrow R$ is true.

From this and the fact that $Q$ is true, we see that $R$ is true, by modus ponens.

We have shown that $R$ is true under $A_1$ and $A_2$ together.

Discharging $A_2$, we see that $P \Rightarrow R$ is true under $A_1$ alone.\(^{16}\)

Finally, discharging $A_1$, we see that $[(P \Rightarrow Q) \land (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$ is true under no assumptions,\(^{17}\) so it is a tautology. ■

2.26 Remark. Maybe it will help you to understand the solution of Example 2.25 if we go over it using notation that is chosen to highlight its general structure. Observe that the sentence (11) has the following structure:

$$\frac{[(P \Rightarrow Q) \land (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)}{A_1}$$

In other words, the sentence (11) is of the form

$$A_1 \rightarrow C_1$$

where $A_1$ is $(P \Rightarrow Q) \land (Q \Rightarrow R)$ and $C_1$ is $P \Rightarrow R$. (We write “$A_1$” for “Antecedent 1” and “$C_1$” for “Consequent 1.”) Accordingly, proceeding by the method of conditional proof, our first assumption is that $A_1$ is true, and under this assumption our goal is to show that $C_1$ is true. But $C_1$ itself is of the form

$$A_2 \Rightarrow C_2,$$

\(^{13}\) By the way, this tautology is called transitivity of implication. Another name for it is hypothetical syllogism.

\(^{14}\) We have assumed the antecedent, $(P \Rightarrow Q) \land (Q \Rightarrow R)$, from the original conditional sentence, and under this assumption, we wish to prove the consequent, $P \Rightarrow R$.

\(^{15}\) The consequent, $P \Rightarrow R$, from the original sentence, is itself a conditional sentence. So to prove that it is true, we may use the method of conditional proof again. In other words, we assume the antecedent $P$ and under this assumption, together with $A_1$, we seek to prove the consequent $R$. This is what we meant when we spoke of applying the method of conditional proof in a nested way. Within the first conditional proof, we have a second conditional proof.

\(^{16}\) Under $A_1$, in the case where $P$ is true, we have just shown $R$ is true so that $P \Rightarrow R$ is true, while in the case where $P$ is false, $P \Rightarrow R$ is true by definition. Hence under $A_1$, $P \Rightarrow R$ is true whether or not $P$ is true. In other words, under $A_1$, $P \Rightarrow R$ is true whether or not $A_2$ holds.

\(^{17}\) The case where $(P \Rightarrow Q) \land (Q \Rightarrow R)$ is true is the case where $A_1$ holds. In this case, we have just shown that $P \Rightarrow R$ is true, so that $[(P \Rightarrow Q) \land (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$ is true. In the case where $(P \Rightarrow Q) \land (Q \Rightarrow R)$ is false, $[(P \Rightarrow Q) \land (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$ is true by definition. Of course, the whole point of the method of conditional proof is that these long winded explanations can be omitted because they are essentially the same in all conditional proofs. So in your answers to exercises, you are not expected to supply these explanations that we have given in footnotes, and from now on we shall omit them too.
where \( A_2 \) is \( P \) and \( C_2 \) is \( R \). (We write “\( A_2 \)” for “Antecedent 2” and “\( C_2 \)” for “Consequent 2.”) Accordingly, proceeding by the method of conditional proof once again, our second assumption is that \( A_2 \) is true. Then, under both these assumptions, our goal is to show that \( C_2 \) is true. Having done this, it follows that the conditional sentence \( A_2 \Rightarrow C_2 \) is true under the assumption that \( A_1 \) is true, whether or not \( A_2 \) is true, since if \( A_2 \) happens to be false, then \( A_2 \Rightarrow C_2 \) is automatically true. In other words, \( C_1 \) is true under the assumption that \( A_1 \) is true. (At this point, the assumption that \( A_2 \) is true is no longer in effect and is said to have been discharged.) Since \( C_1 \) is true under the assumption that \( A_1 \) is true, the conditional sentence \( A_1 \Rightarrow C_1 \) is true whether or not \( A_1 \) is true, since if \( A_1 \) happens to be false, then \( A_1 \Rightarrow C_1 \) is automatically true. Thus \( A_1 \Rightarrow C_1 \) is true under no assumptions. In other words, the sentence (11) is true under no assumptions. (At this point, the assumption that \( A_1 \) is true is no longer in effect and is said to have been discharged.) Since the sentence (11) is true under no assumptions, it is a tautology.

**2.27 Remark.** We may display the structure of the sentence (11) succinctly as follows:

\[
[(P \Rightarrow Q) \land (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R).
\]

\( \underbrace{A_1}_{\text{Assumptions}} \quad \underbrace{C_1}_{\text{Conclusion}} \)

**Exercise 17.** Use the method of conditional proof to explain in words why the sentence

\[(P \Rightarrow Q) \Rightarrow [(P \Rightarrow (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)]\]

(12)

is a tautology. (Do not use cases.) Be careful not to skip any steps. Be explicit about discharging assumptions, as we were in the solution of Example 2.25.

**Hint for Exercise 17.** Our solution of Example 2.25 involved nesting of assumptions to a depth of 2. Your solution of Exercise 17 should involve nesting of assumptions to a depth of 3. Here is why. The sentence (12) has the following structure:

\[
(P \Rightarrow Q) \Rightarrow [(P \Rightarrow (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)].
\]

\( \underbrace{A_1}_{\text{Assumptions}} \quad \underbrace{C_1}_{\text{Conclusion}} \)

In other words, the sentence (12) is of the form

\[A_1 \Rightarrow C_1,\]

where \( A_1 \) is \( P \Rightarrow Q \) and \( C_1 \) is \( [P \Rightarrow (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R) \). The sentence \( C_1 \) in turn has the following structure:

\[
(P \Rightarrow (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R).
\]

\( \underbrace{A_2}_{\text{Assumptions}} \quad \underbrace{C_2}_{\text{Conclusion}} \)

In other words, the sentence \( C_1 \) is of the form

\[A_2 \Rightarrow C_2,\]

where \( A_2 \) is \( P \Rightarrow (Q \Rightarrow R) \) and \( C_2 \) is \( P \Rightarrow R \). Finally, the sentence \( C_2 \) in turn is of the form

\[A_3 \Rightarrow C_3,\]

where \( A_3 \) is \( P \) and \( C_3 \) is \( R \). To express all this succinctly, the structure of the sentence (12) may be displayed as follows:

\[
(P \Rightarrow Q) \Rightarrow [P \Rightarrow (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R).
\]

\( \underbrace{A_1}_{\text{Assumptions}} \quad \underbrace{A_2}_{\text{Assumptions}} \quad \underbrace{C_1}_{\text{Conclusion}} \quad \underbrace{C_2}_{\text{Conclusion}} \)

By the way, you need not introduce all the notation in this hint when you write your solution to Exercise 17. You may write your answer in the style of Example 2.25, except that you will have three assumptions instead of two.
2.28 Remark. The next exercise will provide you with an “acid test” of whether you understand the idea of nested applications of the method of conditional proof.

Exercise 18. Use the method of conditional proof to explain in words why the sentence
\[ \{ A \Rightarrow [ B \Rightarrow (C \Rightarrow D)] \} \]
\[ \Rightarrow \{ [ A \Rightarrow (B \Rightarrow C)] \]
\[ \Rightarrow [(A \Rightarrow B) \]
\[ \Rightarrow (A \Rightarrow D)] \} \]
is a tautology. (Do not use cases.) Be careful not to skip any steps. Be explicit about discharging assumptions.

2.29 Example. Consider the equation
\[ \frac{3x - 15}{x^2 - 7x + 10} = \frac{1}{2}. \]
One might be tempted to solve this equation as follows:
\[ 3x - 15 = (1/2)(x^2 - 7x + 10) \]
\[ 6x - 30 = x^2 - 7x + 10 \]
\[ 0 = x^2 - 13x + 40 = (x - 5)(x - 8) \]
x = 5, 8
However, unlike what we saw in Example 2.16, the steps above do not all correspond to true biconditional sentences. Note that if \( x = 5 \), then \( x^2 - 7x + 10 = 25 - 35 + 10 = 0 \), so \( (3x - 15)/(x^2 - 7x + 10) \) is undefined. Thus \( x = 5 \) is not a solution of the original equation. What the attempt at solving the equation really showed is just that if \( (3x - 15)/(x^2 - 7x + 10) = 1/2 \), then \( x = 5 \) or \( x = 8 \). When we multiplied both sides of the original equation by \( x^2 - 7x + 10 \), the resulting equation was true if the original equation was, but not conversely. (To go back to the original equation, we would need to be able to divide both sides of the equation \( 3x - 15 = (1/2)(x^2 - 7x + 10) \) by \( x^2 - 7x + 10 \). But we may not do this if \( x^2 - 7x + 10 = 0 \).) Thus the very first step in the calculation displayed above corresponds to a conditional sentence that is true but whose converse can be false. To solve the original equation correctly, we should not just write formulas. We should also include words to express the logic of what is being done, as follows.

Suppose \( (3x - 15)/(x^2 - 7x + 10) = 1/2 \). Then \( 3x - 15 = (1/2)(x^2 - 7x + 10) \), so \( 6x - 30 = x^2 - 7x + 10 \), so \( 0 = x^2 - 13x + 40 = (x - 5)(x - 8) \), so \( x - 5 = 0 \) or \( x - 8 = 0 \), so \( x = 5 \) or \( x = 8 \). Thus if \( (3x - 15)/(x^2 - 7x + 10) = 1/2 \), then \( x = 5 \) or \( x = 8 \). (We have established this by the method of conditional proof.) Now if \( x = 5 \), then \( x^2 - 7x + 10 = 25 - 35 + 10 = 0 \), so \( (3x - 15)/(x^2 - 7x + 10) \) is undefined, so \( (3x - 15)/(x^2 - 7x + 10) = 1/2 \) is false. If \( x = 8 \), then \( x^2 - 7x + 10 = 64 - 56 + 10 = 18 \) and \( 3x - 15 = 24 - 15 = 9 \), so \( (3x - 15)/(x^2 - 7x + 10) = 9/18 = 1/2 \). Therefore \( (3x - 15)/(x^2 - 7x + 10) = 1/2 \) if and only if \( x = 8 \).

2.30 Remark. In the preceding example, we have seen that the conditional sentence
\[ \text{If } (3x - 15)/(x^2 - 7x + 10) = 1/2, \text{ then } x = 5 \text{ or } x = 8 \]
is true no matter what real number the variable \( x \) stands for. For instance, it is true when \( x = 5 \), in which case the antecedent is false and the consequent is true, and it is true when \( x = 4 \), in which case the antecedent and consequent are both false.

Exercise 19. Consider the following calculation:
\[ x = \sqrt{x + 2} \]
\[ x^2 = x + 2 \]
\[ x^2 - x - 2 = 0 \]
\[ (x + 1)(x - 2) = 0 \]
x = -1, 2
Is \( x = -1 \) a solution of the original equation? Solve the equation \( x = \sqrt{x + 2} \) correctly. Your solution should include words to express the logic involved.
Exercise 20.

(a) Solve the equation \( \frac{3x - 15}{x^2 - 7x + 10} = 1 \).

You should write your answer in a way that shows that you understand the point of Example 2.29 and Exercise 19.

(b) Solve the equation \( \frac{3}{x - 2} = 1 \).

The instruction at the end of part (a) applies here too.

(c) Notice that \( \frac{3x - 15}{x^2 - 7x + 10} = \frac{3(x - 5)}{(x - 2)(x - 5)} \).

Does it follow from this that the equations in parts (a) and (b) have the same solutions? If not, then why not? Be careful! Many students give the wrong answer at first. (Hint: For which values of \( x \) is the equation \( \frac{3(x - 5)}{(x - 2)(x - 5)} = \frac{3}{x - 2} \) true?)

More about Conditional Sentences.

2.31 Example. Let \( A \) be the sentence \( Q \Rightarrow (P \Rightarrow Q) \). We saw in Exercise 16 that \( A \) is a tautology. Let \( B \) be the converse of \( A \). Then \( B \) is the sentence \( (P \Rightarrow Q) \Rightarrow Q \). Let us show that \( B \) is not a tautology. We could see this just by writing out a truth table. However, it will be more instructive to proceed as follows.

Suppose that \( B \) is false. Let’s see what this tells us about the truth values of \( P \) and \( Q \). Recall that \( B \) is the sentence \( (P \Rightarrow Q) \Rightarrow Q \). Since \( B \) is false, \( P \Rightarrow Q \) is true and \( Q \) is false. Since \( Q \) is false and \( P \Rightarrow Q \) is true, \( P \) is false. This shows that the only way \( B \) can be false is if \( P \) and \( Q \) are both false. To show that \( B \) is not a tautology, it remains to show that if \( P \) and \( Q \) are both false, then \( B \) actually is false.

So conversely, suppose \( P \) is false and \( Q \) is false. Then \( P \Rightarrow Q \) is true, so \( (P \Rightarrow Q) \Rightarrow Q \) is false. Thus we have found a combination of truth values for \( P \) and \( Q \) that makes \( B \) false. Therefore \( B \) is not a tautology.

Exercise 21. Let \( A \) be the sentence \( [(P \Rightarrow Q) \land (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R) \). We have seen in Example 2.25 that \( A \) is a tautology. Let \( B \) be the converse of \( A \). Write out what \( B \) is in terms of \( P \), \( Q \), and \( R \). Then show that \( B \) is not a tautology, by finding a combination of truth values for \( P \), \( Q \), and \( R \) that makes \( B \) false. You should be able to do this without writing out a truth table.

Exercise 22. Let \( A \) be the sentence \( (P \Rightarrow Q) \Rightarrow \{[(P \Rightarrow (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)]\} \). We saw in Exercise 17 that \( A \) is a tautology. Let \( B \) be the converse of \( A \). Write out what \( B \) is in terms of \( P \), \( Q \), and \( R \). Then show that \( B \) is not a tautology, by finding a combination of truth values for \( P \), \( Q \), and \( R \) that makes \( B \) false. You should be able to do this without writing out a truth table.

Contradictions.

A contradiction is a sentence of the form \( Q \land \neg Q \). Such a sentence is false whatever the truth value of \( Q \) may be. (Proof: Either \( Q \) is true or \( Q \) is false. If \( Q \) is true, then \( \neg Q \) is false, so \( Q \land \neg Q \) is false. If \( Q \) is false, then \( Q \land \neg Q \) is false. Thus in either case, \( Q \land \neg Q \) is false.)

Copyright Neil Falkner, December 17, 2021
How To Prove a Negative Sentence.

The usual way to prove a negative sentence \( \neg P \) is to assume \( P \) and to deduce a contradiction from this assumption. We shall now explain why this works. Let us begin by introducing a new logical symbol, \( \neg \). The symbol \( \neg \) may be read “falsehood” and should be thought of as standing for a false sentence. (For instance, \( \neg \) might stand for a contradiction \( Q \land \neg Q \).) As the following truth table shows, \( P \Rightarrow \neg P \) has the same truth value as \( \neg P \):

<table>
<thead>
<tr>
<th>( P )</th>
<th>( \neg P )</th>
<th>( P \Rightarrow \neg P )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( T )</td>
<td>( F )</td>
<td>( F )</td>
</tr>
<tr>
<td>( F )</td>
<td>( F )</td>
<td>( T )</td>
</tr>
</tbody>
</table>

Now if we assume \( P \) and deduce a contradiction \( Q \land \neg Q \), then by the method of conditional proof, the conditional sentence \( P \Rightarrow (Q \land \neg Q) \) is true, so as the truth table (13) shows, the negative sentence \( \neg P \) must be true.

Exercise 23. Use the method of conditional proof to explain in words why the sentence

\[
[(P \Rightarrow Q) \land \neg Q] \Rightarrow \neg P
\]

is a tautology.\(^{18}\) (Do not use cases.) The way to prove a negative sentence, in this case \( \neg P \), should also play a role in your proof. Be careful not to skip any steps. Be explicit about discharging assumptions.

Proof by Contradiction.

In the method of proof by contradiction, we prove a given sentence \( P \) in the following way: Assume \( \neg P \) and deduce a contradiction \( Q \land \neg Q \). This shows that \( (\neg P) \Rightarrow (Q \land \neg Q) \) is true, so \( \neg \neg P \) must be true, by the truth table (13) (with \( P \) replaced by \( \neg P \)). But \( \neg \neg P \) is logically equivalent to \( P \). Hence \( P \) must be true.

2.32 Example. Let \( x \) be an integer. We shall illustrate the method of proof by contradiction by using it in the course of proving the sentence

If \( x^2 \) is an even number, then \( x \) is an even number. \( \neg P \)

(14)

The sentence (14) is a conditional sentence and to prove it, we begin in the usual way, by assuming the antecedent and endeavouring to prove the consequent. In other words, we assume that \( x^2 \) is an even number and we wish to prove that \( x \) is an even number. Now we shall use proof by contradiction to prove that \( x \) is an even number. Suppose that \( x \) is not an even number. Then, since \( x \) is an integer, \( x \) must be an odd number. But then \( x^2 \) is an odd number, so \( x^2 \) is not an even number. Thus we are led to the conclusion that \( x^2 \) is both an even number and not an even number. This is a contradiction. Hence we must reject our assumption that \( x \) is not an even number, so we conclude that indeed \( x \) is an even number. We have proved this under the assumption that \( x^2 \) is an even number. Discharging this assumption, we conclude that the conditional sentence (14) is true.

The Contrapositive of a Conditional Sentence.

Given a conditional sentence \( P \Rightarrow Q \), the related conditional sentence \( \neg Q \Rightarrow \neg P \) is called the contrapositive of \( P \Rightarrow Q \). A conditional sentence and its contrapositive are logically equivalent, as the following truth table shows:

<table>
<thead>
<tr>
<th>( P )</th>
<th>( Q )</th>
<th>( P \Rightarrow Q )</th>
<th>( \neg Q )</th>
<th>( \neg P )</th>
<th>( \neg Q \Rightarrow \neg P )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
<td>( F )</td>
<td>( F )</td>
<td>( T )</td>
</tr>
<tr>
<td>( T )</td>
<td>( F )</td>
<td>( F )</td>
<td>( T )</td>
<td>( F )</td>
<td>( F )</td>
</tr>
<tr>
<td>( F )</td>
<td>( T )</td>
<td>( T )</td>
<td>( F )</td>
<td>( T )</td>
<td>( T )</td>
</tr>
<tr>
<td>( F )</td>
<td>( F )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
</tr>
</tbody>
</table>

It is important not to confuse the contrapositive of \( P \Rightarrow Q \) with the converse of \( P \Rightarrow Q \). The contrapositive of \( P \Rightarrow Q \) is \( \neg Q \Rightarrow \neg P \). The converse of \( P \Rightarrow Q \) is \( Q \Rightarrow P \). The contrapositive, \( \neg Q \Rightarrow \neg P \), is logically equivalent to \( P \Rightarrow Q \), but the converse, \( Q \Rightarrow P \), is not.

\(^{18}\) By the way, this tautology is called \textit{modus tollens}. Actually, the full name for this tautology is \textit{modus tollendo tollens}, which is latin for “the way to deny by denying.”
Exercise 24. Let $A$ be the conditional sentence

$$\text{If } x = 2 \text{ and } y = 3, \text{ then } xy = 6.$$  

(a) Write out the contrapositive of $A$ in words. Is the contrapositive of $A$ true?

(b) Write out the converse of $A$ in words. Is the converse of $A$ true, or is it impossible to say without further information about the specific values of $x$ and $y$? (Hint: Can you find specific values for $x$ and $y$ for which the converse of $A$ is true? If so, give an example of such values. Can you find other specific values for $x$ and $y$ for which the converse of $A$ is false? If so, give an example of such values.)

Proof by Contraposition.

The logical equivalence of $P \implies Q$ with $\neg Q \implies \neg P$ is the basis for the method of proof by contraposition: To prove $P \implies Q$, it suffices to prove $\neg Q \implies \neg P$.

2.33 Example. Let $x$ be an integer. We shall illustrate the method of proof by contraposition by using it to prove the conditional sentence (14) that we already considered in Example 2.32. Any conditional sentence is logically equivalent to its contrapositive, so the sentence (14) is logically equivalent to the sentence

$$\text{If } x \text{ is not an even number, then } x^2 \text{ is not an even number.} \tag{15}$$

Hence it suffices to prove (15). The sentence (15) is a conditional sentence and to prove it, we begin in the usual way, by assuming the antecedent and endeavouring to prove the consequent. In other words, we assume that $x$ is not an even number and we wish to prove that $x^2$ is not an even number. Since $x$ is an integer but $x$ is not an even number, $x$ is an odd number. Hence $x^2$ is an odd number, so $x^2$ is not an even number. We have proved this under the assumption that $x$ is not an even number. Discharging this assumption, we conclude that the conditional sentence (15) is true. This completes the proof by contraposition that the conditional sentence (14) is true.

Proof by Contraposition Compared with Proof by Contradiction.

Evidently Example 2.33, on proof by contraposition, and Example 2.32, on proof by contradiction, are similar. In fact, quite generally, proof by contraposition may be regarded as an abbreviated form of a special type of proof by contradiction. To explain this, suppose we wish to prove $P \implies Q$. The standard way to begin is to assume $P$ and try to prove $Q$. If we do not see how to prove $Q$ directly, then we may assume $\neg Q$ in addition, and try to derive a contradiction. Having assumed $P$ and $\neg Q$, suppose that we happen to deduce $\neg P$. Then we have the contradiction $P \land \neg P$, so we conclude that $\neg Q$ cannot be true, so $Q$ must be true, so we have proved $P \implies Q$. But suppose our deduction of $\neg P$ did not use our assumption $P$. Then our argument can be shortened by assuming just $\neg Q$, deducing $\neg P$, and then concluding by conditional proof that $\neg Q \implies \neg P$ is true, so by contraposition, $P \implies Q$ is true.

Still More about Conditional Sentences (Optional).

It can be shown that the sentence $(P \land Q) \implies R$ is logically equivalent to the sentence $(P \implies R) \lor (Q \implies R)$, and the sentence $(P \lor Q) \implies R$ is logically equivalent to the sentence $(P \implies R) \land (Q \implies R)$. In fact, the truth table (13) makes it possible to recognize these two logical equivalences as a disguised form of De Morgan’s laws. We shall now prove the first of these equivalences. The second we leave as an exercise.

2.34 Example. Show by means of an explanation in words that the sentence $(P \land Q) \implies R$ is logically equivalent to the sentence $(P \implies R) \lor (Q \implies R)$.

