Mathematics 3345

Autumn Semester

2022

THE FUNDAMENTALS OF HIGHER MATHEMATICS

Neil Falkner

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

Contents

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:

$$\text{Paris is the capital of France.}$$
$$1 + 3 = 4.$$
$$5 < 7.$$

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

$$\text{The moon is made of green cheese.}$$
$$2 + 3 = 4.$$
$$7 < 5.$$

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 $\neg$, $\wedge$, $\vee$, $\Rightarrow$, 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 $P \wedge Q$ stands for the sentence "Jill likes Jack and Mary had a little lamb." The expression $P \vee Q$ stands for the sentence "Jill likes Jack or Mary had a little lamb." The expression $P \Rightarrow Q$ stands for "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 $\neg P$, $P \wedge Q$, $P \vee Q$, $P \Rightarrow Q$, and $P \Leftrightarrow Q$ stand for change accordingly.

It should be understood that the meanings of the symbols $\neg$, $\wedge$, $\vee$, 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 $\neg$, $\wedge$, $\vee$, $\Rightarrow$, 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 $\neg$, $\wedge$, $\vee$, $\Rightarrow$, 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 $\neg$, $\wedge$, $\vee$, $\Rightarrow$, 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:

P	$\neg P$
T	F
F	T

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 $\neg P$ is false, so $\neg\neg P$ is true, whereas if P is false, then $\neg P$ is true, so $\neg\neg P$ is false. Thus whatever the truth value of P may be, the truth value of $\neg\neg P$ is the same. We describe this situation by saying that $\neg\neg P$ *is logically equivalent to* P. (The order is not important. One may equally well say that P is logically equivalent to $\neg\neg P$.) 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, $P \equiv \neg\neg P$. It is good to keep in mind that while the symbols $\neg$, $\wedge$, $\vee$, $\Rightarrow$, and $\Leftrightarrow$ 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 $A \wedge B$ 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 $\neg P$, 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 $\neg P$, because P is logically equivalent to $\neg\neg P$, which is the negation of $\neg P$. However P is not the negation of $\neg P$.

Here is an example to illustrate the difference between the logical meaning of $\neg$ 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 $\neg$ in logic. Nevertheless, the logical definition of $\neg$ does correspond to the way the word "not" is generally used in mathematics.

Conjunction. Recall that the symbol $\wedge$ is supposed to correspond to the word "and." Given sentences P and Q, the sentence $P \wedge Q$ 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 $P \wedge Q$, where P and Q are some other sentences, and we call the sentences P and Q the *conjunctands* in the sentence R. The meaning of $\wedge$ in logic is defined by the following rule: *Given sentences* P *and* Q*, the sentence* $P \wedge Q$ *is considered to be true just when both of* P *and* Q *are true. If at least one of them is false, then* $P \wedge Q$ *is considered to be false.* Once again, we summarize the logical definition of $\wedge$ in a truth table:

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

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,

TF, FT, and FF. (In the truth table for $\neg P$, we also ordered the lines so that the truth values of the single basic propositional variable P would be listed in reverse alphabetical order: T, F.)

Notice that whatever the truth values of P and Q may be, the sentence $Q \wedge P$ has the same truth value as the sentence $P \wedge Q$, because each of the latter two sentences is true just when both of P and Q are true. Thus $Q \wedge P$ is logically equivalent to $P \wedge Q$. Sometimes one describes this situation by saying that $\wedge$ is *commutative*. It is also true that $\wedge$ is *associative*. This means that $P \wedge (Q \wedge R)$ is logically equivalent to $(P \wedge Q) \wedge R$. (To see this, notice that $P \wedge (Q \wedge R)$ is true just when all three of P, Q, R are true, and that the same holds for $(P \wedge Q) \wedge R$.) Since $\wedge$ is associative, we may omit parentheses in $P \wedge Q \wedge R$.

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 $\wedge$ 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 consider as objects.) In logic, $\wedge$ connects only sentences. This is another difference between the logical meaning of $\wedge$ and the meaning of "and" in ordinary English.

Disjunction. Recall that the symbol $\vee$ is supposed to correspond to the word "or." Given sentences P and Q, the sentence $P \vee Q$ 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 $P \vee Q$, where P and Q are some other sentences, and we call the sentences P and Q the *disjunctands* in the sentence R. The meaning of $\vee$ in logic is defined by the following rule: *Given sentences P and Q, the sentence $P \vee Q$ 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 $\vee$ in a truth table:

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

Thus $P \vee Q$ is false just when both of P and Q are false. In particular, if P and Q are both true, then $P \vee Q$ is considered to be true. Thus $\vee$ 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 $\vee$ for "or" in logic is derived from the first letter of "vel." (And the symbol $\wedge$ for "and" in logic is simply an upside down $\vee$.)

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

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 $\neg$, $\wedge$, and $\vee$. 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) *$\neg(P \wedge Q)$ is logically equivalent to $\neg P \vee \neg Q$.*

(b) *$\neg(P \vee Q)$ is logically equivalent to $\neg P \wedge \neg Q$.*

Proof. First we should point out that $\neg P \vee \neg Q$ means $(\neg P) \vee (\neg Q)$. Similarly, $\neg P \wedge \neg Q$ means $(\neg P) \wedge (\neg Q)$. Now we can see (a) by inspecting the following truth table:

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

The point is that the column of truth values headed by $\neg(P \wedge Q)$ is the same as the column of truth values headed by $\neg P \vee \neg Q$.

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 $\neg(P \wedge Q)$ is true. Then the sentence $P \wedge Q$ is false, so at least one of the sentences P and Q is false, so at least one the sentences $\neg P$ and $\neg Q$ is true, so the sentence $\neg P \vee \neg Q$ is true. This shows that if the sentence $\neg(P \wedge Q)$ is true, then the sentence $\neg P \vee \neg Q$ is true.

Conversely, suppose the sentence $\neg P \vee \neg Q$ is true. Then at least one of the sentences $\neg P$ and $\neg Q$ is true, so at least one of the sentences P and Q is false, so the sentence $P \wedge Q$ is false, so the sentence $\neg(P \wedge Q)$ is true. This shows that if the sentence $\neg P \vee \neg Q$ is true, then the sentence $\neg(P \wedge Q)$ is true.

It follows that the sentence $\neg(P \wedge Q)$ is true exactly when the sentence $\neg P \vee \neg Q$ is true. (Then by elimination, the sentence $\neg(P \wedge Q)$ is false exactly when the sentence $\neg P \vee \neg Q$ is false.) Therefore the sentence $\neg(P \wedge Q)$ is logically equivalent to the sentence $\neg P \vee \neg Q$.

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 where $\neg(P \wedge Q)$ is true, $\neg P \vee \neg Q$ is also true. The second paragraph of the explanation in words shows that in each line of the truth table where $\neg P \vee \neg Q$ is true, $\neg(P \wedge Q)$ is also true. It follows that $\neg(P \wedge Q)$ is true in exactly the same lines of the truth table where $\neg P \vee \neg Q$ is true. (Then by elimination, $\neg(P \wedge Q)$ is false in exactly the same lines of the truth table where $\neg P \vee \neg Q$ is false.) Hence in every line of the truth table, $\neg(P \wedge Q)$ has the same truth value as $\neg P \vee \neg Q$. Therefore $\neg(P \wedge Q)$ is logically equivalent to $\neg P \vee \neg Q$.

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 $\neg R$, 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 $\neg R$, 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 $(1 \leq x) \wedge (x < 3)$. Hence, by De Morgan's first law, the sentence $\neg(1 \leq x < 3)$ is logically equivalent to the sentence $\neg(1 \leq x) \vee \neg(x < 3)$. But since x is a real number, the sentence $\neg(1 \leq x)$ is logically equivalent to the sentence $x < 1$, and the sentence $\neg(x < 3)$ is logically equivalent to the sentence $x \geq 3$. Hence the sentence $\neg(1 \leq x < 3)$ is logically equivalent to the sentence $(x < 1) \vee (x \geq 3)$. With the help of our abbreviation "$\equiv$" for the phrase

"is logically equivalent to," we may summarize this argument as follows:

$$\begin{aligned}\neg(1 \le x < 3) &\equiv \neg[(1 \le x) \wedge (x < 3)] \\ &\equiv \neg(1 \le x) \vee \neg(x < 3) \\ &\equiv (x < 1) \vee (x \ge 3).\end{aligned}$$

In other words, to say that it is not the case that $1 \le x < 3$ is logically equivalent to saying that either $x < 1$ or $x \ge 3$. Another way to see this is to think in terms of the real number line. To say that $1 \le x < 3$ means that x lies between 1 and 3 (and $x \ne 3$ but maybe $x = 1$.) Hence to say that $\neg(1 \le x < 3)$ 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) *$P \wedge (Q \vee R)$ is logically equivalent to $(P \wedge Q) \vee (P \wedge R)$.*

(b) *$P \vee (Q \wedge R)$ is logically equivalent to $(P \vee Q) \wedge (P \vee R)$.*

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:

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

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

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 $P \vee (Q \wedge R)$ is true. Then at least one of the two sentences P and $Q \wedge R$ is true.[1]

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

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

Thus in either case, the sentence $(P \vee Q) \wedge (P \vee R)$ is true.[2] We have shown that if the sentence $P \vee (Q \wedge R)$ is true, then the sentence $(P \vee Q) \wedge (P \vee R)$ is true.

Conversely, suppose the sentence $(P \vee Q) \wedge (P \vee R)$ is true. Then both of the sentences $P \vee Q$ and $P \vee R$ 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 $Q \wedge R$ 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 $Q \wedge R$ 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 $Q \wedge R$ 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 $P \vee (Q \wedge R)$ is true.

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

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

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

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 $P \wedge (Q \vee R)$ is not logically equivalent to the sentence $(P \wedge Q) \vee R$. 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 $P \vee Q$ 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:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

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:

	P	Q	$P \Rightarrow Q$
$x < 1$	T	T	T
$1 \leq x < 3$	F	T	T
$x \geq 3$	F	F	T

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.

A 2 X 3

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/

Vacuously True Conditional Sentences. Sometimes a conditional sentence $P \Rightarrow Q$ which is true just because the sentence P happens to be false is said to be *vacuously true*. For instance, the sentence "If wishes were horses, then beggars would ride" is vacuously true because wishes are not horses. For a mathematical example, when $x = 2$, the sentence "If $x < 1$, then $x < 3$" is vacuously true because it is not the case that $2 < 1$.

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, "$P \Rightarrow Q$" 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 "$(x > 2) \Rightarrow (x^2 > 4)$," we may not infer that $x^2 > 4$. 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 "$P \wedge (P \Rightarrow Q)$," rather than by "$P \Rightarrow Q$." For instance, if we write "$x > 2$, so $x^2 > 4$," we mean that $x > 2$ and therefore $x^2 > 4$.

In this chapter, we are concerned more with studying logic than with applying logic. Beginning with the next chapter, we shall be concerned more with applying what we have learned about logic in this chapter than with studying 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 "$P \Rightarrow Q$."

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:

$$\text{If } x > 2, \text{ then } x^2 > 4. \text{ Therefore } x^4 > 16. \tag{1}$$

Now here is a good way to write it:

$$\text{Suppose } x > 2. \text{ Then } x^2 > 4. \text{ Therefore } x^4 > 16. \tag{2}$$

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 $x^2 > 4$," so the conclusion "$x^4 > 16$" is justified in (2) but is not justifed in (1). Of course, since the argument in (2) is quite short, it is practical to express it in a single sentence such as

$$\text{If } x > 2, \text{ then } x^2 > 4, \text{ so } x^4 > 16.$$

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 $\neg(P \Rightarrow Q)$ is logically equivalent to $P \wedge \neg Q$.*

Proof. Suppose $\neg(P \Rightarrow Q)$ is true. Then $P \Rightarrow Q$ is false, so P is true and Q is false. Since Q is false, $\neg Q$ is true. Thus both of the sentences P and $\neg Q$ are true, so the sentence $P \wedge \neg Q$ is true.

Conversely, suppose the sentence $P \wedge \neg Q$ is true. Then both of the sentences P and $\neg Q$ are true. Since $\neg Q$ is true, Q is false. Thus P is true and Q is false, so $P \Rightarrow Q$ is false, so $\neg(P \Rightarrow Q)$ 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 $\neg A$ is logically equivalent to "$x + y > 0$ and $x \leq 0$ and $y \leq 0$." 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 $\neg A$ true? Explain why.

(c) Let B be the sentence "If $x + y > 2$, then $x > 2$ or $y > 2$." Is B true, or is $\neg B$ 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 $\neg B$ 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 true.)

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

$$a_1 + a_2 + a_3 + \cdots \tag{3}$$

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 $P \Leftarrow Q$ instead of $Q \Rightarrow P$. Here are three synonymous ways to read $P \Leftarrow Q$:

P is implied by Q.
P is necessary for Q.
P if Q.

Biconditional Sentences. A sentence of the form $P \Leftrightarrow Q$ is called a biconditional sentence. Recall that $P \Leftrightarrow Q$ 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 $\Leftrightarrow$ in logic is defined by the following rule: *Given two sentences P and Q, the sentence $P \Leftrightarrow Q$ 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 $\Leftrightarrow$ in a truth table:

P	Q	$P \Leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

Notice that the sentence $P \Leftrightarrow Q$ 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 $P \Leftrightarrow Q$ 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:

$$\begin{aligned} & x^2 = 1 \\ \text{iff} \quad & x^2 - 1 = 0 \\ \text{iff} \quad & (x-1)(x+1) = 0 \\ \text{iff} \quad & x - 1 = 0 \text{ or } x + 1 = 0 \\ \text{iff} \quad & x = 1 \text{ or } x = -1. \end{aligned}$$

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 $P \Leftrightarrow Q$ is logically equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$.*

Proof. Consider the following truth table:

P	Q	$P \Leftrightarrow Q$	$P \Rightarrow Q$	$Q \Rightarrow P$	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$
T	T	T	T	T	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T

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

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

Since $P \Leftrightarrow Q$ is logically equivalent to $(P \Leftarrow Q) \wedge (P \Rightarrow Q)$, we see that $P \Leftrightarrow Q$ is also logically equivalent to "(P is necessary for Q) $\wedge$ (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 $P \Leftrightarrow Q$ is logically equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$, 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 $P \Leftrightarrow Q$, 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 $P \operatorname{xor} Q$ mean "P exclusive or Q." In other words, $P \operatorname{xor} Q$ should be true just when exactly one of P and Q is true.

(a) Write out the truth table table for $P \operatorname{xor} Q$.

(b) Show by a truth table that $P \operatorname{xor} Q$ is logically equivalent to $(P \wedge \neg Q) \vee (Q \wedge \neg P)$.

(c) Show by truth tables that the following four sentences are logically equivalent:

$$P \operatorname{xor} Q, \quad \neg(P \Leftrightarrow Q), \quad (\neg P) \Leftrightarrow Q, \quad P \Leftrightarrow (\neg Q).$$

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

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 $P \wedge (Q \vee R)$ is not logically equivalent to the sentence $(P \wedge Q) \vee R$. 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 $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$. Thus for instance, $\neg P \wedge \neg Q$ means $(\neg P) \wedge (\neg Q)$. We already used this in our discussion of De Morgan's laws (Theorem 2.1). Here are some more examples:

$$\begin{aligned} P \wedge Q \vee R \quad &\text{means} \quad (P \wedge Q) \vee R \\ P \wedge Q \Rightarrow P \vee Q \quad &\text{means} \quad (P \wedge Q) \Rightarrow (P \vee Q) \\ P \Rightarrow (Q \Rightarrow R) \Leftrightarrow P \wedge Q \Rightarrow R \quad &\text{means} \quad [P \Rightarrow (Q \Rightarrow R)] \Leftrightarrow [(P \wedge Q) \Rightarrow R] \end{aligned}$$

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 *in*equivalent:

(a) $P \Rightarrow (Q \Rightarrow R)$;

(b) $(P \Rightarrow Q) \Rightarrow R$;

(c) $(P \Rightarrow Q) \wedge (Q \Rightarrow R)$.