Solution. Either $R$ is false or $R$ is true.\(^{19}\)

\(^{19}\) We consider the case where $R$ is false first because it is the more interesting case.
Case 1. Suppose $R$ is false. Then for any sentence $A$, the sentence $A \Rightarrow R$ has the same truth value as the sentence $\neg A$. Hence $(P \land Q) \Rightarrow R$ has the same truth value as $\neg(P \land Q)$. Similarly, $(P \Rightarrow R) \lor (Q \Rightarrow R)$ has the same truth value as $\neg P \lor \neg Q$. But by one of De Morgan’s laws, $\neg(P \land Q)$ has the same truth value as $\neg P \lor \neg Q$. Hence $(P \land Q) \Rightarrow R$ has the same truth value as $(P \Rightarrow R) \lor (Q \Rightarrow R)$.

Case 2. Suppose $R$ is true. Then for any sentence $A$, the sentence $A \Rightarrow R$ is true. Hence the sentences $(P \land Q) \Rightarrow R$ and $(P \Rightarrow R) \lor (Q \Rightarrow R)$ are both true, so they have the same truth value.

Thus in either case, the sentences $(P \land Q) \Rightarrow R$ and $(P \Rightarrow R) \lor (Q \Rightarrow R)$ have the same truth value. Therefore they are logically equivalent.

**Exercise 25.** Show by means of an explanation in words that the sentence $(P \lor Q) \Rightarrow R$ is logically equivalent to the sentence $(P \Rightarrow R) \land (Q \Rightarrow R)$.

In Example 2.34, we saw that $(P \land Q) \Rightarrow R$ is logically equivalent to $(P \Rightarrow R) \lor (Q \Rightarrow R)$. The next exercise is concerned with another sentence that $(P \land Q) \Rightarrow R$ is logically equivalent to.

**Exercise 26.** Show by means of an explanation in words that $(P \land Q) \Rightarrow R$ is logically equivalent to $P \Rightarrow (Q \Rightarrow R)$.

By the way, the fact that $(P \land Q) \Rightarrow R$ implies $P \Rightarrow (Q \Rightarrow R)$ is known as the law of exportation. The fact that $P \Rightarrow (Q \Rightarrow R)$ implies $(P \land Q) \Rightarrow R$ is known as the law of importation.

**Exercise 27.** Show by means of an explanation in words that $P \Rightarrow (Q \Rightarrow R)$ is logically equivalent to $Q \Rightarrow (P \Rightarrow R)$. (Use Exercise 26.)

**Exercise 28.** Show by means of an explanation in words that:

(a) $P \Rightarrow (Q \land R)$ is logically equivalent to $(P \Rightarrow Q) \land (P \Rightarrow R)$.

(b) $P \Rightarrow (Q \lor R)$ is logically equivalent to $(P \Rightarrow Q) \lor (P \Rightarrow R)$.

(c) $P \Rightarrow (Q \Rightarrow R)$ is logically equivalent to $(P \Rightarrow Q) \Rightarrow (P \Rightarrow R)$.

**Exercise 29.** The results of Exercise 28 may be described by saying that $\Rightarrow$ is “left-distributive” over $\land$, $\lor$, and $\Rightarrow$ respectively. Show that $\Rightarrow$ is not “right-distributive” over any of $\land$, $\lor$, or $\Rightarrow$. (Suggestion: For each part, it suffices to find one choice of truth values for $P$, $Q$, and $R$ for which the two sentences in question have different truth values. You should not need to write out any truth tables in full. See the hint for Exercise 11 for a fuller explanation of what this suggestion means.)

**Truth Functions and General Logical Connectives (Optional).** We have defined the basic logical connectives $\neg$, $\land$, $\lor$, $\Rightarrow$, and $\Leftrightarrow$ by truth functions. By this we mean, for instance, that the truth value of $\neg P$ is a function of the truth value of $P$. In other words, given the truth value of $P$, we can work out the truth value of $\neg P$. The truth table for $\neg$ tells us how to do this. Similarly, the truth value of $P \land Q$ is a function of the truth values of $P$ and $Q$. Given the truth values of $P$ and $Q$, the truth table for $\land$ tells us how find the truth value of $P \land Q$. The connective $\neg$ is called a unary logical connective because it is defined by a truth function of a single propositional variable $P$. The connectives $\land$, $\lor$, $\Rightarrow$, and $\Leftrightarrow$ are called binary logical connectives because each of them is defined by a truth function of two propositional variables $P$ and $Q$. But these are only four out of 16 possibilities for a binary logical connective. Since there are $2^4 = 16$ ways to fill in a column of 4 truth values, there are 16 different truth functions of two propositional variables. They are shown in the following table, which has been broken into two parts because...

---

20 We do not say yet that the sentences $(P \land Q) \Rightarrow R$ and $(P \Rightarrow R) \lor (Q \Rightarrow R)$ are logically equivalent, because to say this means that they have the same truth value, no matter what truth values $P$, $Q$, and $R$ have. We will not know this until the end of the proof.
Some of these 16 truth functions do not really depend on both of the propositional variables \( P \) and \( Q \). For instance, the first one is just \( P \) itself and the last one is identically false. (The ones that do depend on both propositional variables are the five connectives \( \land, \lor, \Rightarrow, \iff, \equiv \), and their five negations.) As the table shows, all 16 of these truth functions can be expressed in terms of \( P, Q \), and the connectives \( \neg, \land, \lor, \Rightarrow, \iff \). Note that a given truth function may be expressible in more than one such way. For instance \( \neg(P \land Q) \) is logically equivalent to \((\neg P) \lor (\neg Q)\), as we know from the first of De Morgan’s laws. The essence of a truth function, or logical connective, is not any such particular way of expressing it. Rather, its essence is its truth table.

**Exercise 30.** Since there are \( 2^2 = 4 \) ways to fill in a column of two truth values, there are 4 different truth functions of a single propositional variable \( P \). Write out a table that shows these 4 truth functions and that also shows a way in which each of them may be expressed in terms of \( P, \neg, \land, \lor \).

**Exercise 31.** Show by means of a truth table that \( P \Rightarrow Q \) is logically equivalent to \((\neg P) \lor Q\).

In general, an \( n \)-ary logical connective would be defined by a truth function of \( n \) propositional variables \( P_1, \ldots, P_n \). It turns out that any such truth function can be expressed in terms of \( P_1, \ldots, P_n, \neg, \land, \lor, \Rightarrow, \iff \). Consider, for instance, suppose \( f(P, Q, R) \) is a truth function of three propositional variables \( P, Q, \land, \lor \). Then \( f(P, Q, R) \) is logically equivalent to \( f(P, Q, T) \lor f(P, Q, F) \). Now \( f(P, Q, T) \) and \( f(P, Q, F) \) are truth functions of two propositional variables \( P \) and \( Q \), so they can be expressed in terms of \( P, Q, \neg, \land, \lor, \Rightarrow, \iff \). Thus the basic logical connectives \( \neg, \land, \lor, \Rightarrow \text{ and } \iff \) are actually sufficient to express any imaginable truth function of any finite number of propositional variables. In fact, not even all of these basic connectives are needed (although this is not very important for understanding mathematical proofs). First of all, \( \iff \) is clearly not needed because it can be expressed in terms of \( \Rightarrow \text{ and } \land: P \iff Q \) is logically equivalent to \( (P \Rightarrow Q) \land (Q \Rightarrow P) \). Next, \( \lor \text{ and } \Rightarrow \) can both be expressed in terms of \( \neg \text{ and } \land: P \lor Q \) is logically equivalent to \((\neg P) \land (\neg Q)\) and, as you were asked to show in Exercise 31, \( P \Rightarrow Q \) is logically equivalent to \((\neg P) \lor Q\). One can also show that \( \land \text{ and } \Rightarrow \) can both be expressed in terms of \( \neg \text{ and } \lor \), and that \( \land \text{ and } \lor \) can be expressed in terms of \( \neg \text{ and } \Rightarrow \). It follows that any truth function \( f(P_1, \ldots, P_n) \) can be expressed in terms of \( P_1, \ldots, P_n, \neg, \land, \lor, \Rightarrow \text{ and } \iff \).

**Exercise 32.** Explain how \( P \land Q \) and \( P \lor Q \) may be expressed in terms of \( P, Q, \neg, \land, \lor \).

2.35 **Remark: The Sheffer Stroke.** As we’ve seen, any logical connective in any number of variables can be expressed in terms of the unary logical connective \( \neg \) and any one of the binary logical connectives \( \land, \lor, \Rightarrow \text{ or } \iff \). There is even a single binary logical connective in terms of which any logical connective can be expressed. One example of such a binary logical connective is the Sheffer stroke, commonly denoted by \( | \), defined by \( (P \mid Q) \equiv (\neg(P \land Q)) \). In view of what we have seen above, to show that any logical connective can be expressed in terms of \( | \), all we need do is verify that \( \neg \text{ and } \land \text{ can be expressed in terms of } | \). This is easily done. Just observe that

\[
\neg P \equiv \neg(P \land Q) \equiv (P \mid P)
\]
and
\[(P \land Q) \equiv \neg \neg (P \land Q) \equiv ((P \mid Q) \mid (P \mid Q)).\]

The fact that any logical connective can be expressed in terms of | is of little importance in understanding mathematical proofs but it is useful in the design of digital circuits, which are used in computers and many other modern products, since it means that any type of electronic “logical gate” can be constructed by connecting together sufficiently many “nand gates” in a suitable way. (The term “nand gate” reflects the fact that \(P \mid Q\) is logically equivalent to not(P and Q). The word “nand” is short for “not and.”) If this sounds like gibberish to you, don’t worry. If you study digital circuit design, it will be explained in more detail.

The next example and two exercises give more insight into why \(\Rightarrow\) is defined the way it is in logic.

2.36 Example. Let \(\ast\) be a binary logical connective that makes \((R \land S) \ast R\) a tautology.

(a) Show that \(P \ast Q\) must be true whenever \(P\) is false.

(b) A trivial way to make \((R \land S) \ast R\) be a tautology would be to make \(P \ast Q\) always true. Suppose we rule out this trivial choice of \(\ast\). In other words, suppose in addition that \(P \ast Q\) is not always true. Show that then \(\ast\) is \(\Rightarrow\). In other words, show that the truth table for \(\ast\) is the same as the truth table for \(\Rightarrow\).

Solution. (a) First, if \(R\) is \(T\) and \(S\) is \(F\), then \((R \land S) \ast R\) is \(F\) because \((\ast T) \ast T\) is \(T\). But since \((R \land S) \ast R\) is a tautology, \((R \land S) \ast R\) is \(T\). Thus \(F \ast T\) is \(T\). Next, if \(R\) is \(F\) and \(S\) is \(F\), then again \((R \land S) \ast R\) is \(F \ast F\). As before, since \((R \land S) \ast R\) is a tautology, \((R \land S) \ast R\) is \(T\). Thus \(F \ast F\) is \(T\). Therefore \(P \ast Q\) must be true whenever \(P\) is false.

(b) If \(R\) is \(T\) and \(S\) is \(T\), then \((R \land S) \ast R\) is \(T \ast T\). But once again, since \((R \land S) \ast R\) is a tautology, \((R \land S) \ast R\) is \(T\). Thus \(F \ast T\) is \(T\). As we saw in (a), \(F \ast T\) is \(T\) and \(F \ast F\) is \(T\). Since \(P \ast Q\) is not always true, it must be that \(T \ast F\) is \(F\). To summarize, \(P \ast Q\) is \(F\) when \(P\) is \(T\) and \(Q\) is \(F\), but otherwise \(P \ast Q\) is \(T\). Thus \(\ast\) is \(\Rightarrow\).

Exercise 33. Let \(\ast\) be a binary logical connective that makes \(R \ast (R \lor S)\) a tautology.

(a) Show that \(P \ast Q\) must be true whenever \(P\) is false.

(b) A trivial way to make \(R \ast (R \lor S)\) be a tautology would be to make \(P \ast Q\) always true. Suppose we rule out this trivial choice of \(\ast\). In other words, suppose in addition that \(P \ast Q\) is not always true. Show that then \(\ast\) is \(\Rightarrow\). In other words, show that the truth table for \(\ast\) is the same as the truth table for \(\Rightarrow\).

2.37 Remark. By similar methods, one can show that if \(\ast\) is a binary connective that makes any one of \((R \land S) \ast S\), \(S \ast (R \lor S)\), or \((R \land S) \ast (R \lor S)\) a tautology, then \(P \ast Q\) must be true whenever \(P\) is false, and if in addition \(P \ast Q\) is not always true, then \(\ast\) is \(\Rightarrow\).

2.38 Remark. Let \(\ast\) be a binary logical connective. In Theorem 2.17, we saw that \((P \Rightarrow Q) \land (Q \Rightarrow P)\) is logically equivalent to \(P \iff Q\). Similarly, it is easy to see that \((P \iff Q) \land (Q \iff P)\) is logically equivalent to \(P \iff Q\). Finally, it should be obvious that \((P \iff Q) \land (Q \iff P)\) is logically equivalent to \(P \iff Q\). Thus if \(\ast\) is \(\Rightarrow\), or if \(\ast\) is \(\iff\), or if \(\ast\) is \(\iff\), then \((P \ast Q) \land (Q \ast P)\) is logically equivalent to \(P \iff Q\). In part (a) of the next exercise, you are asked to prove the converse of this.

Exercise 34. Let \(\ast\) be a binary logical connective that makes \((P \ast Q) \land (Q \ast P)\) logically equivalent to \(P \iff Q\).

(a) Show that \(\ast\) is \(\Rightarrow\), or \(\ast\) is \(\iff\), or \(\ast\) is \(\iff\). In other words, show that the truth table for \(\ast\) is the same as the truth table for \(\Rightarrow\), or the truth table for \(\iff\), or the truth table for \(\iff\). (Warning: In my experience, many students do not solve this exercise correctly. Instead, they prove the converse of what is asked. In other words, they just reprove the facts that are pointed out in Remark 2.38. You should be careful to avoid this error. Hint: First determine \(T \ast T\). Then determine \(F \ast F\). Then figure out as much as you can about \(T \ast F\) and \(F \ast T\).)

(b) Now suppose in addition that \(\ast\) makes \((R \land S) \ast R\) a tautology. Show that then \(\ast\) is \(\Rightarrow\). In other words, show that the truth table for \(\ast\) is the same as the truth table for \(\Rightarrow\). (The warning for part (a) applies here too. Hint: Combine part (a) of this exercise with Example 2.36(a))
Section 3. Quantifiers

Besides the logical connectives, which were discussed in the previous section, the other main ingredients of modern symbolic logic are the quantifiers $\forall$ and $\exists$. These correspond to the phrases “for each” and “for some” respectively and as we shall see, they may be viewed as generalizations of $\land$ and $\lor$.

3.1 Example. Suppose $P(x)$ stands for the sentence “$x$ likes chocolate.” Then $(\forall x)P(x)$ stands for the sentence “For each $x$, $x$ likes chocolate.” In other words, “Everybody likes chocolate.” Similarly, $(\exists x)P(x)$ stands for the sentence “For some $x$, $x$ likes chocolate.” In other words, “Somebody likes chocolate.”

This section will expose you to the basic ideas that are relevant to understanding quantifiers. However, it may be well to say at the outset that most students need a lot of practice to master the use of quantifiers. One reason for this is that most interesting mathematical sentences have several quantifiers in them, not just one. You should not expect to understand everything about quantifiers at the end of this section. It is normal for your understanding of quantifiers to grow gradually, through experience with learning definitions and reading and writing proofs.

There are a number of ways to read $(\forall x)P(x)$, besides “For each $x$, $P(x)$.” Some of these are:

- For all $x$, $P(x)$.
- For every $x$, $P(x)$.
- For any $x$, $P(x)$.

Thus in logic, the phrases “for every” and “for any” always mean the same thing. In contrast, in ordinary English, the modifiers “every” and “any” sometimes mean the same thing and sometimes mean very different things. On the one hand, “Everybody can do that” means the same thing as “Anybody can do that.” On the other hand, “If everybody passes the course, we’ll celebrate” means something quite different from “If anybody passes the course, we’ll celebrate.”

There are also several ways to read $(\exists x)P(x)$, besides “For some $x$, $P(x)$.” Some of these are:

- For at least one $x$, $P(x)$.
- There exists $x$ such that $P(x)$.

In fact, “There exists $x$ such that $P(x)$” is the most common way to read $(\exists x)P(x)$. Note that $(\exists x)$ may be considered to stand for the whole phrase “there exists $x$ such that.” It would be redundant to write “$(\exists x)$ such that $P(x)$.”

The symbol $\forall$ is called the universal quantifier. A sentence of the form $(\forall x)P(x)$ is called a universal sentence. The symbol $\exists$ is called the existential quantifier. A sentence of the form $(\exists x)P(x)$ is called an existential sentence.

Notice that the variable $x$ in $(\forall x)P(x)$ and in $(\exists x)P(x)$ should be thought of as ranging over some collection which is called the universe of discourse. The sentence $(\forall x)P(x)$ is considered to be true when $P(x)$ is true for all values of $x$ in the universe of discourse. The sentence $(\exists x)P(x)$ is considered to be true when $P(x)$ is true for at least one value of $x$ in the universe of discourse. In Example 3.1, the universe of discourse is understood to be a collection of people and the words “everybody” and “somebody” mean respectively everybody in the collection of people under consideration and somebody in that collection.

In other examples, the universe of discourse may be some other collection. It is a good idea to explicitly mention what the universe of discourse is supposed to be, if this is not clear from the context.

The objects that belong to a given collection $A$ are called the members or elements of $A$. If $A$ is a collection and $x$ is an object, we write $x \in A$ to mean $x$ is an element of $A$, and we write $x \notin A$ to mean $x$ is not an element of $A$. A short way to read the notation $x \in A$ is “$x$ is in $A$.”

In mathematical examples, the universe of discourse is usually a collection of mathematical objects. There are standard names and notations for the collections that arise most frequently in mathematical discussions. Let us list some of these now. The notation $\{1, 2, 3, \ldots\}$ stands for the collection whose members or elements are the natural numbers 1, 2, 3, and so on. This collection, the set of natural numbers, is denoted by the boldface letter $\mathbf{N}$. The notation $\{1, 2, 3, \ldots, n\}$ stands for the collection whose
Section 3. Quantifiers

elements are the natural numbers from 1 up to and including \( n \), it being understood that \( n \) is a natural number. Note that \( \{1, 2, 3, \ldots, n\} \) is different from \( \mathbb{N} \). The former collection stops at \( n \) whereas the latter goes on forever. Sometimes one writes \( \mathbb{N} = \{1, 2, 3, \ldots, n, \ldots\} \) to emphasize this. By the way, \( \infty \) is not considered to be an element of \( \mathbb{N} \). There is no largest natural number. Instead, each natural number is followed by another strictly larger natural number. We should mention that some authors include 0 among the natural numbers. However, we shall not do this. Instead, we shall refer to the numbers 0, 1, 2, 3, and so on, as *whole numbers*, and we shall use the boldface Greek letter \( \omega \) to denote the collection \( \{0, 1, 2, \ldots\} \) of whole numbers.\(^{21}\) Note that \( \infty \) is not considered to be an element of \( \omega \). The notation \( \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} \) stands for the collection whose elements are the *integers*, whether positive, negative, or zero. This collection, the set of integers, is denoted by the boldface letter \( \mathbb{Z} \). (This may be from the first letter of the German word *Zahlen*, which means *numbers*.) Recall that a number is said to be *rational* when it is a quotient \( m/n \) of two integers \( m \) and \( n \) where of course \( n \neq 0 \). For instance, \( 2/3 \) and \(-146/62\) are rational numbers, and 12 is a rational number because \( 12 = 12/1 \). Notice that each integer is a rational number, but there are many rational numbers that are not integers. It is customary to use the boldface letter \( \mathbb{Q} \) to denote the set of rational numbers. (This is from the first letter of the word *quotient*.)

The boldface letter \( \mathbb{R} \) denotes the set of real numbers. Each rational number is a real number, but there are many real numbers that are not rational numbers. For instance, \( \sqrt{2} \) is not a rational number. (We shall review the proof of this later.) Each real number can be represented by a decimal expansion. It turns out that a real number is rational if and only if it can be represented by a decimal expansion that either terminates or repeats. But there are many real numbers that are not rational. The decimal expansions of these real numbers appear random and do not terminate or repeat. This suggests that in fact, most real numbers are not rational. We shall see a way to make this precise later, when we discuss how to compare the numbers of elements in different infinite sets. By the way, \( -\infty \) and \( \infty \) are not considered to be elements of \( \mathbb{Z} \), \( \mathbb{Q} \), or \( \mathbb{R} \). Finally, the boldface letter \( \mathbb{C} \) denotes the set of complex numbers.\(^{22}\) Recall that the complex numbers are the numbers of the form \( x + iy \) where \( x \) and \( y \) are real numbers and \( i = \sqrt{-1} \).

### 3.2 Example

Let the universe of discourse be the set of people \( \{ \text{Jack, Jill} \} \). Once again, let \( P(x) \) stand for the sentence “\( x \) likes chocolate.” Then \( (\forall x)P(x) \) is considered to be true when \( P(x) \) is true for all values of \( x \) in the set \( \{ \text{Jack, Jill} \} \). Thus \( (\forall x)P(x) \) is true exactly when \( P(\text{Jack}) \land P(\text{Jill}) \) is true; in other words, exactly when Jack likes chocolate and Jill likes chocolate. Similarly, \( (\exists x)P(x) \) is considered to be true when \( P(x) \) is true for at least one value of \( x \) in the set \( \{ \text{Jack, Jill} \} \). Thus \( (\exists x)P(x) \) is true exactly when \( P(\text{Jack}) \lor P(\text{Jill}) \) is true; in other words, exactly when Jack likes chocolate or Jill likes chocolate.

As Example 3.2 suggests, if the universe of discourse is a set with two elements, or more generally, if the universe of discourse is a specific finite set, then one can get along without quantifiers, by using \( \land \) and \( \lor \) instead. To mention another example, if the universe of discourse is the set \( \{2, 3, 5\} \), then \( (\forall x)P(x) \) has the same truth value as \( P(2) \land P(3) \land P(5) \), and \( (\exists x)P(x) \) has the same truth value as \( P(2) \lor P(3) \lor P(5) \). Although quantifiers are not essential when the universe of discourse is a specific finite set, their use can save writing. But if the universe of discourse is an infinite set, then we really need quantifiers. For instance, if the universe of discourse is the set \( \mathbb{N} = \{1, 2, 3, \ldots\} \) of natural numbers, then \( (\forall x)P(x) \) may be thought of as representing the infinitely long sentence

\[
P(1) \land P(2) \land P(3) \land \cdots
\]

and \( (\exists x)P(x) \) may be thought of as representing the infinitely long sentence

\[
P(1) \lor P(2) \lor P(3) \lor \cdots.
\]

---

\(^{21}\) You should take care to write \( \omega \) and \( w \) differently. The symbol \( w \) is our letter “double-you.” The symbol \( \omega \) is “omega,” the last letter of the Greek alphabet. It is one of the two letters for “o” in Greek. Classical Greek used \( \omega \) to represent a long “o” sound, like “o” in cone, and a different letter \( o \), called “omicron,” to represent a short “o” sound like “o” in “on.” In fact, the names “omega” and “omicron” literally mean “long o” and “short o.” The word “mega” means “big” or “long,” while the word “micron” means “small” or “short.”