(Hint: To show that two sentences are logically inequivalent, it suffices to find one choice of truth values for 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

$$P \Rightarrow Q \Rightarrow R. \tag{4}$$

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

$$(P \Rightarrow Q) \wedge (Q \Rightarrow R).$$

For instance, they might write

$$x > 2 \Rightarrow x^2 > 4 \Rightarrow x^2 + 3 > 7.$$

However, one should not write something like

$$x > 2 \Rightarrow x^2 > 4 \Rightarrow x^2 + x > 6. \tag{5}$$

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

$$\text{If } x > 2, \text{ then } x^2 > 4, \text{ so } x^2 + x > 4 + 2 = 6.$$

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

$$P \Rightarrow Q \Rightarrow R \Rightarrow S. \tag{6}$$

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

$$(P \Rightarrow Q) \wedge (Q \Rightarrow R) \wedge (R \Rightarrow S).$$

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

$$x > 2 \Rightarrow x^2 > 4 \Rightarrow x^2 + 3 > 7 \Rightarrow (x^2 + 3)^2 > 49. \tag{7}$$

But it would be bad to write

$$x > 2 \Rightarrow x^2 > 4 \Rightarrow x^2 + 3 > 7 \Rightarrow x^2 + x + 3 > 9, \tag{8}$$

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

$$\text{If } x > 2, \text{ then } x^2 > 4, \text{ so } x^2 + 3 > 7, \text{ so } x^2 + x + 3 > 9.$$

And a better way to write (7) is

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

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 $P \Leftrightarrow (Q \Leftrightarrow R)$ is logically equivalent to the sentence $(P \Leftrightarrow Q) \Leftrightarrow R$, but that neither of these sentences is logically equivalent to the sentence $(P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R)$. (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 $\Leftrightarrow$ 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

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

without parentheses, they usually mean

$$(P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R), \tag{10}$$

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

$$P \Leftrightarrow Q \Leftrightarrow R \Leftrightarrow S$$

they usually mean

$$(P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R) \wedge (R \Leftrightarrow S).$$

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

Tautologies. Consider the sentence $P \vee \neg P$. If P is true, then the sentence $P \vee \neg P$ is true. If P is false, then $\neg P$ is true, so again the sentence $P \vee \neg P$ is true. Thus whether P is true or false, the sentence $P \vee \neg P$ is true. We describe this situation by saying that the sentence $P \vee \neg P$ is a *tautology*.[6] 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 $\neg$, $\wedge$, $\vee$, $\Rightarrow$, and $\Leftrightarrow$, and not because of the truth values of these basic constituent sentences.

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

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 $(P \wedge Q) \Rightarrow P$ is a tautology.

Solution. We must show that $(P \wedge Q) \Rightarrow P$ 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 $P \wedge Q$ is true or $P \wedge Q$ is false.

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

Case 2. Suppose $P \wedge Q$ is false. Then by $(P \wedge Q) \Rightarrow P$ 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, $(P \wedge Q) \Rightarrow P$ is true. We have shown this under no assumptions on the truth values of P and Q. Hence $(P \wedge Q) \Rightarrow P$ is a tautology. ■

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

[6] By the way, the tautology $P \vee \neg P$ 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 $\Rightarrow$.[7] 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. ■

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 $P \Rightarrow (P \vee Q)$ 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 $Q \Rightarrow (P \vee Q)$ is a tautology.

Exercise 14. Show by means of an explanation in words that the sentence $(P \wedge Q) \Rightarrow (P \vee Q)$ 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 $P \vee Q$ 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 $P \wedge Q$ is true, we have just shown that P is true, so that $(P \wedge Q) \Rightarrow P$ is true, and because in the case where $P \wedge Q$ is false, $(P \wedge Q) \Rightarrow P$ is true by the definition of $\Rightarrow$, so that in either case, $(P \wedge Q) \Rightarrow P$ 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*.[10]

Conditional Proof (Continued).

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

$$\{(P \vee Q) \wedge [(P \Rightarrow R) \wedge (Q \Rightarrow R)]\} \Rightarrow R$$

is a tautology.[11] Be explicit about discharging assumptions.

Solution.

A1: Suppose $(P \vee Q) \wedge [(P \Rightarrow R) \wedge (Q \Rightarrow R)]$ is true.
Then both of $P \vee Q$ and $(P \Rightarrow R) \wedge (Q \Rightarrow R)$ are true.
Since $P \vee Q$ is true, at least one of P and Q is true.

Case 1. Suppose P is true.
Since $(P \Rightarrow R) \wedge (Q \Rightarrow R)$ 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 $(P \Rightarrow R) \wedge (Q \Rightarrow R)$ 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 $(P \vee Q) \wedge [(P \Rightarrow R) \wedge (Q \Rightarrow R)]$ is true.
Discharging A1, we see that $\{(P \vee Q) \wedge [(P \Rightarrow R) \wedge (Q \Rightarrow R)]\} \Rightarrow R$ 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

$$\{(P \vee Q) \wedge [(P \Rightarrow R) \wedge (Q \Rightarrow S)]\} \Rightarrow (R \vee S)$$

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 A1, A2, A3, 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

$$[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R) \tag{11}$$

is a tautology.[13] Be explicit about discharging assumptions.

Solution.

A1: Suppose $(P \Rightarrow Q) \wedge (Q \Rightarrow R)$ 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 A1 and A2 together.

Discharging A2, we see that $P \Rightarrow R$ is true under A1 alone.[16]

Finally, discharging A1, we see that $[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$ 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:

$$\underbrace{[(P \Rightarrow Q) \wedge (Q \Rightarrow R)]}_{A_1} \Rightarrow \underbrace{(P \Rightarrow R)}_{C_1}.$$

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

$$A_1 \Rightarrow C_1$$

where A_1 is $(P \Rightarrow Q) \wedge (Q \Rightarrow R)$ 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, $(P \Rightarrow Q) \wedge (Q \Rightarrow R)$, 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 A1, 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 A1, 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 A1, $P \Rightarrow R$ is true whether or not P is true. In other words, under A1, $P \Rightarrow R$ is true whether or not A2 holds.

[17] The case where $(P \Rightarrow Q) \wedge (Q \Rightarrow R)$ is true is the case where A1 holds. In this case, we have just shown that $P \Rightarrow R$ is true, so that $[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$ is true. In the case where $(P \Rightarrow Q) \wedge (Q \Rightarrow R)$ is false, $[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$ 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:

$$\underbrace{[(P \Rightarrow Q) \wedge (Q \Rightarrow R)]}_{A_1} \Rightarrow \underbrace{(\underbrace{P}_{A_2} \Rightarrow \underbrace{R}_{C_2})}_{C_1}.$$

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

$$(P \Rightarrow Q) \Rightarrow \{[P \Rightarrow (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)\} \tag{12}$$

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:

$$\underbrace{(P \Rightarrow Q)}_{A_1} \Rightarrow \underbrace{\{[P \Rightarrow (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)\}}_{C_1}.$$

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:

$$\underbrace{[P \Rightarrow (Q \Rightarrow R)]}_{A_2} \Rightarrow \underbrace{(P \Rightarrow R)}_{C_2}.$$

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:

$$\underbrace{(P \Rightarrow Q)}_{A_1} \Rightarrow \underbrace{[P \Rightarrow (Q \Rightarrow R)]}_{A_2} \Rightarrow \underbrace{(\underbrace{P}_{A_3} \Rightarrow \underbrace{R}_{C_3})}_{C_2}.$$

$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{C_1}$$

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

$$\begin{aligned}&\{\, A \Rightarrow [\, B \Rightarrow (C \Rightarrow D)\,]\,\}\\ &\qquad\Rightarrow \{\, [\, A \Rightarrow (B \Rightarrow C)\,]\\ &\qquad\qquad\Rightarrow [\, (A \Rightarrow B)\\ &\qquad\qquad\qquad\Rightarrow (A \Rightarrow D)\,]\,\}\end{aligned}$$

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:

$$\begin{aligned}&3x-15 = (1/2)(x^2-7x+10)\\ &6x-30 = x^2-7x+10\\ &0 = x^2-13x+40 = (x-5)(x-8)\\ &x = 5,\, 8\end{aligned}$$

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:

$$\begin{aligned}&x = \sqrt{x+2}\\ &x^2 = x+2\\ &x^2-x-2 = 0\\ &(x+1)(x-2) = 0\\ &x = -1,\, 2\end{aligned}$$

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 a 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 $[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$. 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 $Q \wedge \neg Q$. 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 $Q \wedge \neg Q$ is false. If Q is false, then $Q \wedge \neg Q$ is false. Thus in either case, $Q \wedge \neg Q$ is false.)

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, $\lightning$. The symbol $\lightning$ may be read "falsehood" and should be thought of as standing for a false sentence. (For instance, $\lightning$ might stand for a contradiction $Q \wedge \neg Q$.) As the following truth table shows, $P \Rightarrow \lightning$ has the same truth value as $\neg P$:

P	$\lightning$	$P \Rightarrow \lightning$	$\neg P$
T	F	F	F
F	F	T	T

(13)

Now if we assume P and deduce a contradiction $Q \wedge \neg Q$, then by the method of conditional proof, the conditional sentence $P \Rightarrow (Q \wedge \neg Q)$ 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

$$[(P \Rightarrow Q) \wedge \neg Q] \Rightarrow \neg P$$

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 $Q \wedge \neg Q$. This shows that $(\neg P) \Rightarrow (Q \wedge \neg Q)$ 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

$$\text{If } x^2 \text{ is an even number, then } x \text{ is an even number.} \tag{14}$$

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:

P	Q	$P \Rightarrow Q$	$\neg Q$	$\neg P$	$\neg Q \Rightarrow \neg P$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

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 *modus tollens*. Actually, the full name for this tautology is *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 $P \Rightarrow Q$ with $\neg Q \Rightarrow \neg P$ is the basis for the method of *proof by contraposition*: To prove $P \Rightarrow Q$, it suffices to prove $\neg Q \Rightarrow \neg P$.

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 $P \Rightarrow Q$. 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 $P \wedge \neg P$, so we conclude that $\neg Q$ cannot be true, so Q must be true, so we have proved $P \Rightarrow Q$. 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 $\neg Q \Rightarrow \neg P$ is true, so by contraposition, $P \Rightarrow Q$ is true.

Still More about Conditional Sentences (*Optional*).

It can be shown that the sentence $(P \wedge Q) \Rightarrow R$ is logically equivalent to the sentence $(P \Rightarrow R) \vee (Q \Rightarrow R)$, and the sentence $(P \vee Q) \Rightarrow R$ is logically equivalent to the sentence $(P \Rightarrow R) \wedge (Q \Rightarrow R)$. 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 $(P \wedge Q) \Rightarrow R$ is logically equivalent to the sentence $(P \Rightarrow R) \vee (Q \Rightarrow R)$.

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 $(P \wedge Q) \Rightarrow R$ has the same truth value as $\neg(P \wedge Q)$. Similarly, $(P \Rightarrow R) \vee (Q \Rightarrow R)$ has the same truth value as $\neg P \vee \neg Q$. But by one of De Morgan's laws, $\neg(P \wedge Q)$ has the same truth value as $\neg P \vee \neg Q$. Hence $(P \wedge Q) \Rightarrow R$ has the same truth value[20] as $(P \Rightarrow R) \vee (Q \Rightarrow R)$.

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

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

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

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

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

By the way, the fact that $(P \wedge Q) \Rightarrow R$ implies $P \Rightarrow (Q \Rightarrow R)$ is known as *the law of exportation*. The fact that $P \Rightarrow (Q \Rightarrow R)$ implies $(P \wedge Q) \Rightarrow R$ 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) $P \Rightarrow (Q \wedge R)$ is logically equivalent to $(P \Rightarrow Q) \wedge (P \Rightarrow R)$.

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

(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 $\wedge$, $\vee$, and $\Rightarrow$ respectively. Show that $\Rightarrow$ is not "right-distributive" over any of $\wedge$, $\vee$, 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 $\neg$, $\wedge$, $\vee$, $\Rightarrow$, 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 $P \wedge Q$ is a function of the truth values of P and Q. Given the truth values of P and Q, the truth table for $\wedge$ tells us how find the truth value of $P \wedge Q$. 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 $\wedge$, $\vee$, $\Rightarrow$, 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 $(P \wedge Q) \Rightarrow R$ and $(P \Rightarrow R) \vee (Q \Rightarrow R)$ 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.

it would be too wide to fit on the page in one piece:

P	Q	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \Leftarrow Q$	$P \Leftrightarrow Q$	$P \vee \neg P$
T	T	T	T	T	T	T	T
T	F	F	T	F	T	F	T
F	T	F	T	T	F	F	T
F	F	F	F	T	T	T	T

$\neg$P	$\neg$Q	$\neg$(P $\wedge$ Q)	$\neg$(P $\vee$ Q)	$\neg$(P $\Rightarrow$ Q)	$\neg$(P $\Leftarrow$ Q)	$\neg$(P $\Leftrightarrow$ Q)	P $\wedge \neg$P
F	F	F	F	F	F	F	F
F	T	T	F	T	F	T	F
T	F	T	F	F	T	T	F
T	T	T	T	F	F	F	F

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 $\wedge$, $\vee$, $\Rightarrow$, $\Leftarrow$, $\Leftrightarrow$, 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 $\neg$, $\wedge$, $\vee$, $\Rightarrow$, and $\Leftrightarrow$. Note that a given truth function may be expressible in more than one such way. For instance $\neg(P \wedge Q)$ is logically equivalent to $(\neg P) \vee (\neg Q)$, 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, $\neg$, $\wedge$, and $\vee$.

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

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 $P_1, \ldots, P_n$, $\neg$, $\wedge$, $\vee$, $\Rightarrow$ and $\Leftrightarrow$. For instance, suppose $f(P, Q, R)$ is a truth function of three propositional variables P, Q, and R. Then $f(P, Q, R)$ is logically equivalent to $[f(P, Q, \mathrm{T}) \wedge R] \vee [f(P, Q, \mathrm{F}) \wedge \neg R]$. (To see this, first consider the case where R is true and then consider the case where R is false.) Now $f(P, Q, \mathrm{T})$ and $f(P, Q, \mathrm{F})$ are truth functions of two propositional variables P and Q, so they can be expressed in terms of P, Q, $\neg$, $\wedge$, $\vee$, $\Rightarrow$ and $\Leftrightarrow$. Thus the basic logical connectives $\neg$, $\wedge$, $\vee$, $\Rightarrow$ and $\Leftrightarrow$ 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, $\Leftrightarrow$ is clearly not needed because it can be expressed in terms of $\Rightarrow$ and $\wedge$: $P \Leftrightarrow Q$ is logically equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. Next, $\vee$ and $\Rightarrow$ can both be expressed in terms of $\neg$ and $\wedge$: $P \vee Q$ is logically equivalent to $\neg(\neg P \wedge \neg Q)$ and, as you were asked to show in Exercise 31, $P \Rightarrow Q$ is logically equivalent to $(\neg P) \vee Q$. One can also show that $\wedge$ and $\Rightarrow$ can both be expressed in terms of $\neg$ and $\vee$, and that $\wedge$ and $\vee$ can be expressed in terms of $\neg$ and $\Rightarrow$. It follows that any truth function $f(P_1, \ldots, P_n)$ can be expressed in terms of $P_1, \ldots, P_n$, $\neg$, and any one of $\wedge$, $\vee$, or $\Rightarrow$.

Exercise 32. Explain how $P \wedge Q$ and $P \vee Q$ may be expressed in terms of P, Q, $\neg$, and $\Rightarrow$.

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 $\wedge$, $\vee$, and $\Rightarrow$. 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 $(P \mid Q) \equiv \neg(P \wedge Q)$. In view of what we have seen above, to show that any logical connective can be expresssed in terms of $|$, all we need do is verify that $\neg$ and $\wedge$ can be expressed in terms of $|$. This is easily done. Just observe that

$$\neg P \equiv \neg(P \wedge P) \equiv (P \mid P)$$

and

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

The fact that any logical connective can be expressed in terms of $\mid$ 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 $*$ be a binary logical connective that makes $(R \wedge S) * R$ a tautology.

(a) Show that $P * Q$ must be true whenever P is false.

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

Solution. (a) First, if R is T and S is F, then $R \wedge S$ is F, so $(R \wedge S) * R$ is $\mathrm{F} * \mathrm{T}$. But since $(R \wedge S) * R$ is a tautology, $(R \wedge S) * R$ is T. Thus $\mathrm{F} * \mathrm{T}$ is T. Next, if R is F and S is F, then again $R \wedge S$ is F, so $(R \wedge S) * R$ is $\mathrm{F} * \mathrm{F}$. As before, since $(R \wedge S) * R$ is a tautology, $(R \wedge S) * R$ is T. Thus $\mathrm{F} * \mathrm{F}$ is T. Therefore $P * Q$ must be true whenever P is false.

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

Exercise 33. Let $*$ be a binary logical connective that makes $R * (R \vee S)$ a tautology.

(a) Show that $P * Q$ must be true whenever P is false.

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

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

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

Exercise 34. Let $*$ be a binary logical connective that makes $(P * Q) \wedge (Q * P)$ logically equivalent to $P \Leftrightarrow Q$.

(a) Show that $*$ is $\Rightarrow$, or $*$ is $\Leftarrow$, or $*$ is $\Leftrightarrow$. In other words, show that the truth table for $*$ is the same as the truth table for $\Rightarrow$, or the truth table for $\Leftarrow$, or the truth table for $\Leftrightarrow$. (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 $\mathrm{T} * \mathrm{T}$. Then determine $\mathrm{F} * \mathrm{F}$. Then figure out as much as you can about $\mathrm{T} * \mathrm{F}$ and $\mathrm{F} * \mathrm{T}$.)

(b) Now suppose in addition that $*$ makes $(R \wedge S) * R$ a tautology. Show that then $*$ is $\Rightarrow$. In other words, show that the truth table for $*$ 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 connnectives, 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 $\wedge$ and $\vee$.