\(^{22}\) In your handwritten work, you should not use ordinary capital letters \( N, Z, Q, R, \) and \( C \) to mean \( \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \) and \( \mathbb{C} \). Instead, you should indicate somehow that \( N, Z, Q, R, \) and \( C \) are boldface capital letters. One way to do this is to write them something like \( \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \) and \( \mathbb{C} \). (You might ask your teacher to show you how to write these letters efficiently.) Then the ordinary capital letters \( N, Z, Q, R, \) and \( C \) will remain at your disposal for use as variables.
If the universe of discourse is the set $\mathbb{R}$ of all real numbers, then these ways of thinking of the sentences $(\forall x)P(x)$ and $(\exists x)P(x)$ cannot be taken literally because there is no way to list all the real numbers, even in a list of infinite length. Nevertheless, it makes good sense to say that something is true for all real numbers, or that it is true for at least one real number. For instance, it is true that $(\forall x \in \mathbb{R})[(x + 2)^2 = x^2 + 4x + 4]$ and it is also true that $(\exists x \in \mathbb{R})(x^2 + 5 = 9)$.

Suppose $A$ is a subcollection of the universe of discourse. Then the sentence $(\forall x)[(x \in A) \Rightarrow P(x)]$ is true exactly when the sentence $(x \in A) \Rightarrow P(x)$ is true for all values of $x$ in the universe of discourse. But this happens exactly when the sentence $P(x)$ is true for all values of $x$ in $A$.\footnote{For each value of $x$ that is not in $A$, the sentence $(x \in A) \Rightarrow P(x)$ is true for the trivial reason that the sentence $x \in A$ is false.} Accordingly, we write $(\forall x \in A)P(x)$ as an abbreviation for $(\forall x)[(x \in A) \Rightarrow P(x)]$. Also, the sentence $(\exists x)[(x \in A) \land P(x)]$ is true exactly when the sentence $(x \in A) \land P(x)$ is true for at least one value of $x$ in the universe of discourse. But clearly this happens exactly when the sentence $P(x)$ is true for at least one value of $x$ in $A$. Accordingly, we write $(\exists x \in A)P(x)$ as an abbreviation for $(\exists x)[(x \in A) \land P(x)]$.

The notations $(\forall x > 0)P(x)$ and $(\exists x > 0)P(x)$ may be regarded as special cases of the notation discussed in the preceding paragraph. The sentence $(\forall x > 0)P(x)$ is considered to be true exactly when $P(x)$ is true for all values of $x$ in the collection of strictly positive real numbers. Likewise, the sentence $(\exists x > 0)P(x)$ is considered to be true exactly when $P(x)$ is true for at least one value of $x$ in the collection of strictly positive real numbers. As one more example, the sentence $(\forall x \leq 5)P(x)$ is considered to be true exactly when $P(x)$ is true for all values of $x$ in the set of real numbers that are less than or equal to 5.

### 3.3 Example

For each of the following sentences, write out what it means in words, state whether it is true or false, and prove your statement.

- **(a)** $(\exists x \in \mathbb{R})(x + 2 = 5)$.
- **(b)** $(\forall x \in \mathbb{R})(x + 2 = 5)$.
- **(c)** $(\exists x < 0)(x + 2 = 5)$.
- **(d)** $(\forall x \in \mathbb{R})(x^2 + 4x + 5 > 0)$.
- **(e)** $(\exists x \in \mathbb{R})(x^2 + 4x + 2 = 0)$.

**Solution.**

(a) The sentence $(\exists x \in \mathbb{R})(x + 2 = 5)$ means “There exists a real number $x$ such that $x + 2$ is equal to 5.” This sentence is true, because for instance, 3 is a real number and $3 + 2 = 5$. (In other words, the sentence $(\exists x \in \mathbb{R})(x + 2 = 5)$ is true because 3 is an example of a value of $x$ that belongs to $\mathbb{R}$ such that $x + 2 = 5$.)

(b) The sentence $(\forall x \in \mathbb{R})(x + 2 = 5)$ means “For each real number $x$, $x + 2$ is equal to 5.” We claim that this sentence is false.\footnote{As usual, to show that a sentence $P$ is false, we suppose that $P$ is true and we show that this assumption leads to a contradiction.} Suppose that $(\forall x \in \mathbb{R})(x + 2 = 5)$ is true. Then in particular, since 0 is a real number, $0 + 2 = 5$. But $0 + 2 \neq 5$. This is a contradiction. Hence $(\forall x \in \mathbb{R})(x + 2 = 5)$ must be false.

(c) The sentence $(\exists x < 0)(x + 2 = 5)$ means “There exists a real number $x$ strictly less than 0, such that $x + 2$ is equal to 5.” We claim that this sentence is false. Suppose $(\exists x < 0)(x + 2 = 5)$ is true. Then we can pick $x_0 < 0$ such that $x_0 + 2 = 5$. But then $x_0 = 5 - 2 = 3$, so it is not the case that $x_0 < 0$. Thus we have reached a contradiction. Hence $(\exists x < 0)(x + 2 = 5)$ must be false.

(d) The sentence $(\forall x \in \mathbb{R})(x^2 + 4x + 5 > 0)$ means “For each real number $x$, $x^2 + 4x + 5$ is strictly greater than 0.” We claim that this sentence is true. To see this, consider any $x_0 \in \mathbb{R}$. Then by completing the square, we see that $x_0^2 + 4x_0 + 5 = (x_0^2 + 4x_0 + 4) + 1 = (x_0 + 2)^2 + 1 \geq 0 + 1 = 1 > 0$. Thus $x_0^2 + 4x_0 + 5 > 0$. Now $x_0$ is an arbitrary element of $\mathbb{R}$.\footnote{To say that $x_0$ is an arbitrary element of $\mathbb{R}$ means that we are not assuming anything about $x_0$ except that it is an element of $\mathbb{R}$.

(e) The sentence $(\exists x \in \mathbb{R})(x^2 + 4x + 2 = 0)$ means “There exists a real number $x$ such that $x^2 + 4x + 2$ is equal to 0.” We claim that this sentence is true. To see this, first note that for each $x \in \mathbb{R}$, by completing
the square and factoring a difference of squares, we have

\[
x^2 + 4x + 2 = x^2 + 4x + 4 - 2 = (x + 2)^2 - 2 = (x + 2)^2 - (\sqrt{2})^2
\]

\[
= [(x + 2) - \sqrt{2}][(x + 2) + \sqrt{2}]
\]

\[
= [x - (-2 + \sqrt{2})][x - (-2 - \sqrt{2})].
\]

Thus, letting \(a = -2 + \sqrt{2}\) and \(b = -2 - \sqrt{2}\), we have \(x^2 + 4x + 2 = (x - a)(x - b)\). Therefore the sentence \((\exists x \in \mathbb{R})(x^2 + 4x + 2 = 0)\) is true, because \(a \in \mathbb{R}\) and \(a^2 + 4a + 2 = (a - a)(a - b) = (0)(a - b) = 0\). \(\blacksquare\)

**3.4 Remark.** In the the solution of part (e) of Example 3.3, we could have used the quadratic formula to find the roots of the quadratic polynomial \(x^2 + 4x + 2\). But the quadratic formula is proved by completing the square and factoring a difference of squares. Thus the approach that we took is more fundamental than the quadratic formula. Furthermore, completing the square has more applications than the quadratic formula. For instance, it is the way to solve quadratic inequalities, to graph quadratic functions, to evaluate integrals where a quadratic expression appears under a radical sign, and so on. So if you have forgotten about completing the square, then you should review it, because it is a very important thing for you to know.

**Examples and Counterexamples.** An *example that proves an existential sentence* \((\exists x)P(x)\) is an example of a value of \(x\) for which \(P(x)\) is true. Thus in the solution of part (a) of Example 3.3, we proved the existential sentence \((\exists x \in \mathbb{R})(x + 2 = 5)\) by pointing out that 3 is an example of a value of \(x\) that belongs to \(\mathbb{R}\), for which the sentence \(x + 2 = 5\) happens to be true. In this case, 3 is the only such value of \(x\), but in other situations, there could be many such values of \(x\). The existential sentence is true if there is at least one such value.

Similarly, a *counterexample that disproves a universal sentence* \((\forall x)P(x)\) is an example of a value of \(x\) for which the sentence \(P(x)\) is false. Thus the most common way to write the solution of part (b) of Example 3.3 would be to disprove the universal sentence \((\forall x \in \mathbb{R})(x + 2 = 5)\) by just pointing out that 0 is an example of a value of \(x\) that belongs to \(\mathbb{R}\), for which the sentence \(x + 2 = 5\) happens to be false. In this case, there are many such values of \(x\). In other situations, there might be only one. The universal sentence is false if there is at least one such value.

By the way, the way we actually wrote the solution to part (b) of Example 3.3 was a little bit longer. We wrote it that way to emphasize that in general, one can prove that a sentence is false by showing that if it were true, a contradiction would result. The approach described in the previous paragraph is an abbreviation of this approach that applies in the case where the sentence that we want to show is false is a universal sentence.

**Exercise 1.** For each of the following sentences, write out what it means in words, state whether it is true or false, and prove your statement.

(a) \((\exists x \in \mathbb{R})(2x + 7 = 3)\).
(b) \((\forall x \in \mathbb{R})(2x + 7 = 3)\).
(c) \((\exists x > 0)(2x + 7 = 3)\).
(d) \((\forall x > 0)(2x + 7 = 3)\).
(e) \((\exists x \in \mathbb{R})(x^2 - 4x + 3 > 0)\).
(f) \((\forall x \in \mathbb{R})(x^2 - 4x + 3 > 0)\).
(g) \((\exists x \geq 7)(x^2 - 4x + 3 > 0)\).
(h) \((\forall x \geq 7)(x^2 - 4x + 3 > 0)\).
(i) \((\forall x \in \mathbb{R})(x^2 - 2x + 2 > 0)\).
(j) \((\forall x \geq 0)(\sqrt{x + 3} = \sqrt{x} + \sqrt{3})\).
(k) \((\exists x \geq 0)(\sqrt{x + 3} = \sqrt{x} + \sqrt{3})\).

\(^{26}\) We could equally well say that the sentence \((\exists x \in \mathbb{R})(x^2 + 4x + 2 = 0)\) is true because \(b \in \mathbb{R}\) and \(b^2 + 4b + 2 = (b - a)(b - b) = (b - a)(0) = 0\).
Free Variables and Bound Variables. Learning how to use variables properly is an important part of learning how to work with quantifiers. A variable may be used either as a free variable or as a bound variable. Here is an example to illustrate the distinction between free variables and bound variables. As in Example 3.2, let the universe of discourse be the set of people \{Jack, Jill\} and let \( P(x) \) stand for the sentence “\(x\) likes chocolate.” Then \( P(x) \) is a statement about \( x \). We are free to regard the \( x \) in \( P(x) \) as standing for any particular element of the universe of discourse. Accordingly, the \( x \) in \( P(x) \) is called a free variable. The \( x \) in \( P(x) \) should be thought of as standing for a particular, although unspecified, element of the universe of discourse. As we saw in Example 3.2, the sentence \((\forall x)P(x)\) has the same truth value as the sentence \(P(Jack) \wedge P(Jill)\). But no \( x \) appears in the sentence \(P(Jack) \wedge P(Jill)\). It follows that the sentence \((\forall x)P(x)\) is not a statement about \( x \). For this reason, the \( x \) in \((\forall x)P(x)\) is called a dummy variable or a bound variable. Unlike the \( x \) in \( P(x) \), the \( x \) in \((\forall x)P(x)\) does not stand for any particular element of the universe of discourse. Rather, it should be thought of as varying over the universe of discourse. In the sentence \((\forall x)P(x)\), the letter \( x \) may be replaced by any other letter without changing the meaning of the sentence, provided notational conflicts are avoided. For instance, \((\forall y)P(y)\) means the same thing as \((\forall x)P(x)\) because it too has the same truth value as \(P(Jack) \wedge P(Jill)\). This is typical of the way dummy variables behave. Similarly, as we also saw in Example 3.2, the sentence \((\exists x)P(x)\) has the same truth value as the sentence \(P(Jack) \lor P(Jill)\). No \( x \) appears in the sentence \(P(Jack) \lor P(Jill)\). Therefore the sentence \((\exists x)P(x)\) is not a statement about \( x \). The \( x \) in \((\exists x)P(x)\) is a dummy variable or bound variable. The \( x \) in \((\exists x)P(x)\) does not stand for any particular element of the universe of discourse. Rather, it should be thought of as varying over the universe of discourse. In the sentence \((\exists x)P(x)\), the letter \( x \) may be replaced by any other letter without changing the meaning of the sentence, provided notational conflicts are avoided. For instance, \((\exists y)P(y)\) means the same thing as \((\exists x)P(x)\) because it too has the same truth value as \(P(Jack) \lor P(Jill)\).

The names “free variable” and “bound variable” can be confusing, but they are standard. The following summary may help you to remember the difference between free variables and bound variables: A free variable is free to stand for any particular object that belongs to the universe of discourse. A bound variable or dummy variable is bound to vary over the universe of discourse. It does not stand for any particular object.

Dummy variables arise in other contexts in mathematics. An index of summation is a dummy variable. For instance, the \( k \) in \(\sum_{k=1}^{3}k^{2}\) is a dummy variable because \(\sum_{k=1}^{3}k^{2} = 1^{2}+2^{2}+3^{2} = 1+4+9 = 14\) and there is no \( k \) in 14. We may replace the \( k \) in \(\sum_{k=1}^{3}k^{2}\) by any other letter. For instance, \(\sum_{i=1}^{3}i^{2} = 1^{2}+2^{2}+3^{2} = 14\) too. The \( k \) in \(\sum_{k=1}^{3}k^{2}\) does not stand for any particular object. Rather, it should be thought of as varying over the set \{1, 2, 3\}. In the expression \(\sum_{k=1}^{n}k^{2}\), the \( k \) is a dummy variable which varies over the set \{1, 2, 3, \ldots, n\} and \( n \) is a free variable which stands for a particular, although unspecified, natural number. The \( k \) in \(\sum_{k=1}^{n}k^{2}\) may be replaced by almost any other letter. However, it should not be replaced by \( n \) as that would lead to a conflict of notation. (The letter \( n \) would be used in two different ways.)

The variable of integration in a definite integral is also a dummy variable. For instance, \(\int_{a}^{b}2x\,dx = 9 = \int_{0}^{3}2t\,dt\). In the expression \(\int_{a}^{b}f(x)\,dx\), \( x \) is a dummy variable and \( a \) and \( b \) are free variables. (Yes, \( f \) is a variable. It stands for a particular although unspecified function here. A variable need not stand for a number. A variable can stand for any object, or even for a person.)

It is possible for the same variable to have both free and bound occurrences within the same expression. For instance, the expression \(k + \sum_{k=1}^{3}k^{2}\) stands for \(k + (1^{2}+2^{2}+3^{2})\), in other words, for \(k + 14\). (Thus the first \( k \) in the expression \(k + \sum_{k=1}^{3}k^{2}\) has nothing to do with the second \( k \) or the third \( k \) in it.) In the expression \(k + \sum_{k=1}^{3}k^{2}\), the first occurrence of the variable \( k \) is a free occurrence, while the second and third occurrences of \( k \) are bound (i.e., dummy) occurrences. Similarly, in the expression \([\int_{a}^{b}f(x)\,dx]^2\), the first and second occurrences of \( x \) are bound occurrences, while the third occurrence of \( x \) is a free occurrence.

The Scope of a Quantifier. The part of a sentence that a quantifier applies to is called the scope of the quantifier. For instance, in the sentence \((\forall x)(x \text{ likes ice cream}) \text{ and } (x \text{ likes cake})\), the scope of the quantifier \((\forall x)\) is “\(x\) likes ice cream.” But in the sentence \((\forall x)(x \text{ likes ice cream} \text{ and } x \text{ likes cake})\),
the scope of the quantifier \((\forall x)\) is “\(x\) likes ice cream and \(x\) likes cake.” Accordingly, sentence (2) means “Everybody likes ice cream and \(x\) likes cake.” In contrast, sentence (1) means “Everybody likes ice cream and \(x\) likes cake.” In sentence (1), the first and second occurrences of \(x\) are bound and the third occurrence of \(x\) is free. Sentence (1) means the same thing as the sentence

\[\forall y(\text{likes ice cream}) \land (\text{likes cake}).\]

Exercise 2. Words such as “every” and “any” normally correspond to universal quantifiers. However, the scope of the corresponding quantifier may depend on which of these words is used. In this exercise, you are asked to consider an example which illustrates this point. Let the universe of discourse be the set of students in your class. Let \(P(x)\) be “\(x\) passes the course” and let \(C\) be “we’ll celebrate.”

(a) In the sentence

\[(\forall x)P(x) \Rightarrow C,\]

the scope of the quantifier \((\forall x)\) is just \(P(x)\). In the sentence

\[\forall x[P(x) \Rightarrow C],\]

the scope of the quantifier \((\forall x)\) is \(P(x) \Rightarrow C\). One of these two sentences means “If everybody passes the course, we’ll celebrate.” The other means “If anybody passes the course, we’ll celebrate.” Which is which? (Hint: The sentence \((\forall x)P(x) \Rightarrow C\) could also be written as \(\{[(\forall x)P(x)] \Rightarrow C\}\).

(b) In the sentence

\[(\exists x)P(x) \Rightarrow C,\]

the scope of the quantifier \((\exists x)\) is just \(P(x)\). The sentence (5) means “If somebody passes the course, we’ll celebrate” and it is logically equivalent to one of the two sentences (3) and (4) in part (a). Which one?

Exercise 3. Let the universe of discourse be the set of French words. Let \(P(x)\) be the sentence “Bob does not know \(x\).” Let \(Q\) be the sentence \((\forall x)P(x)\) and let \(R\) be the sentence \((\exists x)P(x)\). Suppose Marie says “Bob does not know a word of French” and Jacques replies “Which word?” Which of the two sentences \(Q\) and \(R\) do you think Marie meant by what she said and which of these sentences did Jacques think she meant? Comment briefly on what this example illustrates about how everyday language compares with the language of logic, with respect to precise expression of meaning.

Exercise 4. One of the following sentences is true and the other is false. Which one is false? Prove that it is false. (You need not prove that the true one is true.)

(a) \((\forall x \in \mathbb{N})(x \text{ is even or } x \text{ is odd})\).

(b) \((\forall x \in \mathbb{N})(x \text{ is even}) \lor (\forall x \in \mathbb{N})(x \text{ is odd})\).

Exercise 5. One of the following sentences is true and the other is false. Which one is false? Prove that it is false. (You need not prove that the true one is true.)

(a) \((\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})[\text{if } x < y, \text{ then } (\exists a \in \mathbb{N})(x + a = y)]\).

(b) \((\forall x \in \mathbb{R})(\forall y \in \mathbb{R})[\text{if } x < y, \text{ then } (\exists a \in \mathbb{N})(x + a = y)]\).

The Generalized De Morgan’s Laws. Recall that De Morgan’s laws tell us that \(\neg(P_1 \land P_2)\) is logically equivalent to \((\neg P_1) \lor (\neg P_2)\) and that \(\neg(P_1 \lor P_2)\) is logically equivalent to \((\neg P_1) \land (\neg P_2)\). The generalized De Morgan’s laws are generalizations of these logical equivalences, in the same way that universal and existential sentences are generalizations of conjunctive and disjunctive sentences.

Here are a couple of examples in ordinary English to illustrate the generalized De Morgan’s laws. To say “It is not the case that everybody likes chocolate” means the same as to say “Somebody dislikes chocolate.” Similarly, to say “It is not the case that somebody likes spinach” means the same as to say “Everybody dislikes spinach.”

Now here is the precise statement and proof of the generalized De Morgan’s laws.
3.5 Theorem. (Generalized De Morgan’s Laws.) Let \( P(x) \) and \( Q(x) \) be statements about \( x \) and let \( A \) be a subcollection of the universe of discourse. Then:

(a) \( \neg(\forall x \in A)P(x) \) is logically equivalent to \( (\exists x \in A)\neg P(x) \).

(b) \( \neg(\exists x \in A)Q(x) \) is logically equivalent to \( (\forall x \in A)\neg Q(x) \).

Proof. (a) The sentence \( \neg(\forall x \in A)P(x) \) is true iff the sentence \( (\forall x \in A)P(x) \) is false iff the sentence \( P(x) \) is false for at least one value of \( x \) in \( A \) iff the sentence \( \neg P(x) \) is true for at least one value of \( x \) in \( A \) iff the sentence \( (\exists x \in A)\neg P(x) \) is true.

(b) The sentence \( \neg(\exists x \in A)Q(x) \) is true iff the sentence \( (\exists x \in A)Q(x) \) is false iff the sentence \( Q(x) \) is false for every value of \( x \) in \( A \) iff the sentence \( \neg Q(x) \) is true for every value of \( x \) in \( A \) iff the sentence \( (\forall x \in A)\neg Q(x) \) is true. ■

3.6 Example. Let \( P \) be the sentence

\[ (\forall x \in \mathbb{R})(x^2 - 4x + 5 > 0). \]

(a) Use one of the generalized De Morgan’s laws to show that \( \neg P \) is logically equivalent to

\[ (\exists x \in \mathbb{R})(x^2 - 4x + 5 \leq 0). \]

Be careful not to skip any steps.

(b) Is \( P \) true or false?

Solution. (a) By the first generalized De Morgan’s law, we have

\[
\neg(\forall x \in \mathbb{R})(x^2 - 4x + 5 > 0) \\
\quad \text{iff} \quad (\exists x \in \mathbb{R})\neg(x^2 - 4x + 5 > 0) \\
\quad \text{iff} \quad (\exists x \in \mathbb{R})(x^2 - 4x + 5 \leq 0).
\]

(b) For each real number \( x \), we have \( x^2 - 4x + 5 = (x - 2)^2 + 1 \geq 0 + 1 = 1 > 0 \). Thus \( P \) is true. ■

Exercise 6. Let \( P \) be the sentence

\[ (\forall x \in \mathbb{R})(x^2 - 6x + 8 \geq 0). \]

(a) Use one of the generalized De Morgan’s laws to show that \( \neg P \) is logically equivalent to

\[ (\exists x \in \mathbb{R})(x^2 - 6x + 8 < 0). \]

Be careful not to skip any steps.