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 $\{1, 2, 3, \dots\}$ 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 $\{1, 2, 3, \dots, n\}$ stands for the collection whose

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 $\mathbf{N}$. The former collection stops at n whereas the latter goes on forever. Sometimes one writes $\mathbf{N} = \{1, 2, 3, \ldots, n, \ldots\}$ to emphasize this. By the way, ∞ is not considered to be an element of $\mathbf{N}$. 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 $\boldsymbol{\omega}$ to denote the collection $\{0, 1, 2, \ldots\}$ of whole numbers.[21] Note that ∞ is not considered to be an element of $\boldsymbol{\omega}$. 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 $\mathbf{Z}$. (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 $\mathbf{Q}$ to denote the set of rational numbers. (This is from the first letter of the word *quotient*.) The boldface letter $\mathbf{R}$ 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 ∞ are not considered to be elements of $\mathbf{Z}$, $\mathbf{Q}$, or $\mathbf{R}$. Finally, the boldface letter $\mathbf{C}$ 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 $P(\text{Jack}) \wedge P(\text{Jill})$ is true; in other word, 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 $P(\text{Jack}) \vee P(\text{Jill})$ 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 $\wedge$ and $\vee$ 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 $P(2) \wedge P(3) \wedge P(5)$, and $(\exists x)P(x)$ has the same truth value as $P(2) \vee P(3) \vee P(5)$. 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 $\mathbf{N} = \{1, 2, 3, \ldots\}$ of natural numbers, then $(\forall x)P(x)$ may be thought of as representing the infinitely long sentence

$$P(1) \wedge P(2) \wedge P(3) \wedge \cdots$$

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

$$P(1) \vee P(2) \vee P(3) \vee \cdots \quad .$$

[21] You should take care to write ω and w differently. The symbol w is our letter "double-yoo." The symbol ω is "omega," the last letter of the Greek alphabet. It is one of the two letters for "o" in Greek. Classical Greek used ω 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 $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$. Instead, you should indicate somehow that $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ 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 $\mathbf{R}$ 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 $(\forall x \in \mathbf{R})[(x+2)^2 = x^2 + 4x + 4]$ and it is also true that $(\exists x \in \mathbf{R})(x^2 + 5 = 9)$.

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.[23] Accordingly, we write $(\forall x \in A)P(x)$ as an abbreviation for $(\forall x)[(x \in A) \Rightarrow P(x)]$. Also, the sentence $(\exists x)[(x \in A) \wedge P(x)]$ is true exactly when the sentence $(x \in A) \wedge P(x)$ 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 $(\exists x)[(x \in A) \wedge P(x)]$.

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) $(\exists x \in \mathbf{R})(x + 2 = 5)$.

(b) $(\forall x \in \mathbf{R})(x + 2 = 5)$.

(c) $(\exists x < 0)(x + 2 = 5)$,

(d) $(\forall x \in \mathbf{R})(x^2 + 4x + 5 > 0)$.

(e) $(\exists x \in \mathbf{R})(x^2 + 4x + 2 = 0)$.

Solution. (a) The sentence $(\exists x \in \mathbf{R})(x + 2 = 5)$ 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 $(\exists x \in \mathbf{R})(x + 2 = 5)$ is true because 3 is an example of a value of x that belongs to $\mathbf{R}$ such that $x + 2 = 5$.)

(b) The sentence $(\forall x \in \mathbf{R})(x + 2 = 5)$ means "For each real number x, $x + 2$ is equal to 5." We claim that this sentence is false.[24] Suppose that $(\forall x \in \mathbf{R})(x + 2 = 5)$ is true. Then in particular, since 0 is a real number, $0 + 2 = 5$. But $0 + 2 \neq 5$. Thus $0 + 2 = 5$ and $0 + 2 \neq 5$. This is a contradiction. Hence $(\forall x \in \mathbf{R})(x + 2 = 5)$ 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 $(\forall x \in \mathbf{R})(x^2 + 4x + 5 > 0)$ 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 $x_0 \in \mathbf{R}$. 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 $\mathbf{R}$.[25] Hence $(\forall x \in \mathbf{R})(x^2 + 4x + 5 > 0)$ is true, as claimed.

(e) The sentence $(\exists x \in \mathbf{R})(x^2 + 4x + 2 = 0)$ 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 $x \in \mathbf{R}$, by completing

[23] 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.

[24] 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.

[25] To say that x_0 is an arbitrary element of $\mathbf{R}$ means that we are not assuming anything about x_0 except that it is an element of $\mathbf{R}$.

the square and factoring a difference of squares, we have

$$\begin{aligned} x^2 + 4x + 2 &= x^2 + 4x + 4 - 2 = (x+2)^2 - 2 = (x+2)^2 - (\sqrt{2})^2 \\ &= [(x+2) - \sqrt{2}][(x+2) + \sqrt{2}] \\ &= [x - (-2 + \sqrt{2})][x - (-2 - \sqrt{2})]. \end{aligned}$$

Thus, letting $a = -2 + \sqrt{2}$ and $b = -2 - \sqrt{2}$, we have $x^2 + 4x + 2 = (x - a)(x - b)$. Therefore the sentence $(\exists x \in \mathbf{R})(x^2 + 4x + 2 = 0)$ is true, because $a \in \mathbf{R}$ and $a^2 + 4a + 2 = (a - a)(a - b) = (0)(a - b) = 0$.[26] ■

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 $(\exists x \in \mathbf{R})(x + 2 = 5)$ by pointing out that 3 is an example of a value of x that belongs to $\mathbf{R}$, 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 $(\forall x \in \mathbf{R})(x + 2 = 5)$ by just pointing out that 0 is an example of a value of x that belongs to $\mathbf{R}$, 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) $(\exists x \in \mathbf{R})(2x + 7 = 3)$.
(b) $(\forall x \in \mathbf{R})(2x + 7 = 3)$.
(c) $(\exists x > 0)(2x + 7 = 3)$.
(d) $(\forall x > 0)(2x + 7 = 3)$.
(e) $(\exists x \in \mathbf{R})(x^2 - 4x + 3 > 0)$.
(f) $(\forall x \in \mathbf{R})(x^2 - 4x + 3 > 0)$.
(g) $(\exists x \geq 7)(x^2 - 4x + 3 > 0)$.
(h) $(\forall x \geq 7)(x^2 - 4x + 3 > 0)$.
(i) $(\forall x \in \mathbf{R})(x^2 - 2x + 2 > 0)$.
(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 $(\exists x \in \mathbf{R})(x^2 + 4x + 2 = 0)$ is true because $b \in \mathbf{R}$ 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 $\{\,\text{Jack, Jill}\,\}$ 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 $P(\text{Jack}) \wedge P(\text{Jill})$. But no x appears in the sentence $P(\text{Jack}) \wedge P(\text{Jill})$. *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 $P(\text{Jack}) \wedge P(\text{Jill})$. 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 $P(\text{Jack}) \vee P(\text{Jill})$. No x appears in the sentence $P(\text{Jack}) \vee P(\text{Jill})$. 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 $P(\text{Jack}) \vee P(\text{Jill})$.

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, $\int_0^3 2x\,dx = 9 = \int_0^3 2t\,dt$. In the expression $\int_a^b f(x)\,dx$, x is a dummy variable and a, b and f 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 $[\int_a^b f(x)\,dx]^x$, 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

$$\text{"}(\forall x)(x \text{ likes ice cream}) \text{ and } (x \text{ likes cake})\text{,"} \tag{1}$$

the scope of the quantifier $(\forall x)$ is "x likes ice cream." But in the sentence

$$\text{"}(\forall x)(x \text{ likes ice cream and } x \text{ likes cake})\text{,"} \tag{2}$$

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 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

"$(\forall y)(y$ likes ice cream) and (x 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

$$(\forall x)P(x) \Rightarrow C, \tag{3}$$

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

$$(\forall x)[P(x) \Rightarrow C], \tag{4}$$

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

$$(\exists x)P(x) \Rightarrow C, \tag{5}$$

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) $(\forall x \in \mathbf{N})(x$ is even or x is odd$)$.

(b) $(\forall x \in \mathbf{N})(x$ is even$)$ or $(\forall x \in \mathbf{N})(x$ 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) $(\forall x \in \mathbf{Z})(\forall y \in \mathbf{Z})[\text{if } x < y, \text{ then } (\exists a \in \mathbf{N})(x + a = y)]$.

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

Vacuously True Universal Sentences. A universal sentence of the form $(\forall x)[P(x) \Rightarrow Q(x)]$ is said to be *vacuously true* when it is true just because there are no values of x for which $P(x)$ is true. Note that in this case, for each value of x, the conditional sentence $P(x) \Rightarrow Q(x)$ is vacuously true, since $P(x)$ is false. Here is an example of a vacuously true universal sentence. If I never buy jewelry, then the universal sentence "I buy all my jewelry at Tiffany's" is vacuously true. For a mathematical example, if A is a set and $P(x)$ is a statement about x and we want to prove the sentence $(\forall x \in A)P(x)$, which you should remember is an abbreviation for the sentence $(\forall x)[(x \in A) \Rightarrow P(x)]$, then we should start by writing "Consider any x. Suppose $x \in A$." and then we should try to prove $P(x)$. If A is empty, then such x exists, but that does not matter, for then the sentence $(\forall x \in A)P(x)$ is vacuously true.

The Generalized De Morgan's Laws. Recall that De Morgan's laws tell us that $\neg(P_1 \wedge P_2)$ is logically equivalent to $(\neg P_1) \vee (\neg P_2)$ and that $\neg(Q_1 \vee Q_2)$ is logically equivalent to $(\neg Q_1) \wedge (\neg Q_2)$. 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

$$(\forall x \in \mathbf{R})(x^2 - 4x + 5 > 0).$$

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

$$(\exists x \in \mathbf{R})(x^2 - 4x + 5 \leq 0).$$

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

$$\begin{aligned} & \neg(\forall x \in \mathbf{R})(x^2 - 4x + 5 > 0) \\ \text{iff} \quad & (\exists x \in \mathbf{R})\neg(x^2 - 4x + 5 > 0) \\ \text{iff} \quad & (\exists x \in \mathbf{R})(x^2 - 4x + 5 \leq 0). \end{aligned}$$

(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

$$(\forall x \in \mathbf{R})(x^2 - 6x + 8 \geq 0).$$

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

$$(\exists x \in \mathbf{R})(x^2 - 6x + 8 < 0).$$

Be careful not to skip any steps.

(b) Is P true or false?

Exercise 7. Let P be the sentence

$$(\exists x \in \mathbf{R})(x \geq 0 \text{ and } \sqrt{x+2} < \sqrt{x} + \sqrt{2}).$$

(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

$$(\forall x \in \mathbf{R})(x < 0 \text{ or } \sqrt{x+2} \geq \sqrt{x} + \sqrt{2}).$$

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 $P\wedge(Q_1\vee Q_2)$ is logically equivalent to $(P\wedge Q_1)\vee(P\wedge Q_2)$ and that $P\vee(Q_1\wedge Q_2)$ is logically equivalent to $(P\vee Q_1)\wedge(P\vee Q_2)$. 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) $P\wedge(\exists x\in A)Q(x)$ *is logically equivalent to* $(\exists x\in A)[P\wedge Q(x)]$.

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

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 $P\wedge(\exists x\in A)Q(x)$ 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 $P\wedge Q(x_0)$ is true. Hence $(\exists x\in A)[P\wedge Q(x)]$ is true, because for instance, x_0 is such a value of x.

Conversely, suppose $(\exists x\in A)[P\wedge Q(x)]$ is true. Then we can pick a value of x in A, say x_0, such that $P\wedge Q(x_0)$ 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 $P\wedge(\exists x\in A)Q(x)$ is true.

(b) Suppose $P\vee(\forall x\in A)Q(x)$ 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 $P\vee Q(x_0)$ is true, because P is true. Now x_0 is an arbitrary element of A. Hence $(\forall x\in A)[P\vee Q(x)]$ 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 $P\vee Q(x_0)$ is true, because $Q(x_0)$ is true. Now x_0 is an arbitrary element of A. Hence $(\forall x\in A)[P\vee Q(x)]$ is true.

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

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

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

Case 2. Suppose P is false. Consider any $x_0\in A$. Then $P\vee Q(x_0)$ is true, because $(\forall x\in A)[P\vee Q(x)]$ 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 $P\vee(\forall x\in A)Q(x)$ is true.

Thus in either case, $P\vee(\forall x\in A)Q(x)$ 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 $A=\mathbf{N}$. Let $R(x)$ be the sentence $P(x)\vee(\forall x\in A)Q(x)$ and let S be the sentence $(\forall x\in A)[P(x)\vee Q(x)]$. 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 $P\wedge(Q_1\wedge Q_2)$ is logically equivalent to $(P\wedge Q_1)\wedge(P\wedge Q_2)$, and that $P\vee(Q_1\vee Q_2)$ is logically equivalent to $(P\vee Q_1)\vee(P\vee Q_2)$. 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) $P \wedge (\forall x \in A)Q(x)$ *is logically equivalent to* $(\forall x \in A)[P \wedge Q(x)]$.

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

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.

$P(x,y)$	$y=a$	$y=b$	$y=c$
$x=a$	F	T	T
$x=b$	T	F	T
$x=c$	T	T	F

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.

	$(\exists y)P(x,y)$
$x=a$	T
$x=b$	T
$x=c$	T

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.

	$y=a$	$y=b$	$y=c$
$(\forall x)P(x,y)$	F	F	F

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.[27] To see how to express the sentence "For some y, everybody likes y" in everyday language, we must 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.

$P(x,y)$	$y=a$	$y=b$	$y=c$
$x=a$	F	T	F
$x=b$	T	T	F
$x=c$	F	T	T

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

[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."

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) $(\forall y \in \mathbf{R})(\exists x \in \mathbf{R})(x \le y)$.
(b) $(\exists x \in \mathbf{R})(\forall y \in \mathbf{R})(x \le y)$.
(c) $(\exists x \in \mathbf{N})(\forall y \in \mathbf{N})(x \le y)$.

Solution. (a) The sentence $(\forall y \in \mathbf{R})(\exists x \in \mathbf{R})(x \le y)$ 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 $y_0 \in \mathbf{R}$. Then $y_0 \le y_0$. Hence $(\exists x \in \mathbf{R})(x \le y_0)$, because for instance, y_0 is such a value of x. Now y_0 is an arbitrary element of $\mathbf{R}$. Hence $(\forall y \in \mathbf{R})(\exists x \in \mathbf{R})(x \le y)$.

(b) The sentence $(\exists x \in \mathbf{R})(\forall y \in \mathbf{R})(x \le y)$ 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 $x_0 \in \mathbf{R}$ such $(\forall y \in \mathbf{R})(x_0 \le y)$. But then in particular, $x_0 \le x_0 - 1$. Thus we have reached a contradiction. Hence $(\exists x \in \mathbf{R})(\forall y \in \mathbf{R})(x \le y)$ must be false.

(c) The sentence $(\exists x \in \mathbf{N})(\forall y \in \mathbf{N})(x \le y)$ 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 $(\forall y \in \mathbf{N})(x \le y)$ is true. We claim that 1 is such a value of x. To see this, consider any $y_0 \in \mathbf{N}$. Then $1 \le y_0$. Now y_0 is an arbitrary element of $\mathbf{N}$. Hence $(\forall y \in \mathbf{N})(1 \le y)$. This proves the claim. Therefore $(\exists x \in \mathbf{N})(\forall y \in \mathbf{N})(x \le y)$, 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) $(\exists y \in \mathbf{R})(\forall x \in \mathbf{R})(x + y = x)$.
(b) $(\forall x \in \mathbf{R})(\exists y \in \mathbf{R})(x + y = x)$.
(c) $(\exists y \in \mathbf{R})(\forall x \in \mathbf{R})(x + y = 0)$.
(d) $(\forall x \in \mathbf{R})(\exists y \in \mathbf{R})(x + y = 0)$.
(e) $(\exists y \in \mathbf{R})(\forall x \in \mathbf{R})(xy = 1)$.
(f) $(\forall x \in \mathbf{R})(\exists y \in \mathbf{R})(xy = 1)$.

3.14 Example. The following sentence is ambiguous:

There exists x such that x is the mother of y for each y. (6)

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. (7)

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. (8)

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. (9)

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

$$\text{There exists } x \text{ such that for each } y,\ x \text{ is the mother of } y. \tag{10}$$

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 $b \in \mathbf{R}$ 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 $b \in \mathbf{R}$, there exists $x \in S$ such that $x > b$. Be careful not to skip any steps.

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

$$\begin{aligned} & S \text{ is not bounded above} \\ \text{iff } & \neg(\exists b \in \mathbf{R})(\forall x \in S)(x \leq b) \\ \text{iff } & (\forall b \in \mathbf{R})\neg(\forall x \in S)(x \leq b) \\ \text{iff } & (\forall b \in \mathbf{R})(\exists x \in S)\neg(x \leq b) \\ \text{iff } & (\forall b \in \mathbf{R})(\exists x \in S)(x > b). \end{aligned}$$

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 $\mathbf{R}$ to $\mathbf{R}$ and let $L \in \mathbf{R}$. To say that $f(x)$ *tends to* L *as* x *tends to* ∞ means that for each $\varepsilon > 0$, there exists $K \in \mathbf{R}$ 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 ∞ iff there exists $\varepsilon > 0$ such that for each $K \in \mathbf{R}$, 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 $\mathbf{R}$ to $\mathbf{R}$ and let $a \in \mathbf{R}$. To say that f *is continuous at* a means that for each $\varepsilon > 0$, there exists $\delta > 0$ such that for each $x \in \mathbf{R}$, 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 $x \in \mathbf{R}$ 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 $(\forall x \in A)P(x, y_0)$. 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:

$$(\exists x)P(x) \wedge (\forall x_1)(\forall x_2)[P(x_1) \wedge P(x_2) \Rightarrow x_1 = x_2]. \tag{11}$$

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, $(\forall x_1)(\forall x_2)[P(x_1) \wedge P(x_2) \Rightarrow x_1 = x_2]$, 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:

$$(\exists x_1)\big[P(x_1) \wedge (\forall x_2)\big(P(x_2) \Rightarrow x_1 = x_2\big)\big]. \tag{12}$$

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 $(\exists!y \in \mathbf{R})(3 + y = 1)$ 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 $(\forall x \in \mathbf{R})(\exists!y \in \mathbf{R})(x + y = 1)$ 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 $x_0 \in \mathbf{R}$. Then $(\exists!y \in \mathbf{R})(x_0 + y = 1)$ 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 $\mathbf{R}$. Therefore $(\forall x \in \mathbf{R})(\exists!y \in \mathbf{R})(x + y = 1)$ is true.

3.19 Example. The sentence $(\exists!x \in \mathbf{R})(x^2 = 4)$ 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 $(\exists!x \in \mathbf{R})(x^2 = -4)$ 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) $(\exists!x \in \mathbf{R})(2x + 7 = 3)$.
(b) $(\exists!x \in \mathbf{R})(x^2 - 4x + 3 < 0)$.
(c) $(\exists!x \in \mathbf{Z})(x^2 - 4x + 3 < 0)$.
(d) $(\exists!x \in \mathbf{R})(x^2 - 4x + 4 = 0)$.
(e) $(\exists!x \in \mathbf{R})(x^2 - 4x + 5 = 0)$.
(f) $(\forall x \in \mathbf{R})(\exists!y \in \mathbf{R})(x + y = 0)$.
(g) $(\forall x \in \mathbf{R})(\exists!y \in \mathbf{R})(xy = 1)$.
(h) $(\forall x \in \mathbf{R})[\text{if } x \neq 0, \text{ then } (\exists!y \in \mathbf{R})(xy = 1)]$.
(i) $(\forall x \in \mathbf{R})(\exists!y \in \mathbf{R})(xy = 0)$.
(j) $(\forall x \in \mathbf{R})[\text{if } x \neq 0, \text{ then } (\exists!y \in \mathbf{R})(xy = 0)]$.

Chapter 2

Mathematical Proofs

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.[1] 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.[2] Before Pythagoras, the word "mathematics" in ancient Greek simply meant "knowledge." The Pythagoreans brought the word "mathematics" closer to its modern sense.[3] 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 $\boxed{x \text{ is an even number}}$ 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

$x + y = (2k_1 + 1) + (2k_2 + 1) = 2(k_1 + k_2 + 1)$. Now $k_1 + k_2 + 1$ is an integer. Hence $x + y$ is even. Thus if x is odd and y is odd, then $x + y$ is even. ■

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 ℓ. 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 ℓ, 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 $P \vee Q$, $\neg P \Rightarrow Q$, 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 ℓ 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 $\neg(P \wedge Q)$, $P \Rightarrow \neg Q$, 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. ■

4.17 Example. The British philospher Bertrand Russell liked to use the following joke to illustrate the point that a false statement implies any conclusion. He would say "I shall prove to you that if $1 = 0$, then I am the pope. The pope and I are surely two. Suppose $1 = 0$. Adding 1 to both sides of this equation, we find that $2 = 1$, so the pope and I are one."

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

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

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 $1/y$ 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 $-n = -(-3) = 3$, 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, π is irrational and e (the base for the natural logarithm function) is irrational. The irrationality of π 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.[6] 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 not have proved anything about the number e, since it was unheard of until the seventeenth century, but they were familiar with π.

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 π 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] 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 "|" is a vertical stroke. It is not slanted, like "/". In other words, "|" 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 $d \nmid x$ as an abbreviation for "d does not divide x."

4.39 Remark. Let $d, x \in \mathbf{N}$. 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 $a, b, c \in \mathbf{Z}$. 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 $a, b, c \in \mathbf{Z}$. 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 $\boldsymbol{\omega}$ of whole numbers, the relation of divisibility is reflexive, antisymmetric, and transitive. In other words,

(a) For each $a \in \boldsymbol{\omega}$, a divides a. (*Reflexivity.*)
(b) For all $a, b \in \boldsymbol{\omega}$, if a divides b and b divides a, then $a = b$. (*Antisymmetry.*)
(c) For all $a, b, c \in \boldsymbol{\omega}$, 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 $x \in \mathbf{N}$ and $x \neq 1$ and for each $a \in \mathbf{N}$, for each $b \in \mathbf{N}$, 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 $x \notin \mathbf{N}$ or $x = 1$ or for some $a \in \mathbf{N}$, for some $b \in \mathbf{N}$, $x = ab$ 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 $n \in \mathbf{N}$, 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 $x = p_1 \cdots p_m$ 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 $y \in \mathbf{N}$ 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 $n \in \mathbf{N}$. 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 1850's 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 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 $d = d_1 d_2$. 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 $x_1 x_2 \cdots x_n$ 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 $d = d_1 d_2 \cdots d_n$. (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 $x_1 x_2 \cdots x_n$ 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 $d = \operatorname{sgn}(d) d_1 d_2 \cdots d_n$, where

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

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

4.51 Remark. The expression $\operatorname{sgn}(d)$ introduced in Remark 4.50 may be read "signum of d." "Signum" is Latin for "sign," so $\operatorname{sgn}(d)$ 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 $a^2 = cb^2$, so $a^2 = (cb)(b)$. 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 $b = b_1 b_2$. 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 $b = b_1 b_2 = (1)(1) = 1$. 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 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 $x^3 = c$, 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

$$x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 = 0,$$

where $n \in \mathbf{N}$ and $c_0, c_1, \ldots, c_{n-1} \in \mathbf{Z}$.

(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

$$c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 = 0,$$

where $n \in \mathbf{N}$ and $c_0, c_1, \ldots, c_{n-1}, c_n \in \mathbf{Z}$. 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 $x \in \mathbf{R}$.

(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 rather 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 $x \in \mathbf{N}$ with $x \neq 1$ and let $r \in \mathbf{N}$ 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 $P \Leftrightarrow Q$, 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 $d, k \in \mathbf{N}$, $x = kd$, $d \neq 1$, 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, $x \in \mathbf{N}$ and $x \neq 1$, so to verify that x is a prime number, according to the definition, it remains to show that for each $a \in \mathbf{N}$, for each $b \in \mathbf{N}$, if $x = ab$, then $a = 1$ or $b = 1$. Consider any $a \in \mathbf{N}$ and any $b \in \mathbf{N}$. Suppose $x = ab$. We wish to show that $a = 1$ or $b = 1$. Now since $a, r \in \mathbf{N}$, 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 $b, r \in \mathbf{N}$, $b \leq r$. 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 $a, b \in \mathbf{N}$ 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 $x, y \in \mathbf{Z}$, 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 $x, y \in \mathbf{Z}$, 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 $n \in \mathbf{N}$, 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 $3^{3^{15}} \approx 3.25 \times 10^{6,846,168}$ is a sum of three primes. Chen and Wang (1989) improved Vinogradov's $3^{3^{15}}$ to $e^{e^{11.503}} \approx 3.33 \times 10^{43,000}$. Oliveira e Silva (2008) verified that each even number between 4 and 12×10^{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 $x, m \in \mathbf{Z}$. 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 $a = a$. (*Reflexivity.*)
(b) For all a and b, if $a = b$, then $b = a$. (*Symmetry.*)
(c) For all a, b, and c, if $a = b$ and $b = c$, then $a = c$. (*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 $m \in \mathbf{Z}$. Show that the relation of congruence modulo m is reflexive, symmetric, and transitive. In other words, show that:

(a) For each $a \in \mathbf{Z}$, we have $a \equiv a \mod m$. (*Reflexivity.*)
(b) For all $a, b \in \mathbf{Z}$, if $a \equiv b \mod m$, then $b \equiv a \mod m$. (*Symmetry.*)
(c) For all $a, b, c \in \mathbf{Z}$, 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 $m, a_1, b_1, a_2, b_2 \in \mathbf{Z}$. 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 $a_1 a_2 \equiv b_1 b_2 \mod m$. (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 ℓ, we have $b_2 = a_2 + \ell m$.)

4.63 Remark. Let $m \in \mathbf{Z}$. 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 $a, b \in \mathbf{Z}$, 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 $u, v, w \in \mathbf{Z}$, $w \not\equiv 0 \mod m$, 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 $a, b \in \mathbf{Z}$ 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 $u, v, w \in \mathbf{Z}$ 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 $p \in \{2, 3, 4, \dots\}$ and congruence modulo p behaves like equality with respect to cancellation, then p is prime.

Exercise 27. Let $p \in \{2, 3, 4, \dots\}$. Suppose that for all $x, y \in \mathbf{Z}$, 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

$$\dots, -9, -6, -3, 0, 3, 6, 9, \dots$$

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

$$\dots, -8, -5, -2, 1, 4, 7, 10, \dots$$

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

$$\dots, -7, -4, -1, 2, 5, 8, 11, \dots$$

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 $k \in \mathbf{Z}$ and a unique remainder $r \in \{0, \dots, m - 1\}$, 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 ??. Notice that `ind` m divides an integer x iff the remainder that is left after we divide m into x is 0. Let x_1 and x_2 be integers. Let $k_1, k_2 \in \mathbf{Z}$ and let $r_1, r_2 \in \{0, \dots, m - 1\}$ 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 $x_2 - x_1 = m(k_2 - k_1) + (r_2 - r_1)$. Of course $k_2 - k_1$ is an integer. Since $0 \leq r_1 \leq r_2 < m - 1$, we have $0 \leq r_2 - r_1 \leq r_2 < m - 1$. But $r_2 - r_1$ is an integer, so $r_2 - r_1 \in \{0, \dots, m - 1\}$. 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 $43,657 \equiv 4+3+6+5+7 \mod 9$. Now $4+3+6+5+7 = 25$. 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:

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

In particular, 2, 6, 10, and 14 are not differences of squares.

4.72 Remark. In what follows, we shall use certain terms more specific than *difference of squares*, such as *difference of even squares*, *difference of odd 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 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 $P \Leftrightarrow Q$, prove each of the conditional sentences $P \Rightarrow Q$ and $Q \Rightarrow P$. In such a proof of $P \Leftrightarrow Q$, 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.
- *Conditional proof.* To prove a conditional sentence $P \Rightarrow Q$, 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 $P \Rightarrow Q$ 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 $P \vee Q$ 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 $P \wedge Q$, 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
$$(\forall x_1)(\forall x_2)(P(x_1) \wedge P(x_2) \Rightarrow x_1 = x_2).$$
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 $Q \wedge \neg Q$. 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. 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 $P \vee Q$ 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 $P \vee Q$ by contradiction, you should remember that $\neg(P \vee Q)$ is logically equivalent to $\neg P \wedge \neg Q$. 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 $P \vee Q$ 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 $P \wedge \neg P$. 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 $P \wedge Q$ 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 $P \vee Q$ 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 $P \vee Q$. 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 $P \vee \neg P$ 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 $\mathbf{N} = \{1, 2, 3, \dots\}$ 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

$$P(1) \text{ is true} \tag{1}$$

and that

$$\text{for each natural number } n\text{, if } P(n) \text{ is true, then } P(n+1) \text{ is true.} \tag{2}$$

Then we may conclude that for each natural number n, $P(n)$ is true.

The principle of mathematical induction may be explained as follows. For each natural number n, let us say that n is *good* if $P(n)$ is true and let us say that n is *bad* if $P(n)$ is false. It conceivable that some natural numbers are good and some are bad. Suppose that we have proved (1) and (2), as stated in the principle of mathematical induction. By (1), the natural number 1 is good. Notice that (2) means that

if 1 is good, then 2 is good;
if 2 is good, then 3 is good;
if 3 is good, then 4 is good;
and so on.

So since 1 is good, 2 must also be good. But then since 2 is good, 3 must also be good. Next, since 3 is good, 4 must also be good. Continuing in this manner, we see that 1 is good, 2 is good, 3 is good, 4 is good, and so on. In other words, $P(1)$ is true, $P(2)$ is true, $P(3)$ is true, $P(4)$ is true, and so on. In other words, for each $n \in \mathbf{N}$, $P(n)$ is true.

Of course, the explanation in the preceding paragraph is not a proof of the principle of mathematical induction. Rather, it is a discussion of it and to some extent a reformulation of it in different words. Notice that in it we made liberal use of the vague words "and so on." It can be said that the principle of mathematical induction is a precise formulation of what these words mean.

The principle of mathematical induction is sometimes explained by analogy with climbing a ladder. If you can get onto the first rung of the ladder and if you can climb from any rung to the next rung, then you can climb up to any desired rung of the ladder.

5.2 Example. For each natural number n, let us try to find the sum of the first n odd natural numbers. The first odd natural number is 1, the sum of the first two odd natural numbers is $1+3=4$, the sum of the first three odd natural numbers is $1+3+5=9$, the sum of the first four odd natural numbers is $1+3+5+7=16$, and so on. Notice that $1+3=2^2$, $1+3+5=3^2$, $1+3+5+7=4^2$, and so on. Notice also the trivial but not irrelevant fact that $1=1^2$. Could it be that for each natural number n, the sum of the first n odd natural numbers is n^2? As our first illustration of the method of proof by induction, we shall show that this is indeed the case.

Before embarking on this proof, we pause to discuss a point of notation. Notice that the first odd natural number is $1 = 2 \cdot 1 - 1$, the second odd natural number is $3 = 2 \cdot 2 - 1$, the third odd natural number is $5 = 2 \cdot 3 - 1$, and so on. Thus for each $n \in \mathbf{N}$, the n-th odd natural number is $2n-1$ and the sum of the first n odd natural numbers may be written as

$$1 + 3 + 5 + \cdots + (2n-1).$$

The notation $\cdots$ stands for the terms that are included in the sum but not written. By the way, when n is small, this notation can be misleading and must be interpreted with care. For instance, when $n=3$, then $2n-1=5$ and the notation $1+3+5+\cdots+(2n-1)$ really just means $1+3+5$. And when $n=2$, then $2n-1=3$ and the notation $1+3+5+\cdots+(2n-1)$ really means $1+3$. And finally, when $n=1$, then $2n-1=1$ and the notation $1+3+5+\cdots+(2n-1)$ really just means 1. You should always pay attention to such points when you use "$\cdots$" notation.

Now here is the proof. Let $P(n)$ be the sentence

$$1 + 3 + 5 + \cdots + (2n-1) = n^2.$$

BASE CASE: First observe that $P(1)$ is true. This is so because if $n=1$, then $1+3+5+\cdots+(2n-1)$ is really just 1, and n^2 is 1^2, which is equal to 1.

INDUCTIVE STEP: Now let $n \in \mathbf{N}$ such that $P(n)$ is true.[9] Then

$$\begin{aligned} &1 + 3 + 5 + \cdots + (2n-1) + [2(n+1) - 1] \\ &= n^2 + [2(n+1) - 1] \qquad \text{(by the inductive hypothesis)} \\ &= n^2 + 2n + 2 - 1 = n^2 + 2n + 1 = (n+1)^2. \end{aligned}$$

Thus $P(n+1)$ is true too.[10]

CONCLUSION: Therefore, by induction, for each $n \in \mathbf{N}$, $P(n)$ is true.[11] In other words, for each natural number n, $1 + 3 + 5 + \cdots + (2n-1) = n^2$. This completes the proof.

Now here are some remarks which are intended to help you to avoid some errors that students often make when they try to write proofs by induction.

5.3 Remark. In the preceding proof, you should notice that $P(n)$ is not the sum $1+3+5+\cdots+(2n-1)$. Instead, $P(n)$ is the whole sentence $1+3+5+\cdots+(2n-1) = n^2$, whereas the sum $1+3+5+\cdots+(2n-1)$ is just the subject of this sentence. By the way, in your handwritten work, if you are anxious to save writing, you could introduce $P(n)$ by writing

$$\text{Let } P(n) \text{ be } \text{“}1 + 3 + 5 + \cdots + (2n-1) = n^2\text{.”}$$

But you should not write

$$\text{Let } P(n) = 1 + 3 + 5 + \cdots + (2n-1) = n^2,$$

because this makes it look like you are letting $P(n)$ be the sum $1+3+5+\cdots+(2n-1)$ which is just the subject of the sentence. You should make it clear that $P(n)$ is the whole sentence “$1 + 3 + 5 + \cdots + (2n-1) = n^2$.”

Notice also that $P(n)$ is not the sentence “For each $n \in \mathbf{N}$, $1 + 3 + 5 + \cdots + (2n-1) = n^2$.” Instead $P(n)$ is just the sentence “$1 + 3 + 5 + \cdots + (2n-1) = n^2$” and what we want to prove is the sentence “For each $n \in \mathbf{N}$, $P(n)$.”

You also should not write “For each $n \in \mathbf{N}$, let $P(n)$ be the sentence $1+3+5+\cdots+(2n-1) = n^2$.” The reason is that $P(n)$ is not a different sentence for each different value of n. Instead, $P(n)$ is one sentence in which n occurs as a free variable.