(b) Is \( P \) true or false?

Exercise 7. Let \( P \) be the sentence

\[ (\exists x \in \mathbb{R})(x \geq 0 \text{ and } \sqrt{x+2} < \sqrt{x+\sqrt{2}}). \]

(a) Use one of the generalized De Morgan’s laws and one of the ordinary De Morgan’s laws to show that \( \neg P \) is logically equivalent to

\[ (\forall x \in \mathbb{R})(x < 0 \text{ or } \sqrt{x+2} \geq \sqrt{x+\sqrt{2}}). \]

Be careful not to skip any steps.

(b) Is \( P \) true or false?

3.7 Example. Here is another illustration of the illogical nature of ordinary English. Let \( P(x) \) be the sentence “\( x \) likes chocolate” and let \( Q(x) \) be the sentence “\( x \) does not like chocolate.” Then the sentence “Everybody likes chocolate” may be expressed as \( (\forall x)P(x) \). It is tempting to think that the sentence “Everybody does not like chocolate” may be expressed as \( (\forall x)Q(x) \). However, in colloquial English, the sentence “Everybody does not like chocolate” is usually taken to mean “Not everybody likes chocolate,” and this may be expressed as \( \neg(\forall x)P(x) \). By one of the generalized De Morgan’s laws, this is logically equivalent to \( (\exists x)\neg P(x) \), which is \( (\exists x)Q(x) \). Thus the sentence \( (\forall x)Q(x) \) does not mean “Everybody does not like chocolate.” Instead, it is the sentence \( (\exists x)Q(x) \) that means “Everybody does not like chocolate.”
The Generalized Distributive Laws. Recall that the distributive laws tell us that $P \land (Q_1 \lor Q_2)$ is logically equivalent to $(P \land Q_1) \lor (P \land Q_2)$ and that $P \lor (Q_1 \land Q_2)$ is logically equivalent to $(P \lor Q_1) \land (P \lor Q_2)$. The generalized distributive laws are generalizations of these logical equivalences, in the same way that universal and existential sentences are generalizations of conjunctive and disjunctive sentences.

3.8 Theorem. (The Generalized Distributive Laws.) Let $Q(x)$ be a statement about $x$, let $P$ be a sentence that is not a statement about $x$, and let $A$ be a subcollection of the universe of discourse. Then:

(a) $P \land (\exists x \in A)Q(x)$ is logically equivalent to $(\exists x \in A)[P \land Q(x)]$.

(b) $P \lor (\forall x \in A)Q(x)$ is logically equivalent to $(\forall x \in A)[P \lor Q(x)]$.

Proof. First let us mention that our assumption that $P$ is not a statement about $x$ means that $x$ does not occur as a free variable in $P$. The importance of this is that it guarantees that the truth value of $P$ does not depend on the value of $x$.

(a) Suppose $P \land (\exists x \in A)Q(x)$ is true. Then $P$ is true and $(\exists x \in A)Q(x)$ is true. Since $(\exists x \in A)Q(x)$ is true, we can pick a value of $x$ in $A$, say $x_0$, such that $Q(x_0)$ is true. Then $P \land Q(x_0)$ is true. Hence $(\exists x \in A)[P \land Q(x)]$ is true, because for instance, $x_0$ is such a value of $x$.

Conversely, suppose $(\exists x \in A)[P \land Q(x)]$ is true. Then we can pick a value of $x$ in $A$, say $x_0$, such that $P \land Q(x_0)$ is true. Then $P$ is true and $Q(x_0)$ is true. Since $Q(x_0)$ is true, $(\exists x \in A)Q(x)$ is true, because for instance, $x_0$ is such a value of $x$. Thus $P \land (\exists x \in A)Q(x)$ is true.

(b) Suppose $P \lor (\forall x \in A)Q(x)$ is true. Then $P$ is true or $(\forall x \in A)Q(x)$ is true.

Case 1. Suppose $P$ is true. Consider any $x_0 \in A$. Then $P \lor Q(x_0)$ is true, because $P$ is true. Now $x_0$ is an arbitrary element of $A$. Hence $(\forall x \in A)[P \lor Q(x)]$ is true.

Case 2. Suppose $(\forall x \in A)Q(x)$ is true. Consider any $x_0 \in A$. Then in particular, $Q(x_0)$ is true. But then $P \lor Q(x_0)$ is true, because $Q(x_0)$ is true. Now $x_0$ is an arbitrary element of $A$. Hence $(\forall x \in A)[P \lor Q(x)]$ is true.

Thus in either case, $(\forall x \in A)[P \lor Q(x)]$ is true.

Conversely, suppose $(\forall x \in A)[P \lor Q(x)]$ is true. Now either $P$ is true or $P$ is false.

Case 1. Suppose $P$ is true. Then $P \lor (\forall x \in A)Q(x)$ is true.

Case 2. Suppose $P$ is false. Consider any $x_0 \in A$. Then $P \lor Q(x_0)$ is true, because $(\forall x \in A)[P \lor Q(x)]$ is true. But $P$ is false. Thus $Q(x_0)$ must be true. Now $x_0$ is an arbitrary element of $A$. Hence $(\forall x \in A)Q(x)$ is true. Thus $P \lor (\forall x \in A)Q(x)$ is true.

Thus in either case, $P \lor (\forall x \in A)Q(x)$ is true. ■

3.9 Example. Let us illustrate in a concrete setting why it is important in the generalized distributive laws that $P$ not be a statement about $x$. Let $P(x)$ be the sentence “$x$ is an odd number,” let $Q(x)$ be the sentence “$x$ is an even number,” and let $A = \mathbb{N}$. Let $R(x)$ be the sentence $P(x) \lor (\forall x \in A)Q(x)$ and let $S$ be the sentence $(\forall x \in A)[P(x) \lor Q(x)]$. Now the sentence $(\forall x \in A)Q(x)$ is false because it says that each natural number is even. Hence the truth value of $R(x)$ is the same as the truth value of $P(x)$. In particular, $P(2)$ is false, because 2 is not odd. But $S$ is true, because $S$ says that each natural number is either even or odd. Thus $R(x)$ is not logically equivalent to $S$.

It is easy to see that $P \land (Q_1 \lor Q_2)$ is logically equivalent to $(P \land Q_1) \lor (P \land Q_2)$, and that $P \lor (Q_1 \lor Q_2)$ is logically equivalent to $(P \lor Q_1) \lor (P \lor Q_2)$. The next result generalizes these facts in the same way that universal and existential sentences generalize conjunctive and disjunctive sentences.

3.10 Theorem. Let $Q(x)$ be a statement about $x$, let $P$ be a sentence that is not a statement about $x$, and let $A$ be a subcollection of the universe of discourse. Then:

(a) $P \land (\forall x \in A)Q(x)$ is logically equivalent to $(\forall x \in A)[P \land Q(x)]$.

(b) $P \lor (\exists x \in A)Q(x)$ is logically equivalent to $(\exists x \in A)[P \lor Q(x)]$.

Proof. This is similar to the proof of the generalized distributive laws. We omit the details. ■
Order of Quantifiers. When a sentence contains both universal and existential quantifiers, it can be very important to pay attention to the order in which these quantifiers occur in the sentence, as the following example illustrates.

3.11 Example. Suppose the universe of discourse is the set of people \{Allen, Betty, Chuck\}. To save writing, sometimes we shall write \( a \) for Allen, \( b \) for Betty, and \( c \) for Chuck. Let \( P(x, y) \) be the sentence “\( x \) likes \( y \).” For the sake of concreteness, suppose the truth value of \( P(x, y) \) depends on \( x \) and \( y \) as shown in the following table in which \( x \) refers to the rows and \( y \) refers to the columns.

<table>
<thead>
<tr>
<th>( P(x, y) )</th>
<th>( y = a )</th>
<th>( y = b )</th>
<th>( y = c )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x = a )</td>
<td>( F )</td>
<td>( T )</td>
<td>( T )</td>
</tr>
<tr>
<td>( x = b )</td>
<td>( T )</td>
<td>( F )</td>
<td>( T )</td>
</tr>
<tr>
<td>( x = c )</td>
<td>( T )</td>
<td>( T )</td>
<td>( F )</td>
</tr>
</tbody>
</table>

Thus Allen, Betty, and Chuck are amicable but self-loathing: Each likes the other two but not himself or herself. Consider the sentence \((\exists y)P(x, y)\). Its truth value depends on \( x \) as shown in the following table.

<table>
<thead>
<tr>
<th>( (\exists y)P(x, y) )</th>
<th>( x = a )</th>
<th>( x = b )</th>
<th>( x = c )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( T )</td>
<td>( T )</td>
<td>( T )</td>
<td></td>
</tr>
</tbody>
</table>

To see this, note that \((\exists y)P(a, y)\) is true because Allen likes Betty and Chuck, \((\exists y)P(b, y)\) is true because Betty likes Allen and Chuck, and \((\exists y)P(c, y)\) is true because Chuck likes Allen and Betty. Note that the sentence \((\exists y)P(a, y)\) means “Allen likes somebody.” Similarly, the sentence \((\exists y)P(b, y)\) means “Betty likes somebody” and the sentence \((\exists y)P(c, y)\) means “Chuck likes somebody.” Thus the sentence \((\exists y)P(x, y)\) means “\( x \) likes somebody.”

Since the sentence \((\exists y)P(x, y)\) is true for each allowed value of \( x \) (namely, for \( x = a \), for \( x = b \), and for \( x = c \)), the sentence \((\forall x)(\exists y)P(x, y)\) is true. Since the sentence \((\exists y)P(x, y)\) means “\( x \) likes somebody,” it follows that the sentence \((\forall x)(\exists y)P(x, y)\) means “For each \( x \), \( x \) likes somebody,” or in other words “Everybody likes somebody.”

To summarize our discussion so far in this example, since we have taken \( P(x, y) \) to mean “\( x \) likes \( y \),” it follows that \((\exists y)P(x, y)\) means “For some \( y \), \( x \) likes \( y \),” or in other words, “\( x \) likes somebody,” and therefore \((\forall x)(\exists y)P(x, y)\) means “For each \( x \), \( x \) likes somebody,” or in other words, “Everybody likes somebody.”

Now consider the sentence \((\forall x)P(x, y)\). Its truth value depends on \( y \) as shown in the following table.

<table>
<thead>
<tr>
<th>( (\forall x)P(x, y) )</th>
<th>( y = a )</th>
<th>( y = b )</th>
<th>( y = c )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( F )</td>
<td>( F )</td>
<td>( F )</td>
<td></td>
</tr>
</tbody>
</table>

Note that the sentence \((\forall x)P(x, a)\) means “Everybody likes Allen.” Similarly, the sentence \((\forall x)P(x, b)\) means “Everybody likes Betty” and the sentence \((\forall x)P(x, c)\) means “Everybody likes Chuck.” Thus the sentence \((\forall x)P(x, y)\) means “Everybody likes \( y \).”

Since the sentence \((\forall x)P(x, y)\) is false in this example for each allowed value of \( y \), the sentence \((\exists y)(\forall x)P(x, y)\) is false. Since the sentence \((\forall x)P(x, y)\) means “Everybody likes \( y \),” it follows that the sentence \((\exists y)(\forall x)P(x, y)\) means “For some \( y \), everybody likes \( y \).” It is tempting to think that this means “Everybody likes somebody.” However this cannot be right, since we saw earlier in this example that instead it is the sentence \((\forall x)(\exists y)P(x, y)\) that means “Everybody likes somebody” and that for the truth values of \( P(x, y) \) that we agreed on, the sentence \((\forall x)(\exists y)P(x, y)\) is true, whereas the sentence \((\exists y)(\forall x)P(x, y)\) is false.\textsuperscript{27} To see how to express the sentence “For some \( y \), everybody likes \( y \)” in everyday language, we must...

\textsuperscript{27} So although for instance the sentence “For some \( y \), Betty likes \( y \)” means “Betty likes somebody,” the sentence “For some \( y \), everybody likes \( y \)” does not mean “Everybody likes somebody.”
rephrase the sentence “Everybody likes y” in the passive voice, as “y is liked by everybody” and then we see that “For some y, everybody likes y” means “For some y, y is liked by everybody,” or in other words, “Somebody is liked by everybody.”

To summarize the second part of the discussion in this example, since we have taken \( P(x, y) \) to mean “x likes y,” it follows that \((\forall x)P(x, y)\) means “For each x, x likes y,” or in other words “Everybody likes y,” or in still other words, “y is liked by everybody,” and therefore \((\exists y)(\forall x)P(x, y)\) means “For some y, y is liked by everybody,” or in other words, “Somebody is liked by everybody.”

In conclusion, in this example, the sentence \((\forall x)(\exists y)P(x, y)\) is true, but the sentence \((\exists y)(\forall x)P(x, y)\) is false. This shows that in general, the two sentences \((\forall x)(\exists y)P(x, y)\) and \((\exists y)(\forall x)P(x, y)\) may have different truth values. Thus it is important to pay attention to the order of the quantifiers in a sentence. Note that in this example, the sentence

\[(\exists y)(\forall x)P(x, y) \Rightarrow (\forall x)(\exists y)P(x, y)\]

is true. We shall see that this is so in the general case too.

**Exercise 8.** Continue with the notation of Example 3.11. Which of the variables \( x \) and \( y \) is free in the sentence \( P(x, y) \)? Answer the same question about each of the four sentences \((\exists y)P(x, y)\), \((\forall x)(\exists y)P(x, y)\), \((\forall x)P(x, y)\), and \((\exists y)(\forall x)P(x, y)\).

**Exercise 9.** Suppose the universe of discourse is the set of people \{ Allen, Betty, Chuck \}. To save writing, sometimes we shall write \( a \) for Allen, \( b \) for Betty, and \( c \) for Chuck. Let \( P(x, y) \) be the sentence “\( x \) likes \( y \).” Suppose the truth value of \( P(x, y) \) depends on \( x \) and \( y \) as shown in the following table.

<table>
<thead>
<tr>
<th>( P(x, y) )</th>
<th>( y = a )</th>
<th>( y = b )</th>
<th>( y = c )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x = a )</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>( x = b )</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>( x = c )</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

Note that in this table, \( x \) refers to the rows and \( y \) refers to the columns. For instance, \( P(c, b) \) is true and \( P(b, c) \) is false.

(a) Is the sentence \((\forall y)P(a, y)\) true or false? What does the sentence \((\forall y)P(a, y)\) mean in ordinary English? Answer the same two questions about each of the two sentences \((\forall y)P(b, y)\) and \((\forall y)P(c, y)\). Make a table showing how the truth value of the sentence \((\forall y)P(x, y)\) depends on \( x \). What does the sentence \((\forall y)P(x, y)\) mean?

(b) Is the sentence \((\exists x)(\forall y)P(x, y)\) true or false? What does this sentence mean in ordinary English?

(c) Make a table showing how the truth value of the sentence \((\exists x)P(x, y)\) depends on \( y \). What does the sentence \((\exists x)P(x, y)\) mean?

(d) Is the sentence \((\forall y)(\exists x)P(x, y)\) true or false? What does this sentence mean in ordinary English?

(e) Consider the two conditional sentences

\[(\exists x)(\forall y)P(x, y) \Rightarrow (\forall y)(\exists x)P(x, y)\]

and

\[(\forall y)(\exists x)P(x, y) \Rightarrow (\exists x)(\forall y)P(x, y)\, .\]

Which of these two sentences is true and which is false in this example?

(f) Which of the variables \( x \) and \( y \) is free in the sentence \( P(x, y) \)? Answer the same question about each of the four sentences \((\forall y)P(x, y)\), \((\exists x)(\forall y)P(x, y)\), \((\exists x)P(x, y)\), and \((\forall y)(\exists x)P(x, y)\).

3.12 Example. Here is an example from algebra that is somewhat analogous to Example 3.11 and Exercise 9. On the one hand,

\[
\sum_{k=3}^{4} \prod_{n=1}^{2} k^n = \sum_{k=3}^{4} k^1k^2 = 3^13^2 + 4^14^2 = 3 \cdot 9 + 4 \cdot 16 = 27 + 64 = 91.
\]
On the other hand,

\[ \prod_{n=1}^{2} \sum_{k=3}^{4} k^n = \prod_{n=1}^{2} (3^n + 4^n) = (3^1 + 4^1)(3^2 + 4^2) = (3 + 4)(9 + 16) = (7)(25) = 175. \]

3.13 Example. For each of the following sentences, write out what it means in words, state whether it is true or false, and prove your statement.

(a) \( (\forall y \in \mathbb{R})(\exists x \in \mathbb{R})(x \leq y) \).

(b) \( (\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(x \leq y) \).

(c) \( (\exists x \in \mathbb{N})(\forall y \in \mathbb{N})(x \leq y) \).

Solution. (a) The sentence \( (\forall y \in \mathbb{R})(\exists x \in \mathbb{R})(x \leq y) \) means “For each real number \( y \), there exists a real number \( x \) such that \( x \) is less than or equal to \( y \).” We claim that this sentence is true. To see this, consider any \( y_0 \in \mathbb{R} \). Then \( y_0 \leq y_0 \). Hence \( (\exists x \in \mathbb{R})(x \leq y_0) \), because for instance, \( y_0 \) is such a value of \( x \). Now \( y_0 \) is an arbitrary element of \( \mathbb{R} \). Hence \( (\forall y \in \mathbb{R})(\exists x \in \mathbb{R})(x \leq y) \).

(b) The sentence \( (\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(x \leq y) \) means “There exists a real number \( x \) such that for each real number \( y \), \( x \) is less than or equal to \( y \).” We claim that this sentence is false. To see this, suppose it is true. Then we can pick \( x_0 \in \mathbb{R} \) such \( (\forall y \in \mathbb{R})(x_0 \leq y) \). But then in particular, \( x_0 \leq x_0 - 1 \). Thus we have reached a contradiction. Hence \( (\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(x \leq y) \) must be false.

(c) The sentence \( (\exists x \in \mathbb{N})(\forall y \in \mathbb{N})(x \leq y) \) means “There exists a natural number \( x \) such that for each natural number \( y \), \( x \) is less than or equal to \( y \).” We claim that this sentence is true. To show this, it suffices to exhibit a value of \( x \) such that the sentence \( (\forall y \in \mathbb{N})(x \leq y) \) is true. We claim that 1 is such a value of \( x \). To see this, consider any \( y_0 \in \mathbb{N} \). Then \( 1 \leq y_0 \). Now \( y_0 \) is an arbitrary element of \( \mathbb{N} \). Hence \( (\forall y \in \mathbb{N})(1 \leq y) \). This proves the claim. Therefore \( (\exists x \in \mathbb{N})(\forall y \in \mathbb{N})(x \leq y) \), because for instance, 1 is such a value of \( x \).

Exercise 10. For each of the following sentences, write out what it means in words, state whether it is true or false, and prove your statement.

(a) \( (\exists y \in \mathbb{R})(\forall x \in \mathbb{R})(x + y = x) \).

(b) \( (\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y = x) \).

(c) \( (\exists y \in \mathbb{R})(\forall x \in \mathbb{R})(x + y = 0) \).

(d) \( (\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y = 0) \).

(e) \( (\exists y \in \mathbb{R})(\forall x \in \mathbb{R})(xy = 1) \).

(f) \( (\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(xy = 1) \).

3.14 Example. The following sentence is ambiguous:

There exists \( x \) such that \( x \) is the mother of \( y \) for each \( y \).

One way to render the sentence (6) unambiguous would be to insert a comma before “for each \( y \)”, as follows:

There exists \( x \) such that \( x \) is the mother of \( y \), for each \( y \).

Another way to render the sentence (6) unambiguous would be to insert a comma before “such that” as follows:

There exists \( x \), such that \( x \) is the mother of \( y \) for each \( y \).

The sentence (7) means “Everybody has a mother.” The sentence (8) means “Somebody is everybody’s mother.” What a difference! A better way to avoid such ambiguity is to write the quantifiers in front. So instead of writing (7), it would be better to write:

For each \( y \), there exists \( x \) such that \( x \) is the mother of \( y \).

And instead of writing (8), it would be better to write:

There exists \( x \) such that for each \( y \), \( x \) is the mother of \( y \).

When we write the quantifiers in front, as we did in the sentences (9) and (10), then there is no doubt about the order of these quantifiers.

It must be admitted that authors of mathematics textbooks are sometimes not as careful as they should be to make the order of quantifiers unambiguous. So occasionally, when you are reading a mathematics textbook, you may need to infer the intended order of quantifiers from the context. This makes it doubly important that you understand the difference in meaning that can result from a different order of quantifiers.
3.15 Example. Let $S$ be a subset of the set of real numbers. If $b$ is a real number, then to say that $b$ is an upper bound for $S$ means that for each $x \in S$, $x \leq b$. To say that $S$ is bounded above means that there exists $b \in \mathbb{R}$ such that $b$ is an upper bound for $S$. Use the generalized De Morgan’s laws to show that $S$ is not bounded above iff for each $b \in \mathbb{R}$, there exists $x \in S$ such that $x > b$. Be careful not to skip any steps.

Solution. $S$ is bounded above iff $(\exists b \in \mathbb{R})(\forall x \in S)(x \leq b)$. Hence

$$S \text{ is not bounded above}$$

iff $$\neg(\exists b \in \mathbb{R})(\forall x \in S)(x \leq b)$$

iff $$(\forall b \in \mathbb{R})\neg(\forall x \in S)(x \leq b)$$

iff $$(\forall b \in \mathbb{R})(\exists x \in S)\neg(x \leq b)$$

iff $$(\forall b \in \mathbb{R})(\exists x \in S)(x > b).$$

This completes the solution. ■

Exercise 11. As in Example 3.15, let $S$ be a subset of the set of real numbers.

(a) If $S$ is the set of all real numbers, is $S$ bounded above?

(b) If $S$ is the set of all numbers $x$ such that some person on earth has $x$ hairs on his or her head, is $S$ bounded above?

Exercise 12. Let $f$ be a function from $\mathbb{R}$ to $\mathbb{R}$ and let $L \in \mathbb{R}$. To say that $f(x)$ tends to $L$ as $x$ tends to $\infty$ means that for each $\varepsilon > 0$, there exists $K \in \mathbb{R}$ such that for each $x > K$, $|f(x) - L| < \varepsilon$. Use the generalized De Morgan’s laws to show that $f(x)$ does not tend to $L$ as $x$ tends to $\infty$ iff there exists $\varepsilon > 0$ such that for each $K \in \mathbb{R}$, there exists $x > K$ such that $|f(x) - L| \geq \varepsilon$. Be careful not to skip any steps.