5.4 Remark. Let us summarize the steps in a proof by induction and point out a common misconception about the logic in a proof by induction. You should always begin a proof by induction by saying what $P(n)$ is. Then you should check the *base case*. In other words, you should check that $P(1)$ is true. And then you should do the main part of the work, the *inductive step*, which is to show that if $n \in \mathbf{N}$ such that $P(n)$ is true, then $P(n+1)$ is also true. The common misconception that we wanted to point out consists in thinking that in the inductive step, one is showing that if $P(n)$ is true for all $n \in \mathbf{N}$, then $P(n+1)$ is true for all $n \in \mathbf{N}$. Really, this misconception consists in thinking that in the inductive step, one is showing that if $P(1)$, $P(2)$, $P(3)$, $P(4)$, and so on, are all true, then $P(2)$, $P(3)$, $P(4)$, and so on, are all true. When we put it this way, it should be clear to you that this is not at all what one is showing in the inductive step. Rather, one is showing that

if $P(1)$ is true, then $P(2)$ is true;
if $P(2)$ is true, then $P(3)$ is true;
if $P(3)$ is true, then $P(4)$ is true;
and so on.

[9] This is called *the inductive hypothesis*. It introduces *the inductive step* in the proof. During the inductive step, n is not an arbitrary natural number. Instead, n is a natural number for which $P(n)$ happens to be true, or in other words, n is what we earlier called a “good” natural number.

[10] This concludes the inductive step. At this point, it is implicit that the inductive hypothesis is discharged, so that n is now arbitrary, and that we infer that for each natural number n, $P(n) \Rightarrow P(n+1)$.

[11] By the base case, we know that $P(1)$ is true. By the inductive step, we know that for each $n \in \mathbf{N}$, if $P(n)$ is true, then so is $P(n+1)$. Therefore, by the principle of mathematical induction, we may conclude that for each $n \in \mathbf{N}$, $P(n)$ is true.

5.5 Remark. Let us mention two common errors students make when they begin the inductive step in a proof by induction. Where we wrote "Let n be a natural number such that $P(n)$ is true," you should not write instead "Let $P(n)$ be true for all natural numbers n," because to do this is to assume the very thing that is to be proved. Neither should you write "Let $P(n)$ be true for some natural number n," because to do that is just to assume that $P(n)$ is true for at least one value of n, and we already know this is so once we have checked, in the base case, that $P(1)$ is true.

5.6 Remark. For now, when you write a proof by induction, you should label the steps just as I have done in the examples. This will help you to avoid some common errors. For instance, it will help you to avoid the error of writing "Thus $P(n+1)$ is true too, so by induction, for each $n \in \mathbf{N}$, $P(n)$ is true." It would be wrong to write this because it would be like beginning a new paragraph in the middle of a sentence. You should finish the inductive step. Then write the conclusion. The conclusion is a new paragraph.

Exercise 1. Prove by induction that for each $n \in \mathbf{N}$,

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Exercise 2. Prove by induction that for each $n \in \mathbf{N}$,

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

Exercise 3.

(a) Prove by induction that for each $n \in \mathbf{N}$,

$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}.$$

(b) Explain why it follows from part (a) and Exercise 1 that for each $n \in \mathbf{N}$,

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2. \tag{3}$$

It is natural to wonder whether (3) is just true by accident. In the next part, you are asked to show that it is no accident.

(c) Work out a geometrical proof of (3) as follows. For $k = 1, \ldots, n$, let R_k be the square region in the xy-plane consisting of all points (x, y) satisfying

$$0 \le x < 1 + 2 + \cdots + k \qquad \text{and} \qquad 0 \le y < 1 + 2 + \cdots + k$$

and notice that

$$\text{area}(R_k) = (1 + 2 + \cdots + k)^2 = \left[\frac{k(k+1)}{2}\right]^2 = \frac{k^2(k+1)^2}{4}, \tag{4}$$

where the second step follows from Exercise 1. In particular,

$$\text{area}(R_n) = (1 + 2 + \cdots + n)^2 = \frac{n^2(n+1)^2}{4}.$$

Let $G_1 = R_1$ and for $k = 2, \ldots, n$, let G_k be the region[12] in the xy-plane consisting all all points (x, y) which lie in R_k but outside R_{k-1}. Obviously $\text{area}(G_1) = \text{area}(R_1) = 1^2 = 1 = 1^3$. Draw a picture to explain why for $k = 2, \ldots, n$, we have

$$\text{area}(G_k) = \text{area}(R_k) - \text{area}(R_{k-1}) \tag{5}$$

and use (5) and (4) to check that $\text{area}(G_k) = k^3$. Deduce that

$$1^3 + 2^3 + \cdots + n^3 = \text{area}(G_1) + \text{area}(G_2) + \cdots + \text{area}(G_n).$$

Draw a picture to explain why we have

$$\text{area}(G_1) + \text{area}(G_2) + \cdots + \text{area}(G_n) = \text{area}(R_n)$$

Finally, explain how to combine these results to get (3). Note that this gives a proof of (3) which does not depend on part (a), though it does depend on Exercise 1.

[12] Such a region is called a *gnomon*. See `https://en.wikipedia.org/wiki/Gnomon`.

5.7 Remark. The next exercise deals with the formula for the sum of a geometric progression. This is arguably the most important summation formula in mathematics. It arises in the theory of interest, in the study of power series, in probability theory, and in many other areas.

Exercise 4. Let x be a real number. Suppose that $x \neq 1$. Prove by induction that for each $n \in \mathbf{N}$,

$$1 + x + x^2 + \cdots + x^{n-1} = \frac{1 - x^n}{1 - x}.$$

5.8 Remark. The method of proof by induction gives us a way to prove formulas such as those in the previous four exercises if these formulas are given to us. However, it would be nicer if we had a way to find these formulas if they are not given to us. This is one of the things that we shall explore in the next section.

5.9 Remark. The method of proof by induction is not limited to the verification of expressions for particular sums, as the next example shows.

5.10 Example. Prove by induction that for each $n \in \mathbf{N}$, 3 divides $4^n - 1$.

Solution. Let $P(n)$ be the sentence

$$3 \text{ divides } 4^n - 1.$$

BASE CASE: Note that $P(1)$ is true, because $4^1 - 1 = 3$ and of course 3 divides 3.

INDUCTIVE STEP: Now let $n \in \mathbf{N}$ such that $P(n)$ is true. Notice that $4^{n+1} - 1 = (4)(4^n) - 1 = (3 + 1)(4^n) - 1 = (3)(4^n) + (1)(4^n) - 1 = (3)(4^n) + (4^n - 1)$. Now obviously 3 divides $(3)(4^n)$ and by the inductive hypothesis, 3 divides $4^n - 1$. Hence 3 divides $(3)(4^n) + (4^n - 1)$. In other words, 3 divides $4^{n+1} - 1$. Thus $P(n + 1)$ is true too.

CONCLUSION: Therefore, by induction, for each $n \in \mathbf{N}$, $P(n)$ is true. In other words, for each $n \in \mathbf{N}$, 3 divides $4^n - 1$. ■

Exercise 5. Prove by induction that for each $n \in \mathbf{N}$, 5 divides $7^n - 2^n$.

In Remark 4.12, we saw that for each $x \in \mathbf{Z}$, x is not both even and odd. In Remark 4.10, it was stated that for each $x \in \mathbf{Z}$, x is even or x is odd, but the proof was deferred because it required induction, which we had not then discussed. Now we can give this proof.

5.11 Example. Prove that for each $x \in \mathbf{Z}$, x is even or x is odd.

Solution. Let $P(x)$ be the sentence

$$x \text{ is even or } x \text{ is odd.}$$

We wish to show that for each $x \in \mathbf{Z}$, $P(x)$ is true. There will be two parts to our proof of this.

PART 1. First, we shall prove by induction that for each $x \in \boldsymbol{\omega}$, $P(x)$ is true.[13]

BASE CASE: Note that $P(0)$ is true because 0 is even.

INDUCTIVE STEP: Let $x \in \boldsymbol{\omega}$ such that $P(x)$ is true. We wish to show that $P(x+1)$ is true. Since $P(x)$ is true, x is even or x is odd. In the case where x is even, $x + 1$ is odd. In the case where x is odd, $x + 1$ is even. So in either case, $x + 1$ is even or $x + 1$ is odd. Thus $P(x + 1)$ is true too.

CONCLUSION (OF PART 1): Therefore, by induction, for each $x \in \boldsymbol{\omega}$, $P(x)$ is true.

PART 2. Consider any $x \in \mathbf{Z}$. Then $x \geq 0$ or $x \leq -1$. If $x \geq 0$, then $x \in \boldsymbol{\omega}$, so $P(x)$ is true by part 1. Suppose $x \leq -1$. Then $-x \in \boldsymbol{\omega}$, so $P(-x)$ is true. In other words, $-x$ is even or $-x$ is odd. Now $x = (-1)(-x)$. If $-x$ is even, then x is even, because any integer times an even integer yields an even integer. If $-x$ is odd, then x is odd, because -1 is odd and the product of two odd integers is odd. Thus x is even or x is odd. In other words, $P(x)$ is true. ■

A common way to prove that a statement $P(x)$ is true for all integers x is to prove by induction that $P(x)$ is true for each nonnegative integer x and then to prove that $P(x)$ is true for each negative integer x by using the fact that if x is a negative integer, then $-x$ is a positive integer, so that $P(-x)$ is true by the first part of the argument. The preceding example illustrates this technique. The next exercise will give you some practice with it.

[13] This is a minor variation on the induction proofs that we have seen before. Since we wish to prove by induction that $P(x)$ is true for all $x \in \boldsymbol{\omega}$, rather that for all $x \in \mathbf{N}$, we must start from 0 rather than from 1.

Exercise 6. Prove that for each $x \in \mathbf{Z}$, 6 divides $x^3 - x$.

Exercise 7. Let

$$A(n) = \frac{1}{2 \cdot 1} + \frac{1}{3 \cdot 2} + \cdots + \frac{1}{n(n-1)} \quad \text{and} \quad B(n) = \frac{3}{2} - \frac{1}{n}.$$

When $n = 6$, we have $A(6) = \frac{1}{2} + \frac{1}{6} + \frac{1}{12} + \frac{1}{20} + \frac{1}{30} = \frac{5}{6}$ and $B(6) = \frac{3}{2} - \frac{1}{6} = \frac{4}{3}$, so $A(6) \neq B(6)$.

(a) Find the mistake in the following argument which purports to prove that $A(n) = B(n)$ in general.

Let $P(n)$ be the sentence

$$A(n) = B(n).$$

BASE CASE: Then $P(1)$ is true because $A(1) = \frac{1}{2}$ and $B(1) = \frac{3}{2} - \frac{1}{1} = \frac{1}{2}$.

INDUCTIVE STEP: Let $n \in \mathbf{N}$ such that $P(n)$ is true. Then

$$\begin{aligned} A(n+1) &= \frac{1}{2 \cdot 1} + \frac{1}{3 \cdot 2} + \cdots + \frac{1}{n(n-1)} + \frac{1}{(n+1)n} \\ &= A(n) + \frac{1}{(n+1)n} = B(n) + \frac{1}{(n+1)n} \\ &= \frac{3}{2} - \frac{1}{n} + \frac{1}{(n+1)n} = \frac{3}{2} - \frac{n+1}{(n+1)n} + \frac{1}{(n+1)n} \\ &= \frac{3}{2} - \frac{n}{(n+1)n} = \frac{3}{2} - \frac{1}{n+1} = B(n+1). \end{aligned}$$

Thus $P(n+1)$ is true too.

CONCLUSION: Therefore, by induction, for each $n \in \mathbf{N}$, $P(n)$ is true.

(b) What should $B(n)$ be? (Hint: $\frac{1}{k(k-1)} = \frac{1}{k-1} - \frac{1}{k}$.)

Exercise 8. Find the mistake in the following argument. (Hint: In the inductive step, an implicit assumption is made which is valid for most values of n but not for all. What is this implicit assumption and for which values of n is it valid?) We claim that all horses have the same color. It suffices to show that for each $n \in \mathbf{N}$, for each set of n horses, all of the horses in the set have the same color. We shall prove this by induction on n. Let $P(n)$ be the sentence

For each set of n horses, all of the horses in the set have the same color.

BASE CASE: Clearly $P(1)$ is true, because all of the horses in a set containing only one horse have the same color.

INDUCTIVE STEP: Let $n \in \mathbf{N}$ such that $P(n)$ is true. Consider any set of $n+1$ horses. Removing one of the horses from the set, we obtain a set of n horses, all of which have the same color by the inductive hypothesis. Removing a different horse from the set of $n+1$ horses, we obtain another set of n horses and all of these horses have the same color by the inductive hypothesis. Thus all of the horses in the set of $n+1$ horses have the same color. Hence $P(n+1)$ is true too.

CONCLUSION: Therefore, by induction, for each $n \in \mathbf{N}$, $P(n)$ is true. ■

The manipulation of summation notation can be confusing. Often such confusion can be resolved by writing the sums in "$\cdots$" notation, such as writing $\sum_{k=m}^{n} a_k$ in the form $a_m + a_{m+1} + \cdots + a_n$. The next exercise gives some practice in this.

Exercise 9. Let m and n be integers with $m < n$ and let $c, a_m, b_m, a_{m+1}, b_{m+1}, \ldots, a_n, b_n$ be real numbers. Without using formal induction, but just by writing the sums out in long form, show that:

(a) $c \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c a_k$.

(b) $\left(\sum_{k=m}^{n} a_k\right) + \left(\sum_{k=m}^{n} b_k\right) = \sum_{k=m}^{n} (a_k + b_k)$.

(c) $\sum_{k=m}^{n} a_k = a_m + \sum_{k=m+1}^{n} a_k$ and $\sum_{k=m}^{n} a_k = \left(\sum_{k=m}^{n-1} a_k\right) + a_n$.

(d) $\sum_{k=m}^{n} a_k = \sum_{k=m+1}^{n+1} a_{k-1}$.

Pascal's Triangle.

In 1654, the French mathematician and philosopher Blaise Pascal wrote a treatise on the following infinite array of numbers:

$$\begin{array}{ccccccccccc} & & & & & & 1 & & & & \\ & & & & & 1 & & 1 & & & \\ & & & & 1 & & 2 & & 1 & & \\ & & & 1 & & 3 & & 3 & & 1 & \\ & & 1 & & 4 & & 6 & & 4 & & 1 \\ 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\ & & & & & & \vdots & & & & \end{array}$$

In his honor, this array is now known as *Pascal's triangle*. The pattern in Pascal's triangle is as follows. The outermost entries are all 1. Each inner entry is the sum of the two entries nearest to it in the previous row. For instance, $2 = 1 + 1$, $3 = 1 + 2$, $3 = 2 + 1$, $4 = 1 + 3$, $6 = 3 + 3$, $4 = 3 + 1$, and so on. Recall that $\boldsymbol{\omega} = \{0, 1, 2, \dots\}$. For all $n \in \boldsymbol{\omega}$ and all $k \in \{0, \dots, n\}$, let $\binom{n}{k}$ be the k-th number in the n-th row in Pascal's triangle. Note that the top row in Pascal's triangle is considered to be the 0-th row and in each row, the leftmost entry is considered to be the 0-th entry. Thus $\binom{2}{1} = 2$, for instance. The notation $\binom{n}{k}$ is read n *choose* k. (The reason for this is that $\binom{n}{k}$ turns out to be equal to the number of k-element subsets of an n-element set, a fact to which we shall return shortly.) In terms of the notation $\binom{n}{k}$, the pattern in Pascal's triangle may be expressed as follows:

$$\binom{0}{0} = 1 \tag{6}$$

and for each $n \in \mathbf{N}$,

$$\binom{n}{0} = \binom{n}{n} = 1, \tag{7}$$

and for each $n \in \mathbf{N}$, for each $k \in \{1, \dots, n\}$,

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}. \tag{8}$$

Equations (6) and (7) are called the *boundary conditions* for Pascal's triangle, since they prescribe the values of the entries on the boundary of Pascal's triangle. Equation (8) is called the *recurrence relation* for Pascal's triangle. It tells us the general rule for determining the inner entries in row $n + 1$ of Pascal's triangle in terms of the entries in row n. Thus the recurrence relation tells us that $\binom{2}{1} = \binom{1}{1} + \binom{1}{0} = 1 + 1 = 2$, $\binom{3}{1} = \binom{2}{1} + \binom{2}{0} = 2 + 1 = 3$, $\binom{3}{2} = \binom{2}{2} + \binom{2}{1} = 1 + 2 = 3$, $\binom{4}{1} = \binom{3}{1} + \binom{3}{0} = 3 + 1 = 4$, $\binom{4}{2} = \binom{3}{2} + \binom{3}{1} = 3 + 3 = 6$, $\binom{4}{3} = \binom{3}{3} + \binom{3}{2} = 1 + 3 = 4$, and so on.

5.12 Remark. Pascal did not invent the triangle that bears his name. His 1654 treatise on it was primarily a survey of the remarkable variety of facts that were then already known about the numbers in this array, not a work introducing new discoveries. Pascal's work on this topic was connected with his study of the so-called *problème des parties* or *division problem*, which was the problem of deciding how to fairly divide the prize money in a game of chance in case the series of plays is for some reason interrupted and cannot be completed.[14]

[14] For an account of Pascal's study of the division problem and related matters, see Oystein Ore's article "Pascal and the Invention of Probability Theory" in the *American Mathematical Monthly*, volume 67 (1960), pages 409–419.

5.13 Remark. It is almost obvious, and is easy to prove by induction, that the conditions (6), (7), and (8) determine the numbers $\binom{n}{k}$ uniquely.

5.14 Remark. As we mentioned, $\binom{n}{k}$ turns out to be the number of k-element subsets of an n-element set. Let us give an example to illustrate the reason behind this. Consider the two-element subsets of the four-element set $\{1,2,3,4\}$. The ones that do not have the number 4 as an element are precisely the two-element subsets of the three-element set $\{1,2,3\}$, namely

$$\{1,2\}, \quad \{1,3\}, \quad \text{and} \quad \{2,3\},$$

and the number of these is 3, which is the same as $\binom{3}{2}$. The ones that do have the number 4 as an element are

$$\{1,4\}, \quad \{2,4\}, \quad \text{and} \quad \{3,4\}$$

and these are in one-to-one correspondence with the sets

$$\{1\}, \quad \{2\}, \quad \text{and} \quad \{3\},$$

and these in turn are the one-element subsets of the set $\{1,2,3\}$, the number of which is also three, which is the same as $\binom{3}{1}$. Thus the number of two-element subsets of the four-element set $\{1,2,3,4\}$ is $\binom{3}{2}+\binom{3}{1}$ and, by (8), this is equal to $\binom{4}{2}$. More generally, we may consider the k-element subsets of the $(n+1)$-element set $\{1,\ldots,n,n+1\}$. The ones that do not have $n+1$ as an element are precisely the k-element subsets of $\{1,\ldots,n\}$. The ones that do have $n+1$ as an element are in one-to-one correspondence with the $(k-1)$-element subsets of $\{1,\ldots,n\}$. Thus if we know that there are $\binom{n}{k}$ of the former and $\binom{n}{k-1}$ of the latter, then it follows that the number of k-element subsets of $\{1,\ldots,n,n+1\}$ is $\binom{n}{k}+\binom{n}{k-1}$ and, by (8), this is equal to $\binom{n+1}{k}$. This idea is the key to a proof by induction that for each $n \in \boldsymbol{\omega}$, for each n-element set A, for each $k \in \{0,\ldots,n\}$, the number of k-element subsets A is $\binom{n}{k}$. See Section ?? for more about this. apc

5.15 Example. Let a and b be real numbers. Let us examine the expansion of $(a+b)^2$. We have

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b) = (a+b)a + (a+b)b \\ &= a^2 + ba \\ &\qquad + ab + b^2 \\ &= a^2 + 2ab + b^2.\end{aligned}$$

The coefficients of a^2, ab, and b^2 in the expansion of $(a+b)^2$ are 1, 2, and 1 respectively. Notice that these are precisely the numbers in row 2 of Pascal's triangle. (Remember that the top row is row 0, not row 1.) Now let us see if there is a similar connection between the expansion of $(a+b)^3$ and the numbers in row 3 of Pascal's triangle. We have

$$\begin{aligned}(a+b)^3 &= (a+b)^2(a+b) = (a+b)^2 a + (a+b)^2 b \\ &= (a^2+2ab+b^2)a + (a^2+2ab+b^2)b \\ &= a^3 + 2a^2b + \ ab^2 \\ &\qquad + \ a^2b + 2ab^2 + b^3 \\ &= a^3 + 3a^2b + 3ab^2 + b^3\end{aligned}$$

Notice that the coefficients of a^3, a^2b, ab^2, and b^3 are 1, 3, 3, and 1 respectively, and these are precisely the numbers $\binom{3}{0}$, $\binom{3}{1}$, $\binom{3}{2}$, and $\binom{3}{3}$ in row 3 of Pascal's triangle. In other words,

$$(a+b)^3 = \tbinom{3}{0}a^3b^0 + \tbinom{3}{1}a^2b^1 + \tbinom{3}{2}a^1b^2 + \tbinom{3}{3}a^0b^3.$$

We can write this more succinctly in summation notation:

$$(a+b)^3 = \textstyle\sum_{k=0}^{3} \binom{3}{k} a^{3-k}b^k.$$

Next let us examine the expansion of $(a+b)^4$ to see how the coefficients in it compare with the numbers in row 4 of Pascal's triangle. This time we shall write the calculation in a way that highlights its connection with the recurrence relation for Pascal's triangle. We have

$$\begin{aligned}
(a+b)^4 &= (a+b)^3(a+b) = (a+b)^3a + (a+b)^3b \\
&= \left[\tbinom{3}{0}a^3b^0 + \tbinom{3}{1}a^2b^1 + \tbinom{3}{2}a^1b^2 + \tbinom{3}{3}a^0b^3\right]a + \left[\tbinom{3}{0}a^3b^0 + \tbinom{3}{1}a^2b^1 + \tbinom{3}{2}a^1b^2 + \tbinom{3}{3}a^0b^3\right]b \\
&= \tbinom{3}{0}a^4b^0 + \tbinom{3}{1}a^3b^1 + \tbinom{3}{2}a^2b^2 + \tbinom{3}{3}a^1b^3 \\
&\qquad + \tbinom{3}{0}a^3b^1 + \tbinom{3}{1}a^2b^2 + \tbinom{3}{2}a^1b^3 + \tbinom{3}{3}a^0b^4 \\
&= \tbinom{3}{0}a^4b^0 + \left[\tbinom{3}{1} + \tbinom{3}{0}\right]a^3b^1 + \left[\tbinom{3}{2} + \tbinom{3}{1}\right]a^2b^2 + \left[\tbinom{3}{3} + \tbinom{3}{2}\right]a^1b^3 + \tbinom{3}{3}a^0b^4 \\
&= \tbinom{4}{0}a^4b^0 + \tbinom{4}{1}a^3b^1 + \tbinom{4}{2}a^2b^2 + \tbinom{4}{3}a^1b^3 + \tbinom{4}{4}a^0b^4,
\end{aligned}$$

because $\binom{3}{0} = 1 = \binom{4}{0}$, $\binom{3}{1} + \binom{3}{0} = \binom{4}{1}$, $\binom{3}{2} + \binom{3}{1} = \binom{4}{2}$, $\binom{3}{3} + \binom{3}{2} = \binom{4}{3}$, and $\binom{3}{3} = 1 = \binom{4}{4}$. Thus the coefficients of a^4, a^3b, a^2b^2, ab^3, and b^4 in the expansion of $(a+b)^4$ are the numbers $\binom{4}{0}$, $\binom{4}{1}$, $\binom{4}{2}$, $\binom{4}{3}$, and $\binom{4}{4}$ respectively from row 4 of Pascal's triangle. Explicitly,

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.$$

In summation notation, this is

$$(a+b)^4 = \textstyle\sum_{k=0}^{4} \binom{4}{k} a^{4-k}b^k.$$

Exercise 10. Let a and b be real numbers. Work out the expansion of $(a+b)^5$ in a way that highlights its connection with the numbers in row 5 of Pascal's triangle, like the way in which we worked out the expansion of $(a+b)^4$ in Example 5.15.

The next exercise is concerned with one of the most important facts about the numbers in Pascal's triangle. It is a generalization of what we saw in Example 5.15 and Exercise 10.

Exercise 11. (*The binomial theorem.*) Let a and b be real numbers. Prove by induction that for each $n \in \boldsymbol{\omega}$,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k.$$

(Hint: As a warm-up, study Example 5.15 and do Exercise 10. You can use Exercise 9 to help you see how to use summation notation in the inductive step. However, you can equally well do the inductive step without using summation notation, by using "..." notation instead. This involves more writing but may be clearer. It is good to understand both ways to write the solution.)

A Little History. The binomial theorem is thought to have been discovered by the Arab mathematician al-Karaji in Baghdad some time soon after the year 1007 and independently by Chia Hsien in China around 1100. The expansion of $(a+b)^3$ was given by the Indian mathematician Brahmagupta in his *Arithmetic* in 628. Brahmagupta's work is believed to have been brought to Baghdad in the eighth century and may have inspired al-Karaji's discovery of the general binomial theorem. The expansion $(a+b)^2 = a^2 + 2ab + b^2$ goes back to the ancient Greeks. For instance, Euclid (*ca.* 300 B.C.) gives it. A. W. F. Edwards has written an excellent historical account of Pascal's triangle.[15]

[15] A. W. F. Edwards, *Pascal's Arithmetical Triangle: The Story of a Mathematical Idea*, Charles Griffin & Company Limited, London, 1987, Johns Hopkins University Press, Baltimore and London, 2002.

Binomial Coefficients. Because the numbers $\binom{n}{k}$ in Pascal's triangle occur as the coefficients of $a^{n-k}b^k$ in the expansion of $(a+b)^n$ that is given in the binomial theorem, they are also known as *binomial coefficients*.

5.16 Remark. By convention, $x^0 = 1$ for each real number x. Even $0^0 = 1$. This is not a theorem, it is a definition. We adopt this definition because it is the most useful way to define x^0. This definition has the disadvantage that it makes 0^y a discontinuous function of y, because $0^y = 0$ for each $y > 0$ but $0^0 = 1$. But this definition has the advantage that it makes x^0 a continuous function of x and the related advantage that with it, a polynomial such as $c_0 + c_1x + \cdots + c_nx^n$ can be written in summation notation as $\sum_{k=0}^{n} c_kx^k$ and this will be valid even if $x = 0$, because the term c_0x^0 is just equal to c_0 even when $x = 0$. To mention another advantage of this convention, it makes the binomial theorem $(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$ valid even if $a = 0$ or $b = 0$. For notice that if $b = 0$, then for $k = 1, \ldots, n$, we have $b^k = 0$, so $\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k = \binom{n}{0}a^{n-0}b^0 = a^nb^0 = a^n0^0 = a^n \cdot 1 = a^n = (a+0)^n = (a+b)^n$. Similar remarks apply if $a = 0$.

Exercise 12. Let $n \in \boldsymbol{\omega}$. Show that the sum of the entries in row n of Pascal's triangle is 2^n. In other words, show that

$$\sum_{k=0}^{n}\binom{n}{k} = 2^n. \tag{9}$$

(Do not use induction. Instead apply the binomial theorem, Exercise 11, with a suitable choice of a and b.)

5.17 Remark. Let us mention an interesting interpretation of (9). As we've indicated, $\binom{n}{k}$ is the number of k-element subsets of an n-element set. Thus $\sum_{k=0}^{n}\binom{n}{k}$ is the total number of subsets of an n-element set. Thus (9) tells us that the number of subsets of an n-element set of 2^n. We can also see this without using (9), as follows. First, let us illustrate the idea of the proof with an example. Consider the subsets of the three-element set $\{1, 2, 3\}$. The ones that do not have the number 3 as an element are precisely the subsets of the two-element set $\{1, 2\}$, namely

$$\emptyset, \quad \{1\}, \quad \{2\}, \quad \text{and} \quad \{1, 2\}, \tag{10}$$

where $\emptyset$ denotes the empty set, which has no elements. The subsets of $\{1, 2, 3\}$ that do have 3 as an element are

$$\{3\}, \quad \{1, 3\}, \quad \{2, 3\}, \quad \text{and} \quad \{1, 2, 3\},$$

and these are in one-to-one correspondence with the subsets of $\{1, 2\}$, which we listed in (10). This shows that the set $\{1, 2, 3\}$ has twice as many subsets as the set $\{1, 2\}$. The same idea can be used to show that in general, the set $\{1, \ldots, n, n+1\}$ has twice as many subsets as the set $\{1, \ldots, n\}$. Since the empty set has one subset, namely itself, and since $1 = 2^0$, it follows by induction that for each $n \in \boldsymbol{\omega}$, the set $\{1, \ldots, n\}$ has 2^n subsets.[16] For more about this, see Section ??. apc

Exercise 13.

(a) Let $n \in \mathbf{N}$. Show that

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0. \tag{11}$$

(Do not use induction. Instead, apply the binomial theorem, Exercise 11, with a suitable choice of a and b.)

(b) If n were 0, would (11) still be true? If not, then where does the proof that you gave in part (a) break down when $n = 0$?

Exercise 14. Prove by induction that for each $n \in \mathbf{N}$,

$$\binom{n}{1} = n \quad \text{and} \quad \binom{n}{n-1} = n.$$

5.18 Example. Prove by induction that for each $n \in \boldsymbol{\omega}$, for each $k \in \{0, \ldots, n\}$,

$$\binom{n}{k} = \binom{n}{n-k}.$$

(This expresses the fact that each row of Pascal's triangle is symmetric about its center.)

[16] If $n = 0$, then $\{1, \ldots, n\}$ denotes the empty set. If $n = 1$, then $\{1, \ldots, n\}$ is just $\{1\}$.

Solution. Let $P(n)$ be the sentence

$$\text{for each } k \in \{0, \ldots, n\},\ \tbinom{n}{k} = \tbinom{n}{n-k}.$$

We wish to show that for each $n \in \boldsymbol{\omega}$, $P(n)$ is true.

BASE CASE: Obviously $\tbinom{0}{0} = \tbinom{0}{0-0}$, so for each $k \in \{0\}$, $\tbinom{0}{k} = \tbinom{0}{0-k}$. In other words, $P(0)$ is true.

INDUCTIVE STEP: Now let $n \in \boldsymbol{\omega}$ such that $P(n)$ is true. We wish to show that $P(n+1)$ is true too. Now $P(n+1)$ is the sentence

$$\text{for each } k \in \{0, \ldots, n+1\},\ \tbinom{n+1}{k} = \tbinom{n+1}{n+1-k}.$$

(Notice that k varies over a different set in the sentence $P(n)$ than in the sentence $P(n+1)$.) Consider any $k \in \{0, \ldots, n+1\}$. For this k, we wish to show that $\tbinom{n+1}{k} = \tbinom{n+1}{n+1-k}$. Now either $k = 0$ or $k \in \{1, \ldots, n\}$ or $k = n+1$.

Case 1. Suppose $k = 0$ or $k = n+1$. Recall that $\tbinom{n+1}{0} = 1$ and $\tbinom{n+1}{n+1} = 1$, by the boundary conditions for Pascal's triangle. Hence $\tbinom{n+1}{k} = 1$ and $\tbinom{n+1}{n+1-k} = 1$, so $\tbinom{n+1}{k} = \tbinom{n+1}{n+1-k}$.

Case 2. Suppose $k \in \{1, \ldots, n\}$. By the recurrence relation for Pascal's triangle, we have

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}, \tag{12}$$

because $k \in \{1, \ldots, n\}$. By the inductive hypothesis that $P(n)$ is true, we have

$$\binom{n}{k} = \binom{n}{n-k}, \tag{13}$$

because $k \in \{0, \ldots, n\}$. Since $k \in \{1, \ldots, n+1\}$, we have $k-1 \in \{0, \ldots, n\}$ too, so the inductive hypothesis that $P(n)$ is true also tells us that

$$\binom{n}{k-1} = \binom{n}{n-(k-1)} = \binom{n}{n+1-k}. \tag{14}$$

Combining the three equations (12), (13), and (14), we see that

$$\binom{n+1}{k} = \binom{n}{n-k} + \binom{n}{n+1-k}. \tag{15}$$

Finally, since $k \in \{1, \ldots, n\}$, we have $n+1-k \in \{1, \ldots, n\}$ too, so the recurrence relation for Pascal's triangle also tells us that

$$\binom{n+1}{n+1-k} = \binom{n}{n+1-k} + \binom{n}{n-k}. \tag{16}$$

Combining the two equations (15) and (16), we see that

$$\binom{n+1}{k} = \binom{n+1}{n+1-k}.$$

Combining Cases 1 and 2, we see that for each $k \in \{0, \ldots, n+1\}$, $\tbinom{n+1}{k} = \tbinom{n+1}{n+1-k}$. In other words, $P(n+1)$ is true too.

CONCLUSION: Therefore, by induction, for each $n \in \boldsymbol{\omega}$, $P(n)$ is true. ■

Remark. In the solution of Example 5.18, the method we used in the case where $k \in \{1, \ldots, n\}$ does not work when $k = 0$ or when $k = n+1$, so it was necessary to consider these as a separate case. Happily, it is a very easy case.

The next three exercises are concerned with a method of calculating the numbers in any row of Pascal's triangle without having first to calculate the numbers in the previous rows.

Exercise 15.