Exercise 13. Let $f$ be a function from $\mathbb{R}$ to $\mathbb{R}$ and let $a \in \mathbb{R}$. To say that $f$ is continuous at $a$ means that for each $\varepsilon > 0$, there exists $\delta > 0$ such that for each $x \in \mathbb{R}$, if $|x - a| < \delta$, then $|f(x) - f(a)| < \varepsilon$. Use the generalized De Morgan’s laws and what we know about the negation of a conditional sentence to show that $f$ is not continuous at $a$ iff there exists $\varepsilon > 0$ such that for each $\delta > 0$, there exists $x \in \mathbb{R}$ such that $|x - a| < \delta$ and $|f(x) - f(a)| \geq \varepsilon$. Be careful not to skip any steps.

3.16 Example. Let $P(x, y)$ be a sentence and let $A$ and $B$ be subcollections of the universe of discourse. As Example 3.11 illustrated in a particular case, the following sentence is always true:

$$(\exists y \in B)(\forall x \in A)P(x, y) \Rightarrow (\forall x \in A)(\exists y \in B)P(x, y).$$

Let us give a formal, step-by-step proof of this sentence. This will serve as another illustration of the methods of proving universal and existential sentences and the methods of drawing inferences from such sentences. (You should compare the proof we are about to give with the discussion in Example 3.11.) The sentence we wish to prove is a conditional sentence, so the way to prove it is to suppose the antecedent and deduce the consequent. In other words, suppose $(\exists y \in B)(\forall x \in A)P(x, y)$ and under this assumption, prove $(\forall x \in A)(\exists y \in B)P(x, y)$. The latter is a universal sentence, so to prove it we consider any $x_0 \in A$ and try to prove $(\exists y \in B)P(x_0, y)$. Now since we are assuming that $(\exists y \in B)(\forall x \in A)P(x, y)$, we can pick $y_0$ in $B$ such that $(\exists y \in B)P(x_0, y_0)$. Then in particular, since $x_0 \in A$, we have $P(x_0, y_0)$. From this it follows that $(\exists y \in B)P(x_0, y)$, because for instance, $y_0$ is such a value of $y$. Now $x_0$ is an arbitrary element of $A$. Hence $(\forall x \in A)(\exists y \in B)P(x, y)$. This completes the proof.

Uniqueness. Sometimes one wishes to say that there is exactly one value of $x$ in the universe of discourse for which $P(x)$ is true. This is commonly expressed by saying “There exists a unique $x$ such that $P(x)$.” This may be abbreviated by writing $(\exists !x)P(x)$. (Note the exclamation mark after $\exists$.) However, a new type of quantifier is not needed to express this idea, because it can be expressed in terms of an ordinary existential quantifier and two universal quantifiers, as follows:

$$(\exists x)P(x) \land (\forall x_1)(\forall x_2)[P(x_1) \land P(x_2) \Rightarrow x_1 = x_2].$$

The first part of this sentence, $(\exists x)P(x)$, expresses the idea that there is at least one value of $x$ in the universe of discourse such that $P(x)$ is true. By itself, this would leave open the possibility that there might
be more than one such value of \( x \). The second part of the sentence, \((\forall x_1)(\forall x_2)(P(x_1) \land P(x_2) \Rightarrow x_1 = x_2)\), expresses the idea that there is at most one value of \( x \) in the universe of discourse such that \( P(x) \) is true. By itself, this would leave open the possibility that there might be no such value of \( x \). The two parts together express the idea that there is exactly one value of \( x \) in the universe of discourse such that \( P(x) \) is true, as intended. By the way, here is another way to express the sentence \((\exists!x)P(x)\) in terms of ordinary quantifiers:

\[
(\exists x_1)[P(x_1) \land (\forall x_2)(P(x_2) \Rightarrow x_1 = x_2)].
\] (12)

You should think about why (12) is logically equivalent to (11). Of course if \( A \) is a subcollection of the universe of discourse, then \((\exists!x \in A)P(x)\) means that there is a unique value of \( x \) in \( A \) such that \( P(x) \) is true.

Perhaps it is appropriate to recall that in correct English, to say that something is unique means that it is the only one of its kind. In recent years, one often hears people say “very unique” when they mean “very unusual” or “very special.” (One should not say “very unique,” because a thing either is the only one of its kind or it is not. One would not say it is “very the only one of its kind.”) When the word “unique” is used in mathematics, its correct English meaning is the intended meaning.

3.17 Example. The sentence \((\exists y \in \mathbb{R})(3 + y = 1)\) means “There exists a unique real number \( y \) such that \( 3 + y \) is equal to 1.” This sentence is true because \(-2\) is a real number, \(3 + (-2) = 1\), and if \( y \) is a real number such that \( 3 + y = 1 \), then \( y = 1 - 3 = -2 \).

3.18 Example. The sentence \((\forall x \in \mathbb{R})(\exists! y \in \mathbb{R})(x + y = 1)\) means “For each real number \( x \), there exists a unique real number \( y \) such that \( x + y \) is equal to 1.” This sentence is true. To see this, consider any \( x_0 \in \mathbb{R} \). Then \((\exists! y \in \mathbb{R})(x_0 + y = 1)\) is true, because \( 1 - x_0 \) is a real number, \( x_0 + (1 - x_0) = 1 \), and if \( y \) is a real number such that \( x_0 + y = 1 \), then \( y = 1 - x_0 \). Now \( x_0 \) is an arbitrary element of \( \mathbb{R} \). Therefore \((\forall x \in \mathbb{R})(\exists! y \in \mathbb{R})(x + y = 1)\) is true.

3.19 Example. The sentence \((\exists! x \in \mathbb{R})(x^2 = 4)\) means “There exists a unique real number \( x \) such that \( x^2 \) is equal to 4.” This sentence is false because \( 2 \) and \(-2 \) are two different real values of \( x \) for which \( x^2 = 4 \).

3.20 Example. The sentence \((\exists! x \in \mathbb{R})(x^2 = -4)\) means “There exists a unique real number \( x \) such that \( x^2 \) is equal to \(-4\).” This sentence is false because there is no real value of \( x \) for which \( x^2 = -4 \), since the square of a real number cannot be negative.

Exercise 14. For each of the following sentences, write out what it means in words, state whether it is true or false, and prove your answer.

(a) \((\exists x \in \mathbb{R})(2x + 7 = 3)\).
(b) \((\exists x \in \mathbb{R})(x^2 - 4x + 3 < 0)\).
(c) \((\exists x \in \mathbb{Z})(x^2 - 4x + 3 < 0)\).
(d) \((\exists x \in \mathbb{R})(x^2 - 4x + 4 = 0)\).
(e) \((\exists x \in \mathbb{R})(x^2 - 4x + 5 = 0)\).
(f) \((\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y = 0)\).
(g) \((\forall x \in \mathbb{R})(\exists! y \in \mathbb{R})(xy = 1)\).
(h) \((\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(xy = 0)\).
(i) \((\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(xy = 0)\).
(j) \((\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(xy = 0)\).
Section 4. First Examples of Mathematical Proofs

In this section we shall consider some examples and exercises involving even numbers, odd numbers, prime numbers, rational numbers, and irrational numbers. Probably most of the results discussed in these examples and exercises will already be familiar to you. The purpose of discussing them is not to introduce new mathematical facts but rather to illustrate the various proof techniques in a concrete setting. At the end of this section, we summarize these proof techniques. You may find it helpful to go back and forth between the examples and that summary.

Some of the results we shall discuss in this section go back to the ancient Greeks and are among the pearls of early mathematical proofs. The proof that there are infinitely many prime numbers is generally attributed to Euclid around 300 B.C. The first of the Greeks of antiquity whose names are prominent in the history of mathematics was Thales (624–548 B.C.). The second was Pythagoras (582–500 B.C.), said by some to have been a pupil of Thales. Thales was from Miletus, which in his time was the greatest Greek city in the East, located on the coast of what is now Turkey. Pythagoras was born on the nearby island of Samos, which is still part of Greece. In what is now Southern Italy, Pythagoras founded a religious and philosophical society which came to be named after him and which flourished from around 520 B.C. to around 450 B.C. when it was dispersed. Before Pythagoras, the word “mathematics” in ancient Greek simply meant “knowledge.” The Pythagoreans brought the word “mathematics” closer to its modern sense. For them, the four mathematical arts were arithmetic, geometry, music, and astronomy. Nowadays these are considered to be the advanced four of the seven liberal arts, the elementary three of these being grammar, logic, and rhetoric. These core subjects of modern education can thus be traced through the medieval universities of Europe and Plato’s academy in ancient Athens, all the way back to the Pythagoreans. Tradition ascribes the discovery of irrational numbers to the Pythagorean philosopher Hippasus of Metapont around 450 B.C. According to Aristotle (Metaphysica, Book I, Chapter 5), the Pythagoreans recognized that the harmonies of musical scales can be understood in terms of ratios of whole numbers and, encouraged by this success, they concluded “that all other things are modelled after [whole] numbers, and that [whole] numbers are the primary objects in the whole of nature.” They therefore were shocked by the discovery of irrational numbers, for it conflicted with their cherished belief in the centrality of whole numbers. (For instance, the irrationality of \( \sqrt{2} \) implies that the lengths of the diagonal and of the side of a square are not both whole number multiples of any common unit.) There is even a legend that Hippasus was punished by the gods for having made public his discovery — it is said that he disappeared at sea. This legend is a story that is too good not to tell, even though we have no real evidence that it is true. But it is generally accepted that the discovery of irrational numbers came as a great surprise to the Pythagoreans.

The proof of the irrationality of \( \sqrt{2} \) depends on the theory of even and odd numbers, which is believed to have been developed by the early Pythagoreans, and to which we now turn.

---

1 The dates for Thales and Pythagoras are approximate.
2 After its dispersal, the society continued to exist for another century or so.
3 However, the original Greek meaning of the word “mathematics” survives in modern English in our word “polymath,” which means a person of much or varied learning.
Even Numbers and Odd Numbers.

4.1 Definition. To say that \( x \) is an even number means that there exists an integer \( k \) such that \( x = 2k \).

4.2 Example. The number 6 is even because \( 6 = 2(3) \) and 3 is an integer. The number 7 is not even because if \( 7 = 2k \), then \( k = 7/2 = 3.5 \), which is not an integer. The number \(-2\) is even because \(-2 = 2(-1)\) and \(-1\) is an integer. The number 0 is even because \(0 = 2(0)\) and 0 is an integer.

4.3 Definition. To say that \( x \) is an odd number means that there exists an integer \( k \) such that \( x = 2k + 1 \).

4.4 Example. The number 7 is odd because \( 7 = 2(3) + 1 \) and 3 is an integer. The number \(-5\) is odd because \(-5 = 2(-3) + 1\) and \(-3\) is an integer. The number \(-6\) is not odd because if \(-6 = 2k + 1\), then \(-7 = 2k\), so \( k = -7/2 = -3.5 \), which is not an integer.

You should make a point of writing definitions in your notes and remembering them exactly as they are written here. To read and write proofs, it is important for you to know the definitions precisely. If you find it difficult to remember definitions precisely, it may mean that you do not understand them as well as you should. In this case, you will probably find that as you gain practice in applying definitions in proofs, it will become easier for you to remember them precisely.

Seemingly subtle aspects of the wording of a definition can be important. For instance, it would be wrong to define the phrase “\( x \) is an odd number” by the phrase “\( k \) is an integer and \( x = 2k + 1 \),” because the former phrase is a statement about \( x \) alone, whereas latter phrase is a statement about both \( x \) and \( k \). Since the phrase “\( x \) is an odd number” is a statement about \( x \) alone, the phrase that defines “\( x \) is an odd number” should also be a statement about \( x \) alone. This is indeed the case, because in the phrase “there exists an integer \( k \) such that \( x = 2k + 1 \),” the variable \( k \) is a dummy variable.

For similar reasons, I recommend that you avoid defining the phrase “\( x \) is an odd number” by a phrase such as “\( x = 2k + 1 \), where \( k \) is an integer.” In mathematical prose, the word “where” is used in a variety of ways and does not necessarily indicate an existential quantifier. For instance, to write “Let \( I \) be the interval \([a, b]\), where \( a \) and \( b \) are real numbers with \( a < b \)” means the same as to write “Let \( a \) and \( b \) be real numbers such that \( a < b \) and let \( I \) be the interval \([a, b]\).” In both versions of this statement, the variables \( a \), \( b \), and \( I \) occur only as free variables and the word “where” does not indicate a quantifier.

In the phrase “there exists an integer \( k \) such that \( x = 2k + 1 \),” since the variable \( k \) is a dummy variable, it could be changed to any other letter (except \( x \)). Notice that to say what it means for \( k \) to be an odd number, we must use a variable other than \( k \) for the dummy variable. For instance, we could write “To say that \( k \) is an odd number means that there exists an integer \( b \) such that \( k = 2b + 1 \).”

Notice that in a definition, it customary to make the phrase that is being defined stand out in some way. In print, this is often done by typesetting it in italics, as we have in done. In your handwritten notes, it is hard to do it this way. Instead, you might enclose the phrase being defined in a box, as we now illustrate:

To say that \( x \) is an even number means that there exists an integer \( k \) such that \( x = 2k \).

By the way, the phrase “if and only if” is usually reserved to express the equivalence of two sentences in both of which all the terms used have already been defined. Thus for example, once the phrase “\( x \) is an even number” has been defined, it would be correct to write “\( x \) is an even number if and only if there exists an integer \( k \) such that \( x = 2k \).” However one would not normally write this as the definition. Instead, in the definition, I wrote “To say that \( x \) is an even number means that there exists an integer \( k \) such that \( x = 2k \).”

Finally, I will mention that it is common to write definitions using a nonlogical instance of the word “if.” For instance, many authors would write the definition of even number as follows: “We say \( x \) is an even number if there exists an integer \( k \) such that \( x = 2k \).” You will see definitions written in this style in other books. In this book, I shall not do this, because I prefer not to use the word “if” in a way that feels like it should be “if and only if.”

4.5 Example. If \( x \) is odd and \( y \) is odd, then \( x + y \) is even.

Proof. Suppose \( x \) is odd and \( y \) is odd. (We wish to show that \( x + y \) is even.) Since \( x \) is odd, we can pick an integer \( k_1 \) such that \( x = 2k_1 + 1 \). Since \( y \) is odd, we can pick an integer \( k_2 \) such that \( y = 2k_2 + 1 \). Then
4.6 Remark. In the preceding proof, it was important to use different variables $k_1$ and $k_2$ rather than just one variable $k$. The reason is that $x$ need not be equal to $y$. However, instead of using $k_1$ and $k_2$ we could have used two other available variable names, such as $k$ and $\ell$. This would have saved a little writing by avoiding unnecessary subscripts.

Exercise 1.
(a) Prove that if $x$ is even and $y$ is even, then $x+y$ is even.
(b) Prove that if $x$ is even and $y$ is odd, then $x+y$ is odd.
(c) Let $x$, $y$, and $z$ be odd. Is $x+y+z$ odd? Or is $x+y+z$ even? Explain your answer. You should not have to use the definitions of odd and even. Instead you should be able to answer this part by combining one of parts (a) and (b) with Example 4.5.

Exercise 2.
(a) Prove that if $x$ is odd and $y$ is odd, then $xy$ is odd.
(b) Let $x$, $y$, and $z$ be odd. Is $xyz$ odd? Or is $xyz$ even? You should not have to use the definitions of odd and even. Instead you should be able to answer this part by applying part (a).

4.7 Example. Let $x$ and $y$ be integers. If $x$ is even or $y$ is even, then $xy$ is even.

Proof. Suppose $x$ is even or $y$ is even.

Case 1. Suppose $x$ is even. Since $x$ is even, we may pick an integer $k$ such that $x = 2k$. Then $xy = (2k)y = 2(ky)$ and $ky$ is an integer. Hence $xy$ is even.

Case 2. Suppose $y$ is even. Since $y$ is even, we may pick an integer $k$ such that $y = 2k$. Then $xy = x(2k) = (2k)x = 2(kx)$ and $kx$ is an integer. Hence $xy$ is even.

Thus in either case, $xy$ is even. Thus if $x$ is even or $y$ is even, then $xy$ is even.

4.8 Remark. In the proof of Example 4.7, the variable $k$ may stand for a different integer in Case 2 than it stood for in Case 1. This is not a conflict, because at the end of Case 1, we are finished with the $k$ in Case 1. If you prefer, you may use a different variable, say $\ell$, instead of $k$ in Case 2. However, this is not essential.

4.9 Remark. In the proof of Example 4.7, it was not necessary to consider the case where both $x$ and $y$ are even. The reason is that in Case 1, it does not matter whether $y$ is even or odd. Thus Case 1 already covers the case where $x$ and $y$ are both even. (So does Case 2, because in Case 2, it does not matter whether $x$ is even or odd.)

4.10 Remark. Let $x$ be an integer. Then:
(a) $x$ is even or $x$ is odd.
(b) If $x$ is not even, then $x$ is odd.
(c) If $x$ is not odd, then $x$ is even.

Proof. To prove (a) requires induction, which we discuss in the next section, so we shall postpone the proof of (a) until then. Taking (a) for granted, let us prove (b). Suppose $x$ is not even. Then since $x$ is even or $x$ is odd, $x$ must be odd. Thus if $x$ is not even, then $x$ is odd. In other words, (b) holds. The proof of (c) is similar.

Exercise 3. Let $x$ be an integer. Prove that $x(x+1)$ is even.

4.11 Remark. It is easy to check that the three sentences $P \lor Q$, $\neg P \Rightarrow Q$, and $\neg Q \Rightarrow P$ are logically equivalent. If we apply this, taking $P$ to be the sentence “$x$ is even” and taking $Q$ to be the sentence “$x$ is odd,” then we see that in Remark 4.10, the statements (a), (b), and (c) are really just three different ways to say the same thing.

4.12 Remark. Let $x$ be an integer. Then:
(a) $x$ is not both even and odd.
(b) If $x$ is even, then $x$ is not odd.
(c) If $x$ is odd, then $x$ is not even.
Proof. First let us prove (a). Suppose \( x \) is both even and odd. (We shall derive a contradiction from this assumption.) Since \( x \) is even, we can pick an integer \( k \) such that \( x = 2k \). Since \( x \) is odd, we can pick an integer \( \ell \) such that \( x = 2\ell + 1 \). Then \( 2k = 2\ell + 1 \). Let \( m = k - \ell \). Then \( 2m = 1 \). But since \( m \) is an integer, either \( m \geq 1 \) or \( m \leq 0 \), so either \( 2m \geq 2 \) or \( 2m \leq 0 \), so \( 2m \neq 1 \). Thus we have reached a contradiction. Hence it must not be the case that \( x \) is both even and odd. This proves (a).\(^4\)

Now let us prove (b). Suppose \( x \) is even. We wish to show that \( x \) is not odd. Suppose \( x \) is odd. Then \( x \) is both even and odd. But by (a), \( x \) is not both even and odd. Thus we have reached a contradiction. Hence it must be that \( x \) is not odd. Thus if \( x \) is even, then \( x \) is not odd. In other words, (b) holds. The proof of (c) is similar. ■

Exercise 4.

(a) Is it true that for each real number \( x \), if \( x \) is an even number, then \( x \) is not an odd number? Explain your answer.

(b) Is it true that for each real number \( x \), if \( x \) is not an odd number, then \( x \) is an even number? Explain your answer.

4.13 Remark. It is easy to check that the three sentences \( \neg(P \land Q) \), \( P \Rightarrow \neg Q \), and \( Q \Rightarrow \neg P \) are logically equivalent. If we apply this, taking \( P \) to be the sentence “\( x \) is even” and taking \( Q \) to be the sentence “\( x \) is odd,” then we see that in Remark 4.12, the statements (a), (b), and (c) are really just three different ways to say the same thing.

The last few examples and exercises illustrated how to draw inferences from existential sentences and how to prove existential sentences. The next few examples and exercises will illustrate the method of proof by contradiction.

4.14 Example. Let \( x \) and \( y \) be integers. If \( x + y \) is odd, then \( x \) is even or \( y \) is even.

Proof. Suppose \( x + y \) is odd. We wish to show that \( x \) is even or \( y \) is even. We shall show this by contradiction. Suppose it is not the case that \( x \) is even or \( y \) is even. Then, by one of De Morgan’s laws, \( x \) is not even and \( y \) is not even. Hence, since \( x \) and \( y \) are integers, \( x \) is odd and \( y \) is odd. But then, by Example 4.5, \( x + y \) is even. Hence \( x + y \) is not odd. Thus \( x + y \) is odd and \( x + y \) is not odd. This is a contradiction. Hence it must be the case that \( x \) is even or \( y \) is even. Thus if \( x + y \) is odd, then \( x \) is even or \( y \) is even. ■

4.15 Remark. We have proved Example 4.14 by contradiction. It can also be proved by contraposition. Recall that the basis for the method of proof by contraposition is the fact that a conditional sentence \( P \Rightarrow Q \) is logically equivalent to its contrapositive \( \neg Q \Rightarrow \neg P \). Hence to prove \( P \Rightarrow Q \), it suffices to prove \( \neg Q \Rightarrow \neg P \).

You should be familiar with proof by contraposition because you will encounter it in your other mathematics textbooks. However, proof by contradiction is a more powerful method than proof by contraposition. More specifically, any conditional sentence \( P \Rightarrow Q \) that can be proved by contraposition can also be proved by supposing \( P \) and proving \( Q \) by contradiction. For this reason, I recommend that you regard proof by contraposition as a refinement to consider once you have found a proof and are in the process of revising it to make it shorter and simpler. When you are trying to find a proof, do not worry about proof by contraposition.

Here is how to prove Example 4.14 by contraposition. Suppose it is not the case that \( x \) is even or \( y \) is even. Then, by one of De Morgan’s laws, \( x \) is not even and \( y \) is not even. Hence, since \( x \) and \( y \) are integers, \( x \) is odd and \( y \) is odd. But then, as we have seen, \( x + y \) is even. Hence \( x + y \) is not odd. Thus if it is not the case that \( x \) is even or \( y \) is even, then \( x + y \) is not odd. Hence, by contraposition, if \( x + y \) is odd, then \( x \) is even or \( y \) is even.

Exercise 5. Let \( x \) and \( y \) be integers. Prove the following statements.

(a) If \( xy \) is even, then \( x \) is even or \( y \) is even.

(b) If \( xy \) is odd, then \( x \) is odd and \( y \) is odd.

\(^4\) A note to the teacher: To be honest, we should admit that to prove (a) in Remark 4.12 from common basic assumptions about the integers or natural numbers, such as Peano’s axioms, actually requires induction, just as the proof of (a) in Remark 4.10 does. However, in a course such as this book is intended for, I believe it is more important for students to develop their ability to make connections than for them to learn how to derive everything from the weakest possible assumptions.
Exercise 6. Let \( a \) be an integer. Use the results of Exercise 5 to prove the following statements.