(a) Check the following assertions:

$$\binom{1}{1} = \binom{1}{0}\frac{1}{1}.$$

$$\binom{2}{1} = \binom{2}{0}\frac{2}{1} \quad \text{and} \quad \binom{2}{2} = \binom{2}{1}\frac{1}{2}.$$

$$\binom{3}{1} = \binom{3}{0}\frac{3}{1}, \quad \binom{3}{2} = \binom{3}{1}\frac{2}{2}, \quad \text{and} \quad \binom{3}{3} = \binom{3}{2}\frac{1}{3}.$$

$$\binom{4}{1} = \binom{4}{0}\frac{4}{1}, \quad \binom{4}{2} = \binom{4}{1}\frac{3}{2}, \quad \binom{4}{3} = \binom{4}{2}\frac{2}{3}, \quad \text{and} \quad \binom{4}{4} = \binom{4}{3}\frac{1}{4}.$$

(b) Part (a) suggests that for each $n \in \mathbf{N}$, we have

$$\binom{n}{1} = \binom{n}{0}\frac{n}{1}, \quad \binom{n}{2} = \binom{n}{1}\frac{n-1}{2}, \quad \dots \quad , \quad \binom{n}{n} = \binom{n}{n-1}\frac{1}{n}.$$

In other words, for each $n \in \mathbf{N}$, for each $k \in \{\,1, \dots, n\,\}$,

$$\binom{n}{k} = \binom{n}{k-1}\frac{n-k+1}{k}.$$

Prove by induction that this is indeed the case. (Such a proof by induction was given by Pascal in his 1654 treatise. Hint: In the inductive step, use the inductive hypothesis and the recurrence relation for Pascal's triangle to express both $\binom{n+1}{k}$ and $\binom{n+1}{k-1}$ in terms of $\binom{n}{k-1}$. This can be done provided $k \in \{\,2, \dots, n\,\}$. The cases where $k = 1$ or $k = n+1$ require a separate but simple argument.)

Exercise 16.

(a) As we know, $\binom{7}{0} = 1$. Use this and the result of Exercise 15(b) to calculate $\binom{7}{k}$ for $k = 1, 2, 3, \dots, 7$.

(b) Explain how the result of Example 5.18 can be used to cut the work in part (a) in half.

5.19 Remark. Recall that $0! = 1$, $1! = 1$, $2! = 2 \cdot 1$, $3! = 3 \cdot 2 \cdot 1$, $4! = 4 \cdot 3 \cdot 2 \cdot 1$, and so on. In general, $n! = n(n-1)(n-2)\cdots(3)(2)(1)$. The expression $n!$ is read "n factorial." Of course, the order in which the factors are multiplied does not matter, so we also have $n! = (1)(2)(3)\cdots(n-2)(n-1)n$.

You may be surprised that $0!$ is defined to be 1. One way to understand this is that a product of no factors should be 1, because if you multiply it by any number a, the result should just be a, since a times no other factors is a product with just one factor, namely a. Another example of this is that by definition, $a^0 = 1$. Similarly, a sum of no terms is 0 by definition, because if you add it to any number a, the result should just be a, since a plus no other terms is a sum with just one term, namely a.

Perhaps we should comment further on the equality $n! = n(n-1)(n-2)\cdots(3)(2)(1)$. If $n = 0$, the expression $n(n-1)(n-2)\cdots(3)(2)(1)$ is considered to be a product of no factors, so it has the value 1, as it should to be equal to $0!$. Similarly, the equality $n! = (1)(2)(3)\cdots(n-2)(n-1)n$ holds even if $n = 0$, because if $n = 0$, the expression $(1)(2)(3)\cdots(n-2)(n-1)n$ does not actually include a factor of n but is instead considered to be a product of no factors, so it has the value 1, as it should to be equal to $0!$. All this is consistent with other pecularities of "dot dot dot" notation. For instance, if $n = 2$, then $1+2+3+\cdots+n$ is considered to be just $1+2$.

In terms of product notation, $n! = \prod_{j=1}^{n} j$. Since the order in which the factors are multiplied does not matter, we also have $n! = \prod_{j=1}^{n}(n-j+1)$. These expressions remain valid even if $n = 0$, provided that when $n = 0$, we consider a product of the form $\prod_{j=1}^{n} a_j$ to be a product of no factors.

Exercise 17.

(a) Let $n \in \boldsymbol{\omega}$. Prove by induction that for each $k \in \boldsymbol{\omega}$, if $k \leq n$, then

$$\binom{n}{k} = \left(\frac{n}{1}\right)\left(\frac{n-1}{2}\right)\left(\frac{n-2}{3}\right)\cdots\left(\frac{n-k+1}{k}\right). \tag{17}$$

If you prefer, you may save some writing by expressing (17) in terms of product notation, as follows

$$\binom{n}{k} = \prod_{j=1}^{k} \frac{n-j+1}{j}. \tag{18}$$

(Hint: We know that $\binom{n}{0} = 1$. By convention, if $k = 0$, then the product on the right side of (17), or equivalently the product on the right side of (18), is a product of no factors, so it has the value 1. You should use this for the base case. For the inductive step, use Exercise 15(b). You may also find Exercise 16(a) to be helpful as a concrete example.)

(b) Let $n \in \boldsymbol{\omega}$ and let $k \in \{0, \ldots, n\}$. Explain why it follows from part (a) that

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}.$$

(Hint:

$$\begin{aligned} n! &= n(n-1)(n-2)\cdots(n-k+1)(n-k)(n-k-1)\cdots(3)(2)(1) \\ &= n(n-1)(n-2)\cdots(n-k+1)(n-k)!. \end{aligned}$$

Hence $\dfrac{n!}{(n-k)!} = n(n-1)(n-2)\cdots(n-k+1)$.)

5.20 Remark. Later we shall learn another way to see the result of Exercise 17(b), connected with the fact that $\binom{n}{k}$ is the number of k-element subsets of an n-element set.

Extended Binomial Coefficients (*Optional*). The formula (17) can be used to define $\binom{n}{k}$ even when n is not a whole number. In this way, we can extend the definition of $\binom{n}{k}$ to all real numbers n and all whole numbers k. Notice that in the special case where n is a whole number and k is a whole number with $k > n$, the extended definition of $\binom{n}{k}$ yields the value 0 because it includes a factor of $\frac{n-n}{n+1}$. By the way, (17) can be rewritten in the following form which may be easier to remember:

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-(k-1))}{k(k-1)(k-2)\cdots(k-(k-1))}.$$

The Binomial Series (*Optional*). Let n be a whole number for the moment. If we take $a = 1$ and $b = x$ in the binomial theorem, then we get

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k. \tag{19}$$

Now by the extended definition of the binomial coefficients, we have $\binom{n}{k} = 0$ for each whole number $k > n$, so we may as well rewrite (19) as

$$(1+x)^n = \sum_{k=0}^{\infty} \binom{n}{k} x^k. \tag{20}$$

Now it is an interesting fact that if n is any real number, not necessarily a whole number, then at least for all real numbers x satisfying $|x| < 1$, the equation (20) remains true, where now the right hand side in (20) is an infinite series which is known as *the binomial series*. This fact is proved in most calculus textbooks. So for example, for $|x| < 1$, we have

$$\sqrt{1+x} = (1+x)^{1/2} = 1 + \frac{1}{2}x + \frac{\frac{1}{2}\left(\frac{1}{2}-1\right)}{2!}x^2 + \frac{\frac{1}{2}\left(\frac{1}{2}-1\right)\left(\frac{1}{2}-2\right)}{3!}x^3 + \cdots.$$

Be sure not to overlook the "$\cdots$" at the end of this equation. It indicates that the terms on the right hand side go on forever.

Induction and Arithmetic (*Optional*).

One of the most fundamental uses of induction is to establish the rules of arithmetic on the basis of assumptions that are as simple as possible. As an illustration of this, we include the following result.

5.21 The Division Lemma. *Let $d \in \mathbf{N}$. Then for each $x \in \mathbf{Z}$, there exist unique numbers $q \in \mathbf{Z}$ and $r \in \{0, \ldots, d-1\}$ such that $x = qd + r$.*

5.22 Remark. The reason why we have used the letters q and r in the statement of the division lemma is that q stands for the quotient that we obtain if we divide d into x and r stands for the remainder. The number q can also be described as the largest integer q such that $qd \leq x$. Then $qd \leq x < (q+1)d$ and $r = x - qd$.

Proof of the Division Lemma. We shall do this in three parts. In part 1, we shall prove existence of q and r when $x \in \boldsymbol{\omega}$. In part 2, we shall prove existence of q and r when $x \in \mathbf{Z}$. And in part 3, we shall prove uniqueness of q and r.

PART 1. Let $P(x)$ be the sentence

$$\text{There exist numbers } q \in \mathbf{Z} \text{ and } r \in \{0, \ldots, d-1\} \text{ such that } x = qd + r.$$

We shall prove by induction that for each $x \in \boldsymbol{\omega}$, $P(x)$ is true.

BASE CASE: Note that $P(0)$ is true, because $0 = 0d + 0$.

INDUCTIVE STEP: Let $x \in \boldsymbol{\omega}$ such that $P(x)$ is true. Then we can pick $q_0 \in \mathbf{Z}$ and $r_0 \in \{0, \ldots, d-1\}$ such that $x = q_0 d + r_0$. Then $x + 1 = q_0 d + r_0 + 1$. Now either $r_0 + 1 \in \{0, \ldots, d-1\}$ or $r_0 + 1 = d$.

Case 1. Suppose $r_0 + 1 \in \{0, \ldots, d-1\}$. Let $q = q_0$ and let $r = r_0 + 1$. Then $q \in \mathbf{Z}$, $r \in \{0, \ldots, d-1\}$, and $x + 1 = qd + r$.

Case 2. Suppose $r_0 + 1 = d$. Then $x + 1 = q_0 d + r_0 + 1 = q_0 d + d = (q_0 + 1)d$. Let $q = q_0 + 1$ and let $r = 0$. Then $q \in \mathbf{Z}$, $r \in \{0, \ldots, d-1\}$, and $x + 1 = qd + r$.

Thus in either case, $P(x+1)$ is true too.

CONCLUSION: Therefore, by induction, for each $x \in \boldsymbol{\omega}$, $P(x)$ is true. This completes part 1.

PART 2. Consider any $x \in \mathbf{Z}$. Then either $x \geq 0$ or $x \leq -1$.

Case 1. Suppose $x \geq 0$. Then $x \in \boldsymbol{\omega}$, so $P(x)$ is true by part 1.

Case 2. Suppose $x \leq -1$. Then $-x \in \mathbf{N}$, so $-x \in \boldsymbol{\omega}$, so $P(-x)$ is true by part 1, so we can pick numbers $q_0 \in \mathbf{Z}$ and $r_0 \in \{0, \ldots, d-1\}$ such that $-x = q_0 d + r_0$. Then $x = -q_0 d - r_0$. Now either $r_0 = 0$ or $r_0 \in \{1, \ldots, d-1\}$.

Subcase (a). Suppose $r_0 = 0$. Then $-r_0 = 0$, so $-r_0 \in \{0, \ldots, d-1\}$. Let $q = -q_0$ and let $r = -r_0$. Then $q \in \mathbf{Z}$, $r \in \{0, \ldots, d-1\}$, and $x = qd + r$.

Subcase (b). Suppose $r_0 \in \{1, \ldots, d-1\}$. Note that $x = -q_0 d - r_0 = -q_0 d - d + d - r_0 = (-q_0 - 1)d + (d - r_0)$. Now since $r_0 \in \{1, \ldots, d-1\}$, we have $d - r_0 \in \{1, \ldots, d-1\}$. Let $q = -q_0 - 1$ and let $r = d - r_0$. Then $q \in \mathbf{Z}$, $r \in \{0, \ldots, d-1\}$, and $x = qd + r$.

Thus in either subcase, $P(x)$ is true.

Thus in either case, $P(x)$ is true. This completes part 2.

PART 3. Now let us prove uniqueness of q and r. Consider any $x \in \mathbf{Z}$. Suppose $q_1, q_2 \in \mathbf{Z}$, $r_1, r_2 \in \{0, \ldots, d-1\}$, $x = q_1 d + r_1$, and $x = q_2 d + r_2$. We wish to show that $q_1 = q_2$ and $r_1 = r_2$. Now $r_1 \leq r_2$ or $r_2 \leq r_1$. The two cases are similar, so let us just consider the case where $r_1 \leq r_2$. Then $0 \leq r_2 - r_1 \leq r_2 \leq d - 1$. Now $0 = x - x = (q_1 d + r_2) - (q_2 d + r_2) = (q_2 - q_1)d + (r_2 - r_1)$, so $(q_1 - q_2)d = r_2 - r_1$. Since $d > 0$ and $r_2 - r_1 \geq 0$, we have $q_1 - q_2 \geq 0$. If $q_1 - q_2 \geq 1$, then $(q_1 - q_2)d \geq d$, so $r_2 - r_1 \geq d$, which is not the case, because $r_2 - r_1 \leq d - 1$. Thus it is not the case that $q_1 - q_2 \geq 1$, so $q_1 - q_2 < 1$. Since $q_1 - q_2 \in \mathbf{Z}$ and $0 \leq q_1 - q_2 < 1$, we have $q_1 - q_2 = 0$, so $q_1 = q_2$. Since $(q_1 - q_2)d = r_2 - r_1$ and $q_1 - q_2 = 0$, we have $r_2 - r_1 = 0$, so $r_1 = r_2$. The shows that q and r are unique, which completes part 3. ■

Further Exercises on Induction (*Optional*).

Exercise 18. Prove by induction that for each $n \in \mathbf{N}$,

$$\frac{d}{dx}x^n = nx^{n-1}.$$

(To treat the case where $n = 1$, you should use the definition of the derivative. In the inductive step, you should use the product rule for differentiation. These topics are covered in any calculus book.)

Exercise 19. Prove by induction that for each $n \in \boldsymbol{\omega}$,

$$\int_0^\infty x^n e^{-x}\,dx = n!.$$

5.23 Remark. Let us recall that if $n \in \boldsymbol{\omega}$, then a *polynomial of degree* n is an expression of the form

$$f(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n$$

where $a_0, a_1, \ldots, a_n$ are constants and $a_n \neq 0$. Let us also recall the formulas for the derivatives of the tangent and secant functions:

$$\frac{d}{dx}\tan x = \sec^2 x \qquad \text{and} \qquad \frac{d}{dx}\sec x = \sec x \tan x.$$

These reminders may help you with the next two exercises.

Exercise 20. Prove by induction that for each $n \in \mathbf{N}$, there is a polynomial f_n of degree $n+1$ such that the n-th derivative of $\tan x$ is given by

$$\frac{d^n}{dx^n}\tan x = f_n(\tan x).$$

Exercise 21. Prove by induction that for each $n \in \mathbf{N}$, there is a polynomial g_n of degree n such that the n-th derivative of $\sec x$ is given by

$$\frac{d^n}{dx^n}\sec x = g_n(\tan x)\sec x.$$

5.24 Remark. The next exercise is the product rule for n-th derivatives and is commonly known as *Leibnitz's formula*. You might like to do it if you want some more practice working with binomial coefficients similar to the binomial theorem, Exercise 11.

Exercise 22. Prove by induction that for each natural number n, for all n times differentiable functions f and g on $\mathbf{R}$,

$$(fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(n-k)} g^{(k)}.$$

(The symbols $(fg)^{(n)}$, $f^{(n-k)}$, and $g^{(k)}$ denote the n-th, $(n-k)$-th, and k-th derivatives of fg, f, and g respectively.)

Exercise 23. In 1202, the Italian mathematician Leonardo Fibonacci introduced the sequence of numbers $F_1, F_2, F_3, \ldots$ defined by $F_1 = 1$, $F_2 = 1$, and for all $n \in \{3, 4, 5, \ldots\}$, $F_n = F_{n-2} + F_{n-1}$. Thus each Fibonacci number after the first two is the sum of the two preceding ones: $F_1 = 1$, $F_2 = 1$, $F_3 = 1+1 = 2$, $F_4 = 1+2 = 3$, $F_5 = 2+3 = 5$, $F_6 = 3+5 = 8$, $F_7 = 5+8 = 13$, $F_8 = 8+13 = 21$, $F_9 = 13+21 = 44$, and so on. It appears that every third Fibonacci number is even and the others are odd. In other words, it appears that

$$\begin{aligned} &F_1 \text{ is odd and } F_2 \text{ is odd and } F_3 \text{ is even} \\ &\text{and } F_4 \text{ is odd and } F_5 \text{ is odd and } F_6 \text{ is even} \\ &\text{and } F_7 \text{ is odd and } F_8 \text{ is odd and } F_9 \text{ is even} \\ &\text{and so on.} \end{aligned}$$

Prove that this is indeed the case. (Hint: First formulate the result to proved in the form "for each $k \in \mathbf{N}$, $P(k)$ is true" where $P(k)$ is a statement about k. Then proceed by induction on k.)

Section 6. Insight versus Induction

Sometimes a proof by induction just verifies a pattern that is not too difficult to guess if you have experience. It would probably be fair to say that this was the case for the applications of proof by induction related to Pascal's triangle in Section 5, for instance. But although we may be able to use proof by induction to verify a formula that we are given, such as

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6},$$

how would we guess this formula if nobody was nice enough to give it to us? In this section, we shall revisit some of the results from Section 5 to learn how to discover them instead of just how to verify them by induction.

Sums of Powers Revisited.

Let us look again at the formulas for sums of powers of natural numbers. Let us write $S_r(n)$ for $1^r + 2^r + 3^r + \cdots + n^r$. Thus

$$\begin{aligned} S_1(n) &= 1 + 2 + 3 + \cdots + n, \\ S_2(n) &= 1^2 + 2^2 + 3^2 + \cdots + n^2, \\ S_3(n) &= 1^3 + 2^3 + 3^3 + \cdots + n^3, \end{aligned}$$

and so on.

6.1 Example. Here is one way to find the formula for

$$S_1(n) = 1 + 2 + 3 + \cdots + n.$$

Since the order in which we add numbers does not affect the result, we may reverse the order of the terms in this sum, getting

$$S_1(n) = n + (n-1) + (n-2) + \cdots + 1.$$

Now we can add these two expressions for $S_1(n)$, getting

$$S_1(n) + S_1(n) = [1+n] + [2+(n-1)] + [3+(n-2)] + \cdots + [n+1].$$

In this expression for $S_1(n) + S_1(n)$, each term adds up to $n+1$ and there are n terms in all. Hence $S_1(n) + S_1(n) = n(n+1)$. In other words, $2S_1(n) = n(n+1)$. Hence $S_1(n) = n(n+1)/2$. In other words,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

6.2 Remark. If we try to apply the trick in Example 6.1 to find the formula for

$$S_2(n) = 1^2 + 2^2 + 3^2 + \cdots + n^2,$$

we find that it does not work. Here is why. Writing the terms in reverse order, we get

$$S_2(n) = n^2 + (n-1)^2 + (n-2)^2 + \cdots + 1^2.$$

Now adding the two expressions for $S_2(n)$, we get

$$S_2(n) + S_2(n) = [1^2 + n^2] + [2^2 + (n-1)^2] + [3^2 + (n-2)^2] + \cdots + [n^2 + 1^2].$$

In this expression for $S_2(n) + S_2(n)$, the different terms on the right do not all add up to the same thing. For instance, when $n = 3$, we have

$$S_2(3) + S_2(3) = (1^2 + 3^2) + (2^2 + 2^2) + (3^2 + 1^2) = 10 + 8 + 10.$$

Hence this way to find the formula for $S_1(n)$ does not help us to find the formula for $S_2(n)$.

6.3 Example. There is a way to find the formula for $S_1(n)$ that will help us to find the formula for $S_2(n)$. It will also make it possible for us to find the formulas for $S_3(n)$, $S_4(n)$, and so on. Here is how it goes. Let

$$T(n) = \sum_{k=1}^{n} [k^2 - (k-1)^2].$$

On the one hand,

$$T(n) = [1^2 - 0^2] + [2^2 - 1^2] + [3^2 - 2^2] + \cdots + [(n-1)^2 - (n-2)^2] + [n^2 - (n-1)^2] = n^2$$

because in the sum, the first part of each term except the last cancels the second part of the next term.[17] On the other hand, since $k^2 - (k-1)^2 = k^2 - (k^2 - 2k + 1) = 2k - 1$,

$$T(n) = \sum_{k=1}^{n} (2k-1).$$

In other words,

$$T(n) = (2 \cdot 1 - 1) + (2 \cdot 2 - 1) + (2 \cdot 3 - 1) + \cdots + (2 \cdot n - 1).$$

Regrouping the terms on the right, we get

$$T(n) = (2 \cdot 1 + 2 \cdot 2 + 2 \cdot 3 + \cdots + 2 \cdot n) - (\underbrace{1 + 1 + 1 + \cdots + 1}_{n \text{ times}}).$$

In other words,

$$T(n) = (2 \cdot 1 + 2 \cdot 2 + 2 \cdot 3 + \cdots + 2 \cdot n) - n.$$

Then factoring out the 2, we get

$$T(n) = 2 \cdot (1 + 2 + 3 + \cdots + n) - n.$$

In other words,

$$T(n) = 2S_1(n) - n.$$

Hence $2S_1(n) = T(n) + n = n^2 + n = n(n+1)$, so $S_1(n) = n(n+1)/2$. In other words,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2},$$

just as before.

6.4 Remark. We have used summation notation sparingly in Example 6.3, in order to minimize the chance of misunderstanding. If you have confidence in working with summation notation, then you could do the calculation in Example 6.3 more briefly as follows. Let

$$T(n) = \sum_{k=1}^{n} [k^2 - (k-1)^2].$$

On the one hand,

$$T(n) = [1^2 - 0^2] + [2^2 - 1^2] + \cdots + [n^2 - (n-1)^2] = n^2.$$

On the other hand, since $k^2 - (k-1)^2 = k^2 - (k^2 - 2k + 1) = 2k - 1$,

$$T(n) = \sum_{k=1}^{n} (2k-1) = \left(\sum_{k=1}^{n} 2k\right) - \left(\sum_{k=1}^{n} 1\right) = 2\left(\sum_{k=1}^{n} k\right) - n = 2S_1(n) - n.$$

Hence $2S_1(n) = T(n) + n = n^2 + n = n(n+1)$, so $S_1(n) = n(n+1)/2$. In other words,

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

6.5 Remark. In general, summation notation is good to save writing and to show the general form of the terms in a sum, but to show the pattern of a sum as a whole, it is better to write it out in long form. Example 6.3 illustrates both of these points. Thus both of these ways to write a sum have their uses, so one should be flexible in choosing which to use and one should not hesitate to switch back and forth as the need arises.

[17] Because it collapses down like an old-fashioned folding telescope, on account of all this cancellation, the sum $T(n)$ is called a *telescoping sum*.

6.6 Remark. It might appear that the method we have used in Example 6.3 to find $S_1(n)$ does not involve proof by induction. But it would be more accurate to say that in Example 6.3, we found $S_1(n)$ without explicit induction. If one were formally to prove the formula $\sum_{k=1}^{n}[k^2-(k-1)^2]=n^2$, then one would use induction to do it. However, this formula is sufficiently obvious that it is not necessary to prove it formally. Thus induction is implicitly involved, but it is shifted to a place in the argument where what it would be used to prove is so clear that the proof by induction can be omitted.

6.7 Remark. There is a way of expressing the method that we have just used to find $S_1(n)$ which should clarify how it fits into a general scheme for finding $S_r(n)$. Notice that

$$\begin{aligned} S_0(n) &= 1^0+2^0+3^0+\cdots+n^0 \\ &= \underbrace{1+1+1+\cdots+1}_{n \text{ times}} = n. \end{aligned}$$

In the notation of Example 6.3, we have on the one hand that

$$T(n)=[1^2-0^2]+[2^2-1^2]+\cdots+[n^2-(n-1)^2]=n^2.$$

and on the other hand that

$$T(n)=\sum_{k=1}^{n}(2k-1)=2\sum_{k=1}^{n}k-\sum_{k=1}^{n}1=2S_1(n)-S_0(n).$$

Hence $n^2=2S_1(n)-S_0(n)$, so $2S_1(n)=n^2+S_0(n)$, so

$$S_1(n)=\frac{n^2}{2}+\frac{S_0(n)}{2}.$$

Since we know that $S_0(n)=n$, we get $S_1(n)=(n^2/2)+(n/2)=n(n+1)/2$. Thus the essence of this method is to express $S_1(n)$ in terms of $S_0(n)$. As we shall see, each of the quantities $S_0(n), S_1(n), S_2(n), S_3(n), \ldots$ can be expressed in terms of the preceding ones, so in principle we can determine them all one after another.

Exercise 1. Let $n\in\mathbf{N}$. Let $T(n)=\sum_{k=1}^{n}[k^3-(k-1)^3]$. By writing $T(n)$ out in long form, show that it is a telescoping sum and that $T(n)=n^3$. Then, by evaluating $T(n)$ in a different way, deduce without explicit induction that

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

Exercise 2. Use a suitable telescoping sum to give a proof without explicit induction that for each $n\in\mathbf{N}$,

$$1^3+2^3+\cdots+n^3=\frac{n^2(n+1)^2}{4}.$$

Exercise 3. Use a suitable telescoping sum to find a simpler expression for the sum $1^4+2^4+\cdots+n^4$, where $n\in\mathbf{N}$. Check your answer by verifying that it works for small values of n. (Given that the answer is a polynomial of degree five in n, it suffices to check six different values of n to be sure that your answer is right. The reason is that if two polynomials of degree five agree at six different points, then these six points are roots of the difference of the two polynomials, and this difference is a polynomial of degree at most five. A polynomial of degree at most five can have at most five roots, unless it is the zero polynomial.)

6.8 Remark. As you should know, the volume of a right circular cone of height h and base radius r is $(1/3)\pi r^2 h$ and the volume of a sphere of radius r is $(4/3)\pi r^3$. You might be interested to know that both of these facts can be proved without calculus by using the formula for $1^2+2^2+\cdots+n^2$ given in Exercise 1. It would be an excellent exercise for you to carry out this proof. The basic idea is to approximate the volume of the cone or the sphere from above and from below by the sum of the volumes of a large number of thin cylindrical discs centered on the axis of the cone or on a diameter of the sphere.

Sums of Geometric Progressions Revisited.

Here we shall describe a method to find the formula for the sum of a of a geometric progression and you will be asked to use a similar method to evaluate certain related sums.

6.9 Example. Let x be a real number. Suppose that $x \neq 1$. Let $n \in \mathbf{N}$. Prove without explicit induction that

$$1 + x + x^2 + \cdots + x^{n-1} = \frac{1 - x^n}{1 - x}. \tag{1}$$

First Solution. Let

$$S = 1 + x + x^2 + \cdots + x^{n-1}.$$

Then

$$xS = \qquad x + x^2 + \cdots + x^{n-1} + x^n.$$

Hence

$$S - xS = 1 + (x - x) + (x^2 - x^2) + \cdots + (x^{n-1} - x^{n-1}) - x^n,$$

so $(1 - x)S = 1 - x^n$. Now $1 - x \neq 0$ because $x \neq 1$. Therefore

$$S = \frac{1 - x^n}{1 - x}.$$

This completes the proof. ■

Second Solution. Let $S = 1 + x + x^2 + \cdots + x^{n-1}$. In summation notation,

$$S = \sum_{k=0}^{n-1} x^k.$$

Hence

$$xS = \sum_{k=0}^{n-1} x^{k+1}.$$

As k goes from 0 to $n - 1$, $k + 1$ goes from 1 to n, so the last sum can be rewritten as

$$xS = \sum_{k=1}^{n} x^k.$$

Thus

$$S = 1 + \sum_{k=1}^{n-1} x^k$$

and

$$xS = \sum_{k=1}^{n-1} x^k + x^n,$$

so $S - xS = 1 - x^n$. In other words, $(1 - x)S = 1 - x^n$. Now $1 - x \neq 0$ because $x \neq 1$. Therefore

$$S = \frac{1 - x^n}{1 - x}.$$

This completes the proof. ■

Exercise 4. Let x be a real number. Suppose that $x \neq 1$. Let $n \in \mathbf{N}$.

(a) Find a simpler expression for the sum

$$T = x + 2x^2 + 3x^3 + \cdots + nx^n.$$

For your final answer, put everything over a common denominator and in the resulting numerator, collect like powers of x. (Hint: By considering $T - xT$, express T in terms of the sum S from Example 6.9.)

(b) In summation notation, the sum T in part (a) may be expressed as follows:

$$T = \sum_{k=1}^{n} kx^k.$$

Redo do part (a) but work entirely in summation notation instead of "$\cdots$" notation. (Hints:

$$\sum_{k=2}^{n+1}(k-1)x^k = \sum_{k=1}^{n+1}(k-1)x^k,$$

because when $k = 1$, we have $k - 1 = 0$. Also,

$$\sum_{k=1}^{n} x^k = x\sum_{k=1}^{n} x^{k-1} = xS,$$

where S is as in Example 6.9.)

Exercise 5. Let x be a real number. Suppose that $x \neq 1$. Let $n \in \mathbf{N}$. Find a simpler expression for the sum

$$U = \sum_{k=1}^{n} k^2x^k.$$

For your final answer, put everything over a common denominator and in the resulting numerator, collect like powers of x. (Hint: By considering $U - xU$, express U in terms of the sum T from Exercise 4 and the sum S from Example 6.9. You will probably find it easier to do this exercise using summation notation instead of "$\cdots$" notation. For this reason, part (b) of Exercise 4 is important preparation for this exercise.)

6.10 Remark. The results of Example 6.9, Exercise 4, and Exercise 5 have many applications in areas such as bank reserves, amortization of mortgages, the theory of power series, and probability theory (for instance, to calculate the expected value and the standard deviation of the number of times a pair of dice must be rolled until a dice sum of 5 occurs).

6.11 Remark. If you have studied infinite series, then it may interest you to know that if $|x| < 1$, then as $n \to \infty$, the parts that depend on n in the formulas obtained in Example 6.9, Exercise 4, and Exercise 5 tend to zero, resulting in the satisfyingly simple expressions

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}, \qquad \sum_{k=1}^{\infty} kx^k = \frac{x}{(1-x)^2}, \qquad \text{and} \qquad \sum_{k=1}^{\infty} k^2x^k = \frac{x(1+x)}{(1-x)^3}.$$

But remember, these infinite series only converge when $|x| < 1$.

Remark. Let a and b be real numbers. Recall that $b^2 - a^2$ and $b^3 - a^3$ can be factored as follows: $b^2 - a^2 = (b-a)(b+a)$ and $b^3 - a^3 = (b-a)(b^2 + ba + a^2)$. Similarly, it is easy to check that $b^4 - a^4 = (b-a)(b^3 + b^2a + ba^2 + a^3)$. The next exercise deals with how to factor $b^n - a^n$ when n is any natural number.

Exercise 6. Let a and b be real numbers and let $n \in \mathbf{N}$.

(a) Verify that

$$b^n - a^n = (b-a)(b^{n-1} + b^{n-2}a + b^{n-3}a^2 + \cdots + ba^{n-2} + a^{n-1}). \tag{2}$$

(Hint: Start with the right hand side and show that it can be simplified to obtain the left hand side.)

(b) Verify that

$$b^{n-1} + b^{n-2}a + b^{n-3}a^2 + \cdots + ba^{n-2} + a^{n-1} = \sum_{k=0}^{n-1} b^{n-1-k}a^k.$$

(c) Use part (b) to reprove part (a) in summation notation.

(d) Also verify that

$$b^{n-1} + b^{n-2}a + b^{n-3}a^2 + \cdots + ba^{n-2} + a^{n-1} = \sum_{k=0}^{n-1} b^k a^{n-1-k}.$$

6.12 Remark. It is worth noticing that when $b = 1$ and $a = x \neq 1$, equation (2) reduces to equation (1).

An Application of Exercise 6. Let $n \in \mathbf{N}$. If $P(x) = (x-a)Q(x)$, where $Q(x)$ is a polynomial of degree $n-1$, then obviously $P(x)$ is a polynomial of degree n and $P(a) = 0$. Conversely, suppose $P(x)$ is a polynomial of degree n and $P(a) = 0$. We shall show that there is a polynomial $Q(x)$ of degree $n-1$ such that $P(x) = (x-a)Q(x)$. To see this first note that since $P(x)$ is a polynomial of degree n, there exist coefficients $c_0, c_1, \ldots c_n$ such that $P(x) = \sum_{m=0}^{n} c_m x^m$ and $c_n \neq 0$. Since $P(a) = 0$,

$$P(x) = P(x) - P(a) = \sum_{m=0}^{n} c_m x^m - \sum_{m=0}^{n} c_m a^m = \sum_{m=0}^{n} c_m (x^m - a^m).$$

Now for $m = 0$, we have $x^m - a^m = 1 - 1 = 0$, while by Exercise 6, for $m = 1, \ldots, n$, we have $x^m - a^m = (x-a)Q_m(x)$, where

$$Q_m(x) = x^{m-1} + x^{m-2}a + x^{m-3}a^2 + \cdots + xa^{m-2} + a^{m-1}.$$

Hence $P(x) = \sum_{m=1}^{n} c_m(x-a)Q_m(x) = (x-a)Q(x)$, where $Q(x) = \sum_{m=1}^{n} c_m Q_m(x)$. Since each $Q_m(x)$ is a polynomial of degree $m-1$ and since $c_n \neq 0$, $Q(x)$ is a polynomial of degree $n-1$.

Divisibility and Congruences Revisited (*Optional*).

Here we shall consider several alternative approaches to some of the results on divisibility from Section 5.

Exercise 7. Let $a, b, m \in \mathbf{Z}$. Suppose $a \equiv b \mod m$. Use the result of Exercise 26(b) in Section 4 to prove by induction that for each $n \in \mathbf{N}$, $a^n \equiv b^n \mod m$.

Exercise 8. Let $a, b, m \in \mathbf{Z}$ and let $n \in \mathbf{N}$. Use the result of Exercise 7 to prove that if m divides $b-a$, then m divides $b^n - a^n$.

Exercise 9. In Example 5.10, we saw that for each $n \in \mathbf{N}$, 3 divides $4^n - 1$, and in Exercise 5 in Section 5 you were asked to prove that for each $n \in \mathbf{N}$, 5 divides $7^n - 2^n$. Explain how the result of Exercise 8 makes it obvious that these statements are true. (You should learn the earlier method as well as the method suggested here. The present method is more enlightening, but the previous method provides a proof that is self-contained and short.)

Exercise 10. Let $a, b, m \in \mathbf{Z}$ and let $n \in \mathbf{N}$. Use the result of Exercise 6 to give a second proof that if m divides $b-a$, then m divides $b^n - a^n$.

Exercise 11. Let $a, b, m \in \mathbf{Z}$ and let $n \in \mathbf{N}$. Use the binomial theorem, Exercise 11 in Section 5, to give a third proof