(a) If \( a^2 \) is even, then \( a \) is even.
(b) If \( a^2 \) is odd, then \( a \) is odd.

4.16 Remark. Let us emphasize that to prove \( P \) by contradiction, one assumes the negation of \( P \) and shows that this leads to a contradiction. One does not assume \( P \).

If one is trying to prove \( P \), one must *never* assume \( P \). If it were legitimate to assume \( P \) to prove \( P \), then we could effortlessly prove anything we wished, including false things, simply by assuming them!

Exercise 7. Explain what is wrong with the following “proof” that \(-3 = 5\): Suppose that \(-3 = 5\). Then \(-3 - 1 = 5 - 1\). Hence \(-4 = 4\). But then \((-4)^2 = 4^2\). In other words, \(16 = 16\). This is true. Hence our assumption that \(-3 = 5\) is correct.

Rational Numbers.

4.18 Definition. To say that \( x \) is a rational number means that there exist integers \( m \) and \( n \) such that \( n \neq 0 \) and \( x = m/n \).

4.19 Example. The number 3 is rational, since \( 3 = 3/1 \). Similarly, each integer is a rational number. The numbers \( 1/2 \), \( 9/5 \), and \( 7/(-3) \) are rational. The number \( \sqrt{2} \) is not rational. We shall see how to prove this soon. Later we shall see that in a sense, most real numbers are not rational.

4.20 Remark. Perhaps you are wondering why we wrote “there exist” rather than “there exists” in Definition 4.18. The answer is that the subject of the verb “exist” in that definition is the plural noun phrase “integers \( m \) and \( n \)” so the plural form of the verb, namely “exist,” should be used. We could alternatively have written “there exists an integer \( m \) and there exists an integer \( n \) such that \( n \neq 0 \) and \( x = m/n \). In this case, the singular form of the verb, namely “exists,” is used because in each instance the subject is singular.

4.21 Example. Let \( u \) and \( v \) be rational numbers. Then \( u + v \) is a rational number.

Proof. Since \( u \) is rational, we can pick integers \( a \) and \( b \) such that \( b \neq 0 \) and \( u = a/b \). Since \( v \) is rational, we can pick integers \( c \) and \( d \) such that \( d \neq 0 \) and \( v = c/d \). Then

\[
\frac{u + v}{b} = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.
\]

Note that \( ad + bc \) and \( bd \) are integers. Also, \( bd \neq 0 \) because \( b \neq 0 \) and \( d \neq 0 \). Hence \( u + v \) is a rational number.

Exercise 8. Let \( u \), \( v \), and \( w \) be rational numbers. Prove the following statements.

(a) \(-v \) is a rational number.
(b) \( u - v \) is a rational number. (You can prove this by going back to the definition of a rational number. Alternatively, you can prove it by observing that \( u - v = u + (-v) \) and combining the results of part (a) and Example 4.21. The second way is shorter but the first is self-contained. It is good to know both ways.)
(c) \( uv \) is a rational number.
(d) If \( w \neq 0 \), then \( 1/w \) is a rational number.
(e) If \( w \neq 0 \), then \( u/w \) is a rational number. (You can prove this by going back to the definition of a rational number. Alternatively, you can prove it by combining the results of parts (c) and (d). The second way is shorter but the first way is self-contained. It is good to know both ways.)
Special Forms for Rational Numbers.

4.22 Remark. Let \( x \) be a rational number. Then there exists an integer \( a \) and a natural number \( b \) such that \( x = a/b \).

Proof. Since \( x \) is rational, we can pick integers \( m \) and \( n \) such that \( n \neq 0 \) and \( x = m/n \). Now either \( n > 0 \) or \( n < 0 \).

Case 1. Suppose \( n > 0 \). Then \( n \) is a natural number. Hence we may take \( a = m \) and \( b = n \).

Case 2. Suppose \( n < 0 \). Then \( -n \) is a natural number.\(^5\) Also, \( x = (-m)/(-n) \) and \( -m \) is an integer. Hence we may take \( a = -m \) and \( b = -n \).

Thus in either case, there exists an integer \( a \) and a natural number \( b \) such that \( x = a/b \). ■

4.23 Remark. It is a familiar fact that each rational number can be written in lowest terms. At this point, we can only illustrate this statement with examples. For instance, \( 6/4 \) can be reduced to \( 3/2 \). To prove in general the fact that a rational number can be written in lowest terms is not difficult but requires complete induction, a method of proof which we shall discuss later. And even to formulate this fact precisely involves the notion of divisibility, which is defined later in this section.

Irrational Numbers.

4.24 Definition. To say that \( x \) is an irrational number means that \( x \) is a real number and \( x \) is not a rational number.

4.25 Remark. Be careful to remember that each irrational number is a real number. It is a common error to think that to say that \( x \) is an irrational number means just that \( x \) is not a rational number. If we were to accept this, then we would have to accept that anything that is not a rational number is an irrational number. For instance, you would be an irrational number. I don’t think you would agree with that!

Exercise 9. Recall that each real number is a complex number but that there are complex numbers, such as \( \sqrt{-1} \) and \( 7 - 3\sqrt{-1} \), that are not real numbers.

(a) Is it true that for each complex number \( x \), if \( x \) is an irrational number, then \( x \) is not a rational number? Explain your answer.

(b) Is it true that for each complex number \( x \), if \( x \) is not a rational number, then \( x \) is an irrational number? Explain your answer.

4.26 Example. Let \( x \) be a rational number and let \( y \) be an irrational number. Then \( x + y \) is an irrational number.

Proof. Since \( x \) and \( y \) are real numbers, \( x + y \) is a real number. It remains to show that \( x + y \) is not rational. Suppose \( x + y \) is rational. Then \( (x + y) - x \) is rational, since it is the difference of the rational numbers \( x + y \) and \( x \). But \( (x + y) - x = y \). Hence \( y \) is rational. But \( y \) is not rational because \( y \) is irrational. Thus \( y \) is rational and \( y \) is not rational. This is a contradiction. Hence our assumption that \( x + y \) is rational must be wrong. Therefore \( x + y \) is not rational. ■

Exercise 10. Let \( x \) be a rational number and let \( y \) be an irrational number.

(a) Prove that \(-y\) is irrational.

(b) Prove that \(x - y\) is irrational.

(c) Prove that \(y - x\) is irrational.

(d) Prove that if \(x \neq 0\), then \(xy\) is irrational. Be sure to explain where you use the condition that \(x \neq 0\) in your proof.

(e) Is it possible that there is a different proof for part (d) that does not use the condition that \(x \neq 0\) but still leads to the conclusion that \(xy\) is irrational? Explain your answer.

(f) Prove that \(y/1\) is irrational. (You should start by explaining why \(y \neq 0\). This does not mean that you should say that it would be bad if \(y\) were equal to zero, since we must not divide by zero. It means that you should explain why \(y\) is not equal to zero.)

---

\(^5\) In case you need a reminder, a number of the form \(-n\) need not be negative. For instance, if \(n = -3\), then \(-n = -(\cdot3) = 3\), which is positive.
(g) Prove that if \( x \neq 0 \), then \( x/y \) is irrational.
(h) Prove that if \( x \neq 0 \), then \( y/x \) is irrational.

4.27 Example. If a product of two real numbers \( x \) and \( y \) is rational, it does not necessarily follow that \( x \) and \( y \) themselves are rational. For instance, if \( x = \sqrt{2} = y \), then \( xy = 2 \), which is rational, but \( x \) and \( y \) are not rational. (As we have mentioned several times already, and as we shall show shortly, \( \sqrt{2} \) is irrational.)

Exercise 11. Give an example of two irrational numbers \( x \) and \( y \) whose sum \( x + y \) is rational.

We now take up the proof that \( \sqrt{2} \) is irrational.

4.28 Theorem.
(a) Let \( x \) be a rational number. Then \( x^2 \neq 2 \).
(b) \( \sqrt{2} \) is irrational.

Proof. (a) Suppose \( x^2 = 2 \). We shall show that this assumption leads to a contradiction. (This is the natural way to proceed, since the sentence that we wish to prove is a negative sentence.) Since \( x \) is rational, we can pick integers \( a \) and \( b \) such that \( b \neq 0 \) and \( x = a/b \). Furthermore, by Remark 4.23, we may pick \( a \) and \( b \) so that the fraction \( a/b \) is in lowest terms. Since \( x^2 = 2 \), we have \((a/b)^2 = 2\), so \( a^2 = 2b^2 \). Hence \( a^2 \) is even. But then \( a \) must be even, so we can pick an integer \( k \) such that \( a = 2k \). Then \((2k)^2 = 2b^2\), so \( 4k^2 = 2b^2 \), so \( 2k^2 = b^2 \). Hence \( b^2 \) is even. But then \( b \) must be even. Thus \( a \) and \( b \) are both even, so the fraction \( a/b \) is not in lowest terms, since there is a factor of 2 that could be cancelled from both \( a \) and \( b \). But \( a \) and \( b \) were picked so that the fraction \( a/b \) would be in lowest terms. Hence we have reached a contradiction. Therefore \( x^2 \neq 2 \).

(b) We know that \( \sqrt{2} \) is a real number. To show that \( \sqrt{2} \) is irrational, it remains to show that \( \sqrt{2} \) is not rational. Suppose \( \sqrt{2} \) is rational. Let \( x = \sqrt{2} \). Then \( x^2 = 2 \). But by part (a), since \( x \) is rational, \( x^2 \neq 2 \). Hence we have reached a contradiction. Therefore \( \sqrt{2} \) is not rational.

There are many other examples of specific numbers that are known to be irrational. For instance, \( \pi \) is irrational and \( e \) (the base for the natural logarithm function) is irrational. The irrationality of \( \pi \) was proved in 1761 by Johann Heinrich Lambert, a Swiss-German mathematician, astronomer, physicist, and philosopher. The irrationality of \( e \) was proved in 1737 by the great Swiss mathematician and physicist Leonhard Euler. Both these proofs are quite different from the proof of the irrationality of \( \sqrt{2} \), as would be expected in view of the fact that they were not found until more than two thousand years after the proof that \( \sqrt{2} \) is irrational. Of course the ancient Greeks could have proved anything about the number \( e \), since it was unheard of until the seventeenth century, but they were familiar with \( \pi \).

There are also many specific numbers for which we do not know whether they are rational or irrational. A couple of these are mentioned in the remark after the next exercise.

Exercise 12. Show that for each real number \( x \), \( \pi + x \) is irrational or \( \pi - x \) is irrational.

4.29 Remark. As was stated above, the number \( \pi \) is irrational. Hence for each rational number \( x \), the numbers \( \pi + x \) and \( \pi - x \) are both irrational. But what if \( x \) is irrational? The previous exercise tells us that for each irrational number \( x \), at least one of the numbers \( \pi + x \) and \( \pi - x \) is irrational. In particular, at least one of the numbers \( \pi + e \) and \( \pi - e \) is irrational. However, to this day, it is not known whether \( \pi + e \) is irrational. It is also not known whether \( \pi - e \) is irrational. Nevertheless, either \( \pi + e \) is irrational or \( \pi - e \) is irrational, or both.

Divisibility.

4.30 Definition. Let \( d \) and \( x \) be integers. To say that \( d \) divides \( x \) means that there exists an integer \( k \) such that \( x = kd \).

4.31 Examples. The integers that divide 6 are 1, 2, 3, 6, −1, −2, −3, and −6. The integers that divide 3 are 1, 3, −1, and −3. The integers that divide 1 are 1 and −1. Every integer divides 0, because for each integer \( d \), \( 0 = 0 \cdot d \). In particular, 0 divides 0 (even though 0/0 is undefined). But 0 is the only integer that 0 divides, because if \( x \) is and integer and 0 divides \( x \), then \( x = k \cdot 0 \) for some integer \( k \), and \( k \cdot 0 = 0 \), so \( x = 0 \).

\[6 \text{ Euler is pronounced “Oiler.”}\]
4.32 Example. Let \( x \) be an integer. Then \( x \) is even iff 2 divides \( x \).

4.33 Remark. Let \( d \) and \( x \) be integers. If \( d \neq 0 \), then it is true that \( d \) divides \( x \) iff \( x/d \) is an integer. Nevertheless, it is not customary to use the operation of division in proofs involving divisibility. Instead, in such proofs, one normally works directly with the definition of divisibility. The definition of divisibility involves multiplication. Specifically, it involves \( k \) multiplied by \( d \). It does not involve division. Specifically, it does not involve \( x \) divided by \( d \). (Note that \( x/d \) might not even be defined, because \( d \) could be 0.) It is fair to say that the operation of multiplication is more fundamental than the operation of division. After all, in elementary school, you learned about multiplication before you learned about division. Accordingly, you should embrace the fact that the definition of divisibility is expressed in terms of the operation of multiplication and not in terms of the operation of division.

4.34 Remark. In Definition 4.30, the sentence “Let \( d \) and \( x \) be integers” is called the preamble. It establishes the context for the definition. It would not mean the same thing to write “To say that \( d \) divides \( x \) means that \( d \) and \( x \) are integers and there exists an integer \( k \) such that \( x = kd \).” This would preclude defining the phrase “\( d \) divides \( x \)” differently in a different context. For instance, when \( d = a + bi \) and \( x = u + vi \) where \( a, b, u, v \) are integers and \( i = \sqrt{-1} \), then the phrase “\( d \) divides \( x \)” customarily has a different meaning from the one given in the preceding definition. It is not our purpose here to go into details about this. We only wish to emphasize that if a definition includes a preamble, then that preamble belongs at the beginning, as in the preceding definition.

4.35 Remark. One often uses the expression “\( x \) is divisible by \( d \)" to mean the same thing as “\( d \) divides \( x \).”

4.36 Remark. You should be careful not to confuse “\( d \) divides \( x \)” with “\( d \) divided into \( x \).” The expression “\( d \) divides \( x \)” is a sentence. For instance, “2 divides 6” is a true sentence, and “2 divides 7” is a false sentence. The expression “\( d \) divided into \( x \)” is a number, provided \( d \neq 0 \). For instance, “2 divided into 6” is 3, which is a number, not a sentence.

4.37 Remark. It is common to write \( d \mid x \) as an abbreviation for “\( d \) divides \( x \).” But you should be careful how you write \( d \mid x \). In this abbreviation, the symbol “\( \mid \)” is a vertical stroke. It is not slanted, like “\( / \).” In other words, “\( \mid \)” is not a fraction bar. It is just an abbreviation for the verb “divides.” The expression \( d \mid x \) is an abbreviation for the sentence “\( d \) divides \( x \).” The expression \( d/x \) stands for the number “\( d \) divided by \( x \).” The expressions \( d \mid x \) and \( d/x \) are completely different. For instance 6 \( \mid 3 \) is false but 6/3 = 2.

4.38 Remark. It is also common to write \( d \not| x \) as an abbreviation for “\( d \) does not divide \( x \).”

4.39 Remark. Let \( d, x \in \mathbb{N} \). Suppose \( d \) divides \( x \). Then \( d \leq x \).

Proof. Since \( d \) divides \( x \), we can pick an integer \( k \) such that \( x = kd \). Since \( k \) is an integer, either \( k \geq 1 \) or \( k \leq 0 \). But it is not the case that \( k \leq 0 \), because if \( k \leq 0 \), then \( x = kd \leq 0 \), which contradicts that fact that \( x \geq 1 \). Hence \( k \geq 1 \). Therefore \( kd \geq d \). In other words, \( x \geq d \). 

Exercise 13. Let \( a, b, c \in \mathbb{Z} \). Prove the following statements.
(a) If \( a \) divides \( b \) and \( a \) divides \( c \), then \( a \) divides \( b + c \) and \( a \) divides \( b - c \).
(b) If \( a \) divides \( b \) or \( a \) divides \( c \), then \( a \) divides \( bc \).
(c) If \( a \) divides \( b \), then \( a \) divides \( -b \).
(d) If \( a \) divides \( b \), then \( -a \) divides \( b \).

Exercise 14. Let \( a, b, c \in \mathbb{Z} \). Prove the following statements.
(a) \( a \) divides \( a \).
(b) If \( a \) divides \( b \) and \( b \) divides \( a \), then \( b = a \) or \( b = -a \).
(c) If \( a \) divides \( b \) and \( b \) divides \( c \), then \( a \) divides \( c \).

4.40 Remark. It follows from the results of the Exercise 14 that on the set \( \omega \) of whole numbers, the relation of divisibility is reflexive, antisymmetric, and transitive. In other words,
(a) For each \( a \in \omega \), \( a \) divides \( a \). (Reflexivity.)
(b) For all \( a, b \in \omega \), if \( a \) divides \( b \) and \( b \) divides \( a \), then \( a = b \). (Antisymmetry.)
(c) For all \( a, b, c \in \omega \), if \( a \) divides \( b \) and \( b \) divides \( c \), then \( a \) divides \( c \). (Transitivity.)
4.41 Remark. Now that we have the notion of divisibility, we can give a precise formulation of what it means for a fraction to be in lowest terms. Let $m$ and $n$ be integers, with $n \neq 0$. To say that the fraction $m/n$ is in lowest terms means that for each natural number $d$, if $d$ divides $m$ and $d$ divides $n$, then $d = 1$. More colloquially, to say that $m/n$ is in lowest terms means that 1 is the only natural number that divides both $m$ and $n$.

Prime Numbers.

4.42 Definition. To say that $x$ is a prime number means that $x \in \mathbb{N}$ and $x \neq 1$ and for each $a \in \mathbb{N}$, for each $b \in \mathbb{N}$, if $x = ab$, then $a = 1$ or $b = 1$.

4.43 Examples. 1 is not prime, 2 is prime, 3 is prime, 4 is not prime (because $4 = 2 \cdot 2$), 5 is prime, 6 is not prime (because $6 = 2 \cdot 3$), and so on.

Exercise 15. Show that $x$ is not a prime number iff $x \notin \mathbb{N}$ or $x = 1$ or for some $a \in \mathbb{N}$, for some $b \in \mathbb{N}$, $x = ab$ and $a \neq 1$ and $b \neq 1$. (Hint: Use De Morgan’s laws, the generalized De Morgan’s laws, and what we know about the negation of a conditional sentence. Your solution should proceed one step at a time. In other words, each step of your solution should involve one use of one of these rules.)

4.44 Remark. You are probably familiar with the fact that each natural number, except 1, is prime or is a product of two or more primes. For instance, 2 and 3 are prime, $4 = (2)(2)$, 5 is prime, $6 = (2)(3)$, and so on. At this point, we can only illustrate this fact with examples such as those in the previous sentence. To prove it in general is not difficult but requires complete induction, a method of proof which, as we have already mentioned, we shall discuss later.

By the way, the root meaning of the word “prime” is “first”, as in “prime minister,” which means “first minister.” Prime numbers are “first numbers” in the sense that if we list the natural numbers different from 1 according to the number of prime factors that they have, then the prime numbers

$$2, 3, 5, 7, 11, \ldots$$

would be listed first since each of them has just one prime factor. The numbers with two prime factors would be listed next:

$$4 = (2)(2), 6 = (2)(3), 9 = (3)(3), 10 = (2)(5), \ldots$$

Then would come the numbers with three prime factors:

$$8 = (2)(2)(2), 12 = (2)(2)(3), \ldots$$

Then we would list the numbers with four prime factors, five prime factors, and so on. Each natural number, except 1, occurs in one of these lists, because each natural number, except 1, is prime or is a product of two or more prime factors.

4.45 Remark. From the fact that each natural number, except 1, is prime or is a product of two or more primes, it follows that for each $n \in \mathbb{N}$, if $n \neq 1$, then there exists a prime number $p$ such that $p$ divides $n$. This observation is put to use in the following famous theorem, which is believed to have been proved by Euclid around 300 B.C.\(^7\)

4.46 Theorem. There are infinitely many prime numbers.

Proof. What we wish to show is that it is not the case that there are only finitely many primes. Suppose that there are only finitely primes. We shall show that this assumption leads to a contradiction. Let $p_1, p_2, \ldots, p_m$ be all the primes that there are. Let $x = p_1 \cdot \cdots \cdot p_m$ be their product and let $y = x + 1$. Notice that each of $p_1, \ldots, p_m$ divides $x$, so none of them divides $y$, for if one did, it would also divide $y - x$, which is

\(^7\) Euclid wrote a collection of thirteen books, called the Elements, in which he gave a systematic exposition of the most important mathematical knowledge of his time. While these books are best known for their treatment of geometry, several of them deal with number theory. The fact that each natural number, except 1, is divisible by some prime number is Proposition 31 in Book VII. The theorem that there are infinitely many prime numbers is Proposition 20 in Book IX. It is one of the few important theorems in the Elements that are believed to have been established by Euclid himself.
impossible, since \( y - x = 1 \) and no prime divides 1. Now \( y \in \mathbb{N} \) and \( y \neq 1 \), so there is a prime \( q \) such that \( q \) divides \( y \). Since none of \( p_1, \ldots, p_m \) divides \( y \), \( q \) cannot be one of \( p_1, \ldots, p_m \). But \( p_1, \ldots, p_m \) are all the primes that there are, so \( q \) must be one of \( p_1, \ldots, p_m \). Thus we have reached a contradiction. Hence our assumption that there are only finitely many primes must be wrong. Therefore there must be infinitely many primes. ■

**Exercise 16.** Let \( n \in \mathbb{N} \). Prove that there exists a prime number \( q \) such that \( n < q \leq 1 + n! \). (Hint: Adapt part of the proof of Theorem 4.46. Reminder: \( n! \) is the product of the natural numbers from 1 to \( n \). Thus \( 1! = 1, 2! = 2 \cdot 1, 3! = 3 \cdot 2 \cdot 1 \), and so on.)

**4.47 Remark.** In 1848, the Russian mathematician P. L. Chebyshev proved that for each natural number \( n \), there is a prime number between \( n \) and \( 2n \). Notice that when \( n \) is at all large, \( 2n \) is much smaller than \( 1 + n! \). Thus this theorem of Chebyshev’s is much sharper than Exercise 16 (but it is also much harder to prove).

**4.48 Remark.** There is a remarkable result, called the prime number theorem, that tells approximately how often prime numbers occur. The great German mathematician Carl Friedrich Gauss conjectured it in 1792 or 1793, when he was around 16 years old, by perusing tables of prime numbers. Chebyshev made progress on it in the 1850s and it was finally proved in 1896, by the French mathematician Jacques Hadamard and the Belgian mathematician Charles de la Vallée-Poussin independently. Roughly speaking, the prime number theorem says that when \( n \) is large, the fraction of the numbers in the set \( \{1, \ldots, n\} \) that are prime is approximately \( 1/\log n \), where \( \log n \) is the natural logarithm of \( n \). It can be shown that another way to say this is that when \( k \) is large, the \( k \)-th prime number is about \( k \log k \), where the percentage error tends to 0 as \( k \) tends to infinity.

**4.49 Remark.** A pair of prime numbers \( p \) and \( q \) such that \( p + 2 = q \) is called a pair of twin primes. Some pairs of twin primes are 3 and 5, 5 and 7, 11 and 13, 17 and 19, and 29 and 31. Mathematicians believe that there are infinitely many pairs of twin primes. They even have a formula that they believe describes how about how often pairs of twin primes occur (analogous to the prime number theorem that describes about how often primes occur). But nobody has been able to prove that there actually are infinitely many pairs of twin primes, nor has anybody been able to prove that there are not. How remarkable it is that a question which is so natural and so easy to pose should be still be unanswered.

**4.50 Remark.** A fact about prime numbers which is probably familiar to you is that if a prime number \( p \) divides a product \( xy \) of two integers \( x \) and \( y \), then \( p \) divides \( x \) or \( p \) divides \( y \). This conclusion need not hold if \( p \) is not prime. For instance, \( 6 \) divides \((2)(3)\), but \( 6 \) does not divide 2 and \( 6 \) does not divide 3. But if a natural number \( d \) divides a product \( xy \) of two integers \( x \) and \( y \), then there exist natural numbers \( d_1 \) and \( d_2 \) such that \( d_1 \) divides \( x \), \( d_2 \) divides \( y \), and \( d = d_1d_2 \). For instance, \( 6 \) divides \((4)(9)\), and \( 6 = (2)(3) \) where \( 2 \) divides \( 4 \) and \( 3 \) divides \( 9 \). More generally, if a natural number \( d \) divides a product \( x_1x_2\cdots x_n \) of \( n \) integers \( x_1, x_2, \ldots, x_n \), then there exist natural numbers \( d_1, d_2, \ldots, d_n \) such that \( d_1 \) divides \( x_1 \), \( d_2 \) divides \( x_2 \), ..., \( d_n \) divides \( x_n \), and \( d = d_1d_2\cdots d_n \). (The proofs of these facts also require complete induction and are surprisingly intricate, as we shall see later.) Still more generally, if an integer \( d \) divides a product \( x_1x_2\cdots x_n \) of \( n \) integers \( x_1, x_2, \ldots, x_n \), then there exist natural numbers \( d_1, d_2, \ldots, d_n \) such that \( d_1 \) divides \( x_1 \), \( d_2 \) divides \( x_2 \), ..., \( d_n \) divides \( x_n \), and \( d = \text{sgn}(d)d_1d_2\cdots d_n \), where

\[
\text{sgn}(d) = \begin{cases} 
1 & \text{if } d > 0, \\
0 & \text{if } d = 0, \\
-1 & \text{if } d < 0.
\end{cases}
\]

For instance, \(-6\) divides \((4)(9)\), and \(-6 = (-1)(2)(3)\), where \(-1 = \text{sgn}(-6)\), \(2\) divides \(4\), and \(3\) divides \(9\).

**4.51 Remark.** The expression \( \text{sgn}(d) \) introduced in Remark 4.50 may be read “signum of \( d \).” “Signum” is Latin for “sign,” so \( \text{sgn}(d) \) could also be read “sign of \( d \)” but then it might be confused with “sine of \( d \),” which is a very different quantity.
More about Rational Numbers and Irrational Numbers.

4.52 Example. As we have seen, \( \sqrt{2} \) is irrational. In fact, much more than this is true:

(a) Let \( x \) be a rational number such that \( x^2 = c \), where \( c \) is a whole number. Then \( x \) is an integer.

(b) Let \( c \) be a whole number which is not a perfect square. Then \( \sqrt{c} \) is irrational.

Proof. (a) Since \( x \) is rational, we can pick an integer \( a \) and a natural number \( b \) such that \( x = a/b \) and the fraction \( a/b \) is in lowest terms, by Remark 4.22 and Remark 4.23. Since \( x^2 = c \) and \( x = a/b \), we have \( (a/b)^2 = c \), so \( a^2/b^2 = c \), so \( a^2 = cb^2 \). Since \( cb \) is an integer, this shows that \( b \) divides \( a^2 \). In other words, \( b \) divides the product \( (a)(a) \). Hence by Remark 4.50, we can pick natural numbers \( b_1 \) and \( b_2 \) such that \( b_1 \) divides \( a \), \( b_2 \) divides \( a \), and \( b = b_1b_2 \). Then \( b_1 \) divides both \( a \) and \( b \). But then \( b_1 = 1 \), because \( a/b \) is in lowest terms.\(^8\) Similarly, \( b_2 = 1 \). Hence \( b = b_1b_2 = (1)(1) = 1 \). But then \( x = a/b = a/1 = a \), so \( x \) is an integer, because \( a \) is an integer.

(b) Since \( c \) is a whole number, \( c \geq 0 \), so \( \sqrt{c} \) is real. To show that \( \sqrt{c} \) is irrational, it remains to show that \( \sqrt{c} \) is not rational. Suppose \( \sqrt{c} \) is rational. Let \( x = \sqrt{c} \). Then \( x^2 = c \). But by part (a), since \( x \) is rational and \( c \) is a whole number, \( x \) is an integer. But since \( c \) is not a perfect square, there is no integer whose square is \( c \). In particular, \( x^2 \neq c \). We have reached a contradiction. Therefore \( \sqrt{c} \) is not rational. □

4.53 Remark. In the proof of Example 4.52(a), the fact that \( b_1 \) divides \( a \) and \( b_2 \) divides \( a \) is part of how \( b_1 \) and \( b_2 \) are chosen. It is a common mistake for students to think it is a consequence of the fact that \( (b_1)(b_2) \) divides \( (a)(a) \). This is not the case. For instance, \((4)(9)\) divides \((6)(6)\), but \(4\) does not divide \(6\) and \(9\) does not divide \(6\). Make sure you avoid this common mistake.

Exercise 17.

(a) Let \( x \) be a rational number such that \( x^2 = c \), where \( c \) is an integer. Prove that \( x \) is an integer.

(b) Let \( c \) be an integer which is not a perfect cube. Prove that the cube root of \( c \) is irrational.

Exercise 18. Let \( x \) be a real number such that \( x^3 = rx^2 + sx + t \), where \( r \), \( s \), and \( t \) are integers.

(a) Prove that if \( x \) is rational, then \( x \) is an integer.

(b) Prove that if \( x \) is not an integer, then \( x \) is irrational.

Exercise 19. Let \( x \) be a real number such that

\[ x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 = 0, \]

where \( n \in \mathbb{N} \) and \( c_0, c_1, \ldots, c_{n-1} \in \mathbb{Z} \).

(a) Prove that if \( x \) is rational, then \( x \) is an integer.

(b) Prove that if \( x \) is not an integer, then \( x \) is irrational.

Exercise 20. (The rational roots theorem.) Let \( x \) be a rational number such that

\[ c_nx^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 = 0, \]

where \( n \in \mathbb{N} \) and \( c_0, c_1, \ldots, c_{n-1}, c_n \in \mathbb{Z} \). Prove that \( x \) can be written in the form \( x = a/b \) where \( a \) is an integer that divides \( c_0 \) and \( b \) is a natural number that divides \( c_n \). (Hint: Pick \( a \) and \( b \) so that the fraction \( a/b \) is in lowest terms.)

Exercise 21. Let \( f(x) = 3x^3 - 40x^2 + 97x + 10 \) for all \( x \in \mathbb{R} \).

(a) Find a rational number \( r \) such that \( f(r) = 0 \). (Hint: Use Exercise 20 to narrow down the possibilities for \( r \).)

(b) Find two other numbers \( s \) and \( t \) such that \( f(s) = 0 \) and \( f(t) = 0 \). (Hint: The cubic polynomial \( f(x) \) can be expressed as \((x-r)g(x)\) where \( r \) is as in part (a) and where \( g(x) \) is a quadratic polynomial.)

(c) Explain why \( s \) and \( t \) must be irrational. (There are several ways to do this. One elegant way is to notice that \( g(x) = 3h(x) \), where \( h \) is a quadratic polynomial to which it is particularly easy to apply Exercise 20.)

\(^8\) Here we are taking advantage of the fact that we chose \( b \) to be a natural number. If we had taken \( b \) to be an integer other than a natural number, then at this point we could only conclude that \( b_1 = 1 \) or \( b_1 = -1 \), and similarly that \( b_2 = 1 \) or \( b_2 = -1 \). Then we would get \( b = 1 \) or \( b = -1 \), so \( x = a \) or \( x = -a \). Thus we would still be able to conclude that \( x \) is an integer, but the proof would be a little bit more complicated.
More about Prime Numbers (Optional).

You may be familiar with the fact that a natural number \(x \geq 2\) is prime if and only if no natural number between 2 and \(\sqrt{x}\) divides \(x\). In the next example, we shall prove this. This example illustrates several important points of logic, including how to prove a biconditional sentence, how to prove a universal sentence, and how to draw inferences from a universal sentence.

4.54 Example. Let \(x \in \mathbb{N}\) with \(x \neq 1\) and let \(r \in \mathbb{N}\) with \(r^2 \leq x < (r+1)^2\). Then \(x\) is a prime number iff for each \(d \in \{2, \ldots, r\}\), \(d\) does not divide \(x\).

Proof. The sentence we wish to prove is a biconditional sentence \(P \iff Q\), where \(P\) is “\(x\) is a prime number” and \(Q\) is “for each \(d \in \{2, \ldots, r\}\), \(d\) does not divide \(x\).” The way to prove such a biconditional sentence is to prove the forward implication \(P \Rightarrow Q\) and the reverse implication \(Q \Rightarrow P\). To prove the forward implication, we shall suppose that \(P\) is true and under this assumption we shall prove that \(Q\) is true. To prove the reverse implication, we shall suppose conversely that \(Q\) is true and under this assumption we shall prove that \(P\) is true. In the next two paragraphs, we shall write the proof as it would usually be written, without the long-winded remarks of the present paragraph concerning the general approach. The next paragraph presents the proof of the forward implication and the one after it presents the proof of the reverse implication.

Suppose \(x\) is a prime number. We wish to show that for each \(d \in \{2, \ldots, r\}\), \(d\) does not divide \(x\). Consider any \(d \in \{2, \ldots, r\}\). We wish to show that \(d\) does not divide \(x\). Suppose \(d\) does divide \(x\). Then \(x = kd\) for some integer \(k\). Now \(r < x\), because \(r^2 \leq x\) and \(x > 1\). Hence \(1 < d < x\), so \(1 < k < x\). Thus \(d, k \in \mathbb{N}\), \(x = kd\), \(d \neq 1\), and \(k \neq 1\). But then \(x\) is not prime. This is a contradiction. Thus it must not be the case that \(d\) divides \(x\). This holds for each \(d \in \{2, \ldots, r\}\). This completes the proof of the forward implication.

Conversely, suppose for each \(d \in \{2, \ldots, r\}\), \(d\) does not divide \(x\). Now by assumption, \(x \in \mathbb{N}\) and \(x \neq 1\), so to verify that \(x\) is a prime number, according to the definition, it remains to show that for each \(a \in \mathbb{N}\), for each \(b \in \mathbb{N}\), if \(x = ab\), then \(a = 1\) or \(b = 1\). Consider any \(a \in \mathbb{N}\) and any \(b \in \mathbb{N}\). Suppose \(x = ab\). We wish to show that \(a = 1\) or \(b = 1\). Now since \(a, r \in \mathbb{N}\), either \(a \leq r\) or \(a \geq r + 1\).

Case 1. Suppose \(a \leq r\). We shall show that then \(a = 1\). Suppose \(a \neq 1\). Then \(a \in \{2, \ldots, r\}\), so \(a\) does not divide \(x\). But \(a\) does divide \(x\), because \(x = ba\) and \(b\) is an integer. Thus \(a\) divides \(x\) and \(a\) does not divide \(x\). This is a contradiction. Hence it must be the case that \(a = 1\).

Case 2. Suppose \(a \geq r + 1\). Then \(b = x/a \leq x/(r + 1) < (r + 1)^2/(r + 1) = r + 1\), so since \(b, r \in \mathbb{N}\), \(b \leq r\). We shall show that \(b = 1\). Suppose \(b \neq 1\). Then \(b \in \{2, \ldots, r\}\), so \(b\) does not divide \(x\). But \(b\) does divide \(x\), because \(x = ab\) and \(a\) is an integer. Thus \(b\) divides \(x\) and \(b\) does not divide \(x\). This is a contradiction. Hence it must be the case that \(b = 1\).

Thus in either case, \(a = 1\) or \(b = 1\). This holds for all \(a, b \in \mathbb{N}\) such that \(x = ab\). This completes the proof of the reverse implication.

4.55 Remark. Let \(p \in \{2, 3, 4, \ldots\}\). As we stated in Remark 4.50, if \(p\) is a a prime number, then for all \(x, y \in \mathbb{Z}\), if \(p\) divides \(xy\), then \(p\) divides \(x\) or \(p\) divides \(y\). In the next exercise, you are asked to prove the converse of this.

Exercise 22. Let \(p \in \{2, 3, 4, \ldots\}\). Suppose that for all \(x, y \in \mathbb{Z}\), if \(p\) divides \(xy\), then \(p\) divides \(x\) or \(p\) divides \(y\). Show that \(p\) is prime.

Exercise 23. Is it true that for each \(n \in \mathbb{N}\), the quantity \(n^2 + n + 41\) is a prime number? Either prove that it is true or find a natural number \(n\) such that \(n^2 + n + 41\) is not prime. (Hint: There is an easy solution. Remark: This example was noticed by Leonhard Euler in 1772.)

Goldbach’s Conjecture. Notice that \(4 = 2 + 2\), \(6 = 3 + 3\), \(8 = 3 + 5\), \(10 = 3 + 7 = 5 + 5\), \(12 = 5 + 7\), and so on. These examples suggest that perhaps each even number strictly greater than 2 is a sum of two primes. The assertion that this is so has come to be known as Goldbach’s conjecture. It originated in letters that were exchanged between Christian Goldbach and Leonhard Euler in 1742. Today, more than two and a half centuries later, it still has neither been proved nor refuted. Thus the next exercise provides an intriguing example of a true conditional sentence in which the truth value of the antecedent is not known.
Exercise 24. Prove that if each even number strictly greater than 2 is a sum of two primes, then each odd number strictly greater than 5 is a sum of three primes.

4.56 Remark. Some odd numbers are sums of two primes. These are the numbers of the form \( p + 2 \), where \( p \) is prime. But most odd numbers cannot be written as a sum of two primes. Then smallest odd number that is not a sum of two primes is 11. The smallest nonprime odd number that is not a sum of two primes is 27.

More About Goldbach’s Conjecture. Schnirelman (1939) proved that each even number can be written as a sum of not more than 300,000 primes. Vinogradov (1937, 1954) proved that each odd number greater than or equal to \( 3^{15} \approx 3.25 \times 10^{6.846.168} \) is a sum of three primes. Chen and Wang (1989) improved Vinogradov’s \( 3^{15} \) to \( e^{11.563} \approx 3.33 \times 10^{14.000} \). Oliveira e Silva (2008) verified that each even number between 4 and \( 12 \times 10^{17} \) is a sum of two primes.

Congruences of Integers.

4.57 Definition. Let \( a \), \( b \), and \( m \) be integers. To say that \( a \) is congruent to \( b \) modulo \( m \) (written \( a \equiv b \mod m \)) means that \( m \) divides \( b - a \).

For example, \( 3 \equiv 27 \mod 12 \) because \( 27 - 3 = 24 \) and \( 12 \) divides \( 24 \). Your watch keeps track of time modulo 12. For instance, 3 hours from now is not the same time as 27 hours from now, but the hands of your watch will be in the same position at both times.

4.58 Remark. Let \( x, m \in \mathbb{Z} \). Then \( x \equiv 0 \mod m \) iff \( m \) divides \( x \).

Proof. By the definition of congruence, we have \( x \equiv 0 \mod m \) iff \( m \) divides \( 0 - x \). But \( 0 - x = -x \) and \( m \) divides \( -x \) iff \( m \) divides \( x \). Hence \( x \equiv 0 \mod m \) iff \( m \) divides \( x \). ■

4.59 Remark. Notice that evenness and oddness may be expressed in terms of congruence modulo 2: for each integer \( x \), we have \( x \) is even iff \( x \equiv 0 \mod 2 \), whereas \( x \) is odd iff \( x \equiv 1 \mod 2 \).

4.60 Remark. A minor point to notice is that for all integers \( a \) and \( b \), we have \( a \equiv b \mod 0 \) iff \( a = b \).

4.61 Remark. The relation of congruence modulo \( m \) has certain properties in common with the relation of equality. The relation of equality is reflexive, symmetric, and transitive. In other words,

(a) For each \( a \), we have \( a \equiv a \mod m \). (Reflexivity.)

(b) For all \( a \) and \( b \), if \( a \equiv b \mod m \), then \( b \equiv a \mod m \). (Symmetry.)

(c) For all \( a \), \( b \), and \( c \), if \( a \equiv b \mod m \) and \( b \equiv c \mod m \), then \( a \equiv c \mod m \). (Transitivity.)

In the next exercise, you are asked to prove that on the set of integers, the relation of congruence modulo \( m \) has these properties too.

Exercise 25. Let \( m \in \mathbb{Z} \). Show that the relation of congruence modulo \( m \) is reflexive, symmetric, and transitive. In other words, show that:

(a) For each \( a \in \mathbb{Z} \), we have \( a \equiv a \mod m \). (Reflexivity.)

(b) For all \( a, b \in \mathbb{Z} \), if \( a \equiv b \mod m \), then \( b \equiv a \mod m \). (Symmetry.)

(c) For all \( a, b, c \in \mathbb{Z} \), if \( a \equiv b \mod m \) and \( b \equiv c \mod m \), then \( a \equiv c \mod m \). (Transitivity.)

4.62 Remark. In the next exercise, you are asked to show that congruence modulo \( m \) has two other properties in common with equality. Specifically, you are asked to show that like equations, congruences can be added and multiplied.

Exercise 26. Let \( m, a_1, b_1, a_2, b_2 \in \mathbb{Z} \). Suppose that \( a_1 \equiv b_1 \mod m \) and \( a_2 \equiv b_2 \mod m \).

(a) Prove that \( a_1 + a_2 \equiv b_1 + b_2 \mod m \).

(b) Prove that \( a_1a_2 \equiv b_1b_2 \mod m \). (Hint: Since \( a_1 \equiv b_1 \mod m \), \( m \) divides \( b_1 - a_1 \), so for some integer \( k \), we have \( b_1 - a_1 = km \), so \( b_1 = a_1 + km \). Similarly, for some integer \( \ell \), we have \( b_2 = a_2 + \ell m \).)
4.63 Remark. Let \( m \in \mathbb{Z} \). In Exercise 25 and Exercise 26, you were asked to show that congruence modulo \( m \) has certain properties in common with equality. Now we wish to observe that in an important respect, congruence modulo \( m \) can behave quite differently than equality. As we know, for all \( a, b \in \mathbb{Z} \), if \( ab = 0 \), then \( a = 0 \) or \( b = 0 \). The analogous statement for congruence modulo \( m \) is not always true. For instance, if \( m = 6 \), then \((2)(3) \equiv 0 \mod m\), but \( 2 \not\equiv 0 \mod m \) and \( 3 \not\equiv 0 \mod m \). A related phenomenon is that for congruence modulo \( m \), cancellation does not always work. In other words, if \( u, v, w \in \mathbb{Z} \), \( w \not\equiv 0 \mod m \), and \( uw \equiv vw \mod m \), we cannot always conclude that \( u \equiv v \mod m \). For instance, if \( m = 6 \), then \( 3 \not\equiv 0 \mod m \) and \((5)(3) \equiv (7)(3) \mod m \) (because 6 divides \( 21 - 15 \)), but \( 5 \not\equiv 7 \mod m \).

There is a case when congruence modulo \( m \) does behave like equality with respect to cancellation. It is when \( m \) is prime. To see this, suppose \( m \) is prime. Let \( a, b \in \mathbb{Z} \) such that \( ab \equiv 0 \mod m \). We claim that \( a \equiv 0 \mod m \) or \( b \equiv 0 \mod m \). Since \( ab \equiv 0 \mod m \), we have that \( m \) divides \( ab \). But then since \( m \) is prime, it follows that \( m \) divides \( a \) or \( m \) divides \( b \). Hence \( a \equiv 0 \mod m \) or \( b \equiv 0 \mod m \). Thus we have proved the claim. Now let \( u, v, w \in \mathbb{Z} \) such that \( w \not\equiv 0 \mod m \) and \( uw \equiv vw \mod m \). We claim that \( u \equiv v \mod m \). Since \( uw \equiv vw \mod m \), we have \( uw - vw \equiv vw - vw \mod m \), so \((u - v)w \equiv 0 \mod m \). Hence by the first claim, \( u - v \equiv 0 \mod m \) or \( w \equiv 0 \mod m \). But by assumption, \( w \not\equiv 0 \mod m \). Hence \( u - v \equiv 0 \mod m \), so \((u - v) + v \equiv 0 + v \mod m \), so \( u \equiv v \mod m \). Thus we have proved the second claim.

In the next exercise, you are asked to prove that conversely, if \( p \in \{2, 3, 4, \ldots\} \) and congruence modulo \( p \) behaves like equality with respect to cancellation, then \( p \) is prime.

Exercise 27. Let \( p \in \{2, 3, 4, \ldots\} \). Suppose that for all \( x, y \in \mathbb{Z} \), if \( xy \equiv 0 \mod p \), then \( x \equiv 0 \mod p \) or \( y \equiv 0 \mod p \). Show that \( p \) is prime.

4.64 Remark. In Remark 4.59, we saw that for each integer \( x \), we have \( x \equiv 0 \mod 2 \) iff \( x \) is even, and we have \( x \equiv 1 \mod 2 \) iff \( x \) is odd. Let us consider how this generalizes to the case of congruence modulo \( 3 \). The integers which are of the form \( 3k \) for some integer \( k \) are

\[
\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots
\]

and these are congruent modulo \( 3 \) to \( 0 \). The integers which are of the form \( 3k + 1 \) for some integer \( k \) are

\[
\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots
\]

and these are congruent modulo \( 3 \) to \( 1 \). And the integers which are of the form \( 3k + 2 \) for some integer \( k \) are

\[
\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots
\]

and these are congruent modulo \( 3 \) to \( 2 \). These three sets of integers are called the congruence classes modulo \( 3 \). Each integer belongs to exactly one of these three congruence classes. For each integer \( x \) and for each \( r \in \{0, 1, 2\} \), we have \( x \equiv r \mod 3 \) iff \( x = 3k + r \) for some integer \( k \) iff \( r \) is the remainder that is left after we divide \( 3 \) into \( x \).

4.65 Remark. Now let us consider how Remark 4.64 generalizes to the case of congruence modulo \( m \), where \( m \) is a natural number. For any integer \( x \), we may divide \( m \) into \( x \), to get a unique quotient \( k \in \mathbb{Z} \) and a unique remainder \( r \in \{0, \ldots, m-1\} \), with \( x = mk + r \). This is called the division lemma. Its proof requires induction, so for now we shall just take it for granted. We shall prove it in Section 5. Notice that \( m \) divides \( x \) iff the remainder that is left after we divide \( m \) into \( x \) is \( 0 \). Let \( x_1 \) and \( x_2 \) be integers. Let \( k_1, k_2 \in \mathbb{Z} \) and let \( r_1, r_2 \in \{0, \ldots, m-1\} \) such that \( x_1 = mk_1 + r_1 \) and \( x_2 = mk_2 + r_2 \). In other words, for \( j = 1, 2 \), let \( k_j \) be the quotient and let \( r_j \) be the remainder that we get if we divide \( m \) into \( x_j \). We claim that \( x_1 \equiv x_2 \mod m \) iff \( r_1 = r_2 \). Now either \( r_1 \leq r_2 \) or \( r_2 \leq r_1 \). The two cases are similar, so let us just consider the case where \( r_1 \leq r_2 \). Note that \( x_2 - x_1 = mk_2 + k_1 + (r_2 - r_1) \). Of course \( k_2 - k_1 \) is an integer. Since \( 0 \leq r_1 \leq r_2 \leq m - 1 \), we have \( 0 \leq r_2 - r_1 \leq r_2 - r_1 \leq m - 1 \). But \( r_2 - r_1 \) is an integer, so \( r_2 - r_1 \in \{0, \ldots, m-1\} \). Thus \( r_2 - r_1 \) is the remainder that is left after we divide \( m \) into \( x_2 - x_1 \). Thus \( x_1 \equiv x_2 \mod m \) iff \( m \) divides \( x_2 - x_1 \) iff \( r_2 - r_1 = 0 \) iff \( r_1 = r_2 \). This proves the claim. To summarize, we have shown that two integers are congruent modulo \( m \) if and only if the remainders that are left when the two integers are divided by \( m \) are the same.
4.66 Example. Find the remainder that is left after we divide 9 into 43,657.

Solution. We have $43,657 \equiv 4 \times 10^4 + 3 \times 10^3 + 6 \times 10^2 + 5 \times 10 + 7 \mod 9$. Now $4 \times 10^4 + 3 \times 10^3 + 6 \times 10^2 + 5 \times 10 + 7 = 25$. Next, $25 \equiv 2 + 5 \mod 9$. Of course $2 + 5 = 7$. Therefore $43,657 \equiv 7 \mod 9$, so 7 is the remainder that is left after we divide 9 into 43,657. ■

Exercise 28. If the solution that we just presented for Example 4.66 mystifies you, it is not surprising, because we deliberately left out most of the explanation of why what we did there works. Use Exercise 25 and Exercise 26 to explain why what we did in Example 4.66 works. (Hint: Note that

$$43,657 = 4 \times 10^4 + 3 \times 10^3 + 6 \times 10^2 + 5 \times 10 + 7.$$ 

Now $10 \equiv 1 \mod 9$. Hence, by Exercise 26(b), $10^2 \equiv 1^2 \mod 9$, $10^3 \equiv 1^3 \mod 9$, and $10^4 \equiv 1^4 \mod 9$.)

4.67 Remark. The method that is used in Example 4.66 is called “casting out nines.”

Exercise 29. Find the remainder that is left after we divide 9 into $19,261,024$.

Differences of Squares (Optional).

4.68 Definition. Let $x$ be an integer. To say that $x$ is a difference of squares means that there exist integers $a$ and $b$ such that $x = a^2 - b^2$.

4.69 Remark. Some integers are differences of squares and some are not. For instance, $1 = 1^2 - 0^2$ and $3 = 2^2 - 1^2$, but as we shall see, 2 is not a difference of squares. Of course 0 can be expressed as a difference of squares in infinitely many ways, because $0 = a^2 - a^2$ for each integer $a$, but that is not very interesting.

4.70 Remark. Ways of expressing an integer as a difference of squares are related to special ways of factoring it. Recall that $a^2 - b^2 = (a + b)(a - b)$. Suppose $x = a^2 - b^2$, where $a$ and $b$ are integers. Then $x = uv$ where $u = a + b$ and $v = a - b$. Notice that $u + v = 2a$ and $u - v = 2b$. Thus $u + v$ and $u - v$ are both even, $a = (u + v)/2$, and $b = (u - v)/2$. Conversely, we have the following result.

Exercise 30. Let $x$ be an integer. Suppose $x = uv$, where $u$ and $v$ are integers.

(a) Prove that $x = a^2 - b^2$ where $a = (u + v)/2$ and $b = (u - v)/2$.

(b) Prove that if at least one of $u + v$ and $u - v$ is even, then both are even, so that $a$ and $b$ are both integers and $x$ is a difference of squares.

4.71 Remark. Thus ways of expressing $x$ as a difference of squares correspond to ways of expressing $x$ as a product of two integers whose sum is even.

Exercise 31. Use the preceding analysis to prove that the following is an exhaustive listing of all the ways to write natural numbers from 1 through 15 as differences of squares of nonnegative integers:

\begin{align*}
1 &= 1^2 - 0^2 \\
3 &= 2^2 - 1^2 \\
4 &= 2^2 - 0^2 \\
5 &= 3^2 - 2^2 \\
7 &= 4^2 - 3^2 \\
8 &= 3^2 - 1^2 \\
9 &= 3^2 - 0^2 = 5^2 - 4^2 \\
11 &= 6^2 - 5^2 \\
12 &= 4^2 - 2^2 \\
13 &= 7^2 - 6^2 \\
15 &= 4^2 - 1^2 = 8^2 - 7^2
\end{align*}

In particular, 2, 6, 10, and 14 are not differences of squares.
Thus Exercise 34. which integers are differences of squares, and so on. These terms should be self-explanatory and we shall not trouble to define them formally.

4.73 Example. Let \( x \) be an integer. Prove that \( x \) is a difference of consecutive squares if and only if \( x \) is odd.

Solution. Suppose \( x \) is a difference of consecutive squares. Then \( x = (k+1)^2 - k^2 \) for some integer \( k \). Now \( (k+1)^2 - k^2 = 2k + 1 \). Thus \( x \) is odd.

Conversely, suppose \( x \) is odd. Then \( x = 2k + 1 \) for some integer \( k \). Now \( 2k + 1 = (k+1)^2 - k^2 \). Thus \( x \) is a difference of consecutive squares. ■

4.74 Example. Let \( x \) be a nonnegative integer and suppose \( x \) is a difference of nonconsecutive squares. Prove that \( x \geq 4 \) and \( x \) is not prime.

Solution. Since \( x \geq 0 \) and \( x \) is a difference of nonconsecutive squares, there exist integers \( a \) and \( b \) such that \( x = a^2 - b^2 \), \( b \geq 0 \), and \( a \geq b + 2 \). Then \( x = (a - b)(a + b) \), \( a - b \geq 2 \), and \( a + b \geq b + 2 + b \geq 2 \).

Hence \( x \geq (2)(2) = 4 \). Also, \( x \) factors nontrivially, so \( x \) is not prime. ■

4.75 Remark. Let \( x \) be an integer. Notice that \( x \) is a difference of squares if and only if \(-x\) is a difference of squares, for the trivial reason that \(-a^2 - b^2 = b^2 - a^2\). Notice also that if \( x = a^2 - b^2 \), where \( a \) and \( b \) are integers, then \(-a \) and \(-b \) are also integers, \((-a)^2 = a^2 \), \((-b)^2 = b^2 \), and \( x = \pm a^2 - \pm b^2 \). Thus to understand all ways of expressing integers as differences of squares, it is enough to understand all ways of expressing nonnegative integers as differences of squares of nonnegative integers.

4.76 Remark. If \( x \) is a nonnegative integer, then by the number of ways of expressing \( x \) as a difference of squares we mean the number of ways of expressing \( x \) as a differences of squares of nonnegative integers.

Exercise 32. (Fermat, 1643.) Let \( x \) be an integer. Suppose \( x \geq 3 \), \( x \) is odd, and \( x \) can be expressed as a difference of squares in only one way. Prove that \( x \) is prime.

Exercise 33. Let \( x \) be an integer.
   (a) Prove that \( x \) is an odd square minus an even square if and only if \( x \equiv 1 \mod 4 \).
   (b) Prove that \( x \) is an even square minus an odd square if and only if \( x \equiv -1 \mod 4 \).
   (c) Prove that if \( x \) is a difference of even squares, then \( x \) is divisible by 4.
   (d) Prove that if \( x \) is a difference of odd squares, then \( x \) is divisible by 4.
   (e) By parts (c) and (d), if \( x \) is a difference of squares that are both even or both odd, then \( x \) is divisible by 4. Prove that conversely, if \( x \) is divisible by 4, then \( x \) is a difference of squares that are both even or both odd.
   (f) Deduce from earlier parts of this exercise that \( x \) is a difference of squares if and only if \( x \) is not congruent to 2 modulo 4.

4.77 Remark. As we saw in Exercise 31, the integers from 0 to 15 that are not differences of squares are 2, 6, 10, and 14. Notice that these are also the integers from 0 to 15 that are congruent to 2 modulo 4, as they must be by Exercise 33(f).

4.78 Remark. As we’ve observed, 0 and 8 are differences of odd squares. The next exercise tells us exactly which integers are differences of odd squares.

Exercise 34. Let \( x \) be an integer.
   (a) Prove that if \( x \) is an odd square, then \( x \equiv 1 \mod 8 \). (Hint: Review Exercise 3.)
   (b) Prove that if \( x \) is a difference of odd squares, then \( x \equiv 0 \mod 8 \). Deduce that \( x \) is divisible by 8. (This sharpens the conclusion of Exercise 33(d).)
   (c) Conversely, prove that if \( x \) is divisible by 8, then \( x \) is a difference of odd squares. Thus \( x \) is a difference of odd squares if and only if \( x \) is divisible by 8.

4.79 Remark. As we’ve observed, 0 and 4 are differences of even squares. Since \( 12 = 4^2 - 2^2 \) and \( 16 = 4^2 - 0^2 \), 12 and 16 are also differences of even squares. The next exercise tells us exactly which integers are of this type.
Exercise 35. Let $x$ be an integer. Prove that $x$ is a difference of even squares if and only if $x$ is congruent to 0, 4, or 12 modulo 16.

4.80 Remark. As we’ve observed, 0 is a difference of even squares and 0 is also a difference of odd squares, because $0 = 0^2 - 0^2 = 1^2 - 1^2$. Two other such examples are 16 and 32, because $16 = 4^2 - 0^2 = 5^2 - 3^2$ and $32 = 6^2 - 2^2 = 9^2 - 7^2$. The next exercise tells us exactly which integers are of this type.

Exercise 36. Let $x$ be an integer.

(a) Prove that if $x$ is a difference of even squares and $x$ is also a difference of odd squares, then $x$ is divisible by 16.
(b) Prove that if $x$ is divisible by 16, then $x$ is a difference of even squares and $x$ is also a difference of odd squares.

Exercise 37. Let $x$ be an integer.

(a) Prove that $x$ is a difference of even squares but not a difference of odd squares if and only if $x \equiv 4 \mod 8$.
(b) Prove that $x$ is a difference of odd squares but not a difference of even squares if and only if $x \equiv 8 \mod 16$.

Exercise 38.

(a) Let $z$ be an integer. Prove that $z \equiv 2 \mod 4$ iff $z$ is even and $z/2$ is odd.
(b) Let $x$ and $y$ be integers. Suppose $xy \equiv 2 \mod 4$. Prove that $x \equiv 2 \mod 4$ or $y \equiv 2 \mod 4$.
(c) Use part (b) and Exercise 33(f) to prove that if $x$ and $y$ are differences of squares, then $xy$ is a difference of squares. Thus the set of integers which are differences of squares is closed under multiplication.
(d) Verify the identity

$$(a^2 - b^2)(c^2 - d^2) = (ac - bd)^2 - (ad - bc)^2.$$  

(Suggestion: To keep the calculation from getting messy, let $u = ac - bd$ and $v = ad - bc$. Notice that then $(ac - bd)^2 - (ad - bc)^2 = u^2 - v^2 = (u + v)(u - v)$. It should be easy to check that this is $(a - b)(c + d)(a + b)(c - d)$ and that this in turn is $(a^2 - b^2)(c^2 - d^2)$.)

(e) Use part (d) to give a second proof that if $x$ and $y$ are differences of squares, then $xy$ is a difference of squares.

4.81 Remark. There are many other facts which can be proved about differences of squares. For instance, there are theorems about the number of ways in which an integer can be expressed as a difference of squares, about which integers can be expressed as a difference of squares which have no common divisors other than 1 and −1, and so on. These topics are commonly treated in textbooks on number theory.

General Guidelines for Constructing Proofs.

While it does require inventiveness to write proofs, the majority of steps in most proofs are remarkably predictable. If you pay attention to the kind of sentence you are trying to prove, the appropriate next step will often be obvious. We now list the proof techniques that are based on this strategy. Each of these techniques is a way to reduce what you are trying to prove to something that may be simpler to prove.

• To prove a biconditional sentence $P \iff Q$, prove each of the conditional sentences $P \implies Q$ and $Q \implies P$.

In such a proof of $P \iff Q$, the proof of $P \implies Q$ is called the proof of the forward implication and the proof of $Q \implies P$ is called the proof of the reverse implication.

• Conditional proof. To prove a conditional sentence $P \implies Q$, assume $P$ (temporarily) and prove $Q$. (Words such as assume, suppose, and let signal the introduction of assumptions.) Once you have proved $Q$ under the assumption $P$ together with whatever other assumptions $A_1, \ldots, A_n$ are currently in effect, then you have proved $P \implies Q$ under the assumptions $A_1, \ldots, A_n$ alone. The assumption $P$ is then no longer in effect and is said to have been discharged. (See also proof by contraposition.)

• One way to prove a disjunctive sentence $P \lor Q$ is to prove $P$ or prove $Q$. (If it is not obvious how to prove either $P$ or $Q$ alone, then you should try proof by contradiction, which is discussed below.)
• **Existential generalization.** One way to prove an existential sentence \((\exists x)P(x)\) is to find a value of \(x\), say \(x_0\), such that \(P(x_0)\) is true. (If it is not obvious how to find such a value of \(x\), then you should try proof by contradiction.)

• To prove a conjunctive sentence \(P \land Q\), prove \(P\) and prove \(Q\).

• **Universal generalization.** To prove a universal sentence \((\forall x)P(x)\), consider any \(x_0\) and prove \(P(x_0)\). (The phrase “consider any \(x_0\)” means let \(x_0\) be a variable about which nothing is assumed. Thus \(x_0\) must a variable that is not already in use in the proof.)

• **Proof of existence and uniqueness.** To prove that there exists a unique \(x\) such that \(P(x)\), first prove the existential sentence \((\exists x)P(x)\), as explained above under existential generalization, and then prove the sentence

\[
(\forall x_1)(\forall x_2)(P(x_1) \land P(x_2) \Rightarrow x_1 = x_2).
\]

The way to prove the latter sentence is to use universal generalization and conditional proof. Specifically, consider any \(x_1\) and any \(x_2\), assume that \(P(x_1)\) and \(P(x_2)\) are both true, and under this assumption, prove that \(x_1 = x_2\).

• To prove a negative sentence \(\neg P\), assume \(P\) (temporarily) and prove a contradiction \(Q \land \neg Q\). Once you have proved a contradiction under the assumption \(P\) together with whatever other assumptions \(A_1, \ldots, A_n\) are currently in effect, then you have proved \(\neg P\) under the assumptions \(A_1, \ldots, A_n\) alone. The assumption \(P\) is then no longer in effect and is said to have been discharged.

• **Proof by contradiction.** To prove a sentence \(R\) by contradiction, assume \(\neg R\) (temporarily) and prove a contradiction \(Q \land \neg Q\). Once you have proved a contradiction under the assumption \(\neg R\) together with whatever other assumptions \(A_1, \ldots, A_n\) are currently in effect, then you have proved \(\neg \neg R\) under the assumptions \(A_1, \ldots, A_n\) alone. (The assumption \(\neg R\) has been discharged.) Then \(R\) follows because it is logically equivalent to \(\neg \neg R\). Proof by contradiction may be appropriate when you are trying to prove a disjunctive sentence \(P \lor Q\) or an existential sentence \((\exists x)P(x)\). A third case where proof by contradiction may be appropriate is when you are trying to prove a sentence that cannot be broken down into shorter sentences. For example, the sentence “\(x^2 = y\)” cannot be broken down into shorter sentences. Neither can the sentence “\(x \in A\).” Such sentences are called “atomic” sentences. (If the sentence you are trying to prove is neither disjunctive, existential, nor atomic, then proof by contradiction may not be wrong but it will be a detour.) When you are trying to prove a disjunctive sentence \(P \lor Q\) by contradiction, you should remember that \(\neg(P \lor Q)\) is logically equivalent to \(\neg P \land \neg Q\). When you are trying to prove an existential sentence \((\exists x)P(x)\) by contradiction, you should remember that \(\neg(\exists x)P(x)\) is logically equivalent to \((\forall x)\neg P(x)\). A variation on the use of proof by contradiction to prove a disjunctive sentence \(P \lor Q\) is to assume \(\neg P\) and prove \(Q\), or to assume \(\neg Q\) and prove \(P\).

• **Proof by contraposition.** This method of proof is based on the fact that a conditional sentence \(P \Rightarrow Q\) is logically equivalent to its contrapositive \(\neg Q \Rightarrow \neg P\). To prove a conditional sentence \(P \Rightarrow Q\) by contraposition, assume \(\neg Q\) (temporarily) and prove \(\neg P\). This method of proof is a shortcut in certain cases, not an indispensable proof technique. To prove \(P \Rightarrow Q\), one may always start by assuming \(P\) and trying to prove \(Q\). If you then get stuck, you might try assuming \(\neg Q\) in addition and try to prove a contradiction. If from \(\neg Q\) you manage to prove \(\neg P\), then from \(P\) you get the contradiction \(P \land \neg P\). If your proof of \(\neg P\) from \(\neg Q\) did not use \(P\), then you can shorten your argument by using proof by contraposition.

At each step in a proof, you must decide whether to apply one of the preceding techniques, or whether to use some of the things that are already known (or are given, or have been temporarily assumed). We now list the techniques to use the things that are known (or given, or temporarily assumed).

• If you know that a biconditional sentence \(P \Leftrightarrow Q\) is true, then you may conclude that the conditional sentence \(P \Rightarrow Q\) is true and you may also conclude that the conditional sentence \(Q \Rightarrow P\) is true.

• **Modus ponens.** If you know that a conditional sentence \(P \Rightarrow Q\) is true and you also know that the sentence \(P\) is true, then you may conclude that the sentence \(Q\) is true.

• If you know that a conjunctive sentence \(P \land Q\) is true, then you may conclude that the sentence \(P\) is true and you may also conclude that the sentence \(Q\) is true.
• **Universal instantiation.** If you know that a universal sentence \((\forall x)P(x)\) is true, then whatever \(x_0\) may be, you may conclude that \(P(x_0)\) is true.

• **Dilemma.** If you know that a disjunctive sentence \(P \lor Q\) is true, then at least one of the sentences \(P\) and \(Q\) is true. Hence you should consider two cases: first, the case where \(P\) is true, and second, the case where \(Q\) is true. If you succeed in proving the same conclusion \(R\) in each case, then you have shown that \(R\) follows from \(P \lor Q\). Notice that in the first case, \(P\) is a temporary assumption which is discharged at the conclusion of the case. In the second case, \(Q\) is a temporary assumption which is discharged at the conclusion of the case. By the way, it is usually not necessary to consider separately the case where both of \(P\) and \(Q\) are true, since in the case where \(P\) is true, it usually does not matter whether \(Q\) is true or false, and in the case where \(Q\) is true, it usually does not matter whether \(P\) is true or false.

• **Existential instantiation.** If you know that an existential sentence \((\exists x)P(x)\) is true, then you may pick a value of \(x\), say \(x_0\), such that \(P(x_0)\) is true. (The variable \(x_0\) should be a variable about which nothing except \(P(x_0)\) is assumed. Thus \(x_0\) must a variable that is not already in use in the proof.)

• **The Law of the Excluded Middle.** It sometimes helps to remember that no matter what the sentence \(P\) is, the sentence \(P \lor \neg P\) is true. Thus at any stage in a proof, you can pick some relevant sentence \(P\) and say “Either \(P\) is true or \(P\) is not true.” Then as in Dilemma, you should consider the case where \(P\) is true and then the case where \(P\) is not true.

It is worth remarking that the main place where inventiveness is needed in writing proofs is in deciding which known things to use and when to use them. As you work out a proof, you should keep track of which given information you have already used and you should be alert to opportunities to make further use of the given information, especially the given information that you have not yet used. But the greatest inventiveness is needed to decide which known things to use which are not among the pieces of information that are given in the problem.

Of course you will need to work through plenty of examples and exercises to develop a genuine understanding of the proof techniques that are summarized above. But maybe this summary will help you to see the logical patterns in proofs.

By the way, in the rules for existential generalization, universal generalization, universal instantiation, and existential instantiation, there are some restrictions that we did not mention concerning the use of variables. Suffice it to say that these restrictions have to do with avoiding using the same variable for more than one purpose at the same time. If you just use variables in the natural way, you should not encounter problems with these restrictions.

**Natural Deduction.** In mathematical logic, there are a number of different though equivalent formalizations of the basic rules of reasoning. The one which corresponds most closely to how we usually reason was published by the German logician Gerhard Gentzen in 1935 and is fittingly called *natural deduction*. The guidelines for constructing proofs given immediately above are essentially Gentzen’s rules for natural deduction, informally stated.

---

**Section 5. Induction**

In this section we shall discuss the method of proof by mathematical induction and some related matters. As we have seen, one way to prove a universal sentence \((\forall x \in A)P(x)\) is to consider an arbitrary \(x_0\) in \(A\) and to prove \(P(x_0)\). In the case where the set \(A\) is the set \(\mathbb{N} = \{1, 2, 3, \ldots\}\) of natural numbers, there is another common method to prove such a universal sentence. This is the method of proof by mathematical induction or more briefly, proof by induction. The basis for proof by induction is the principle of mathematical induction, which we now state.

**5.1 The Principle of Mathematical Induction.** Let \(P(n)\) be any statement about \(n\). Suppose we have proved that

\[
P(1) \text{ is true}
\]  

(1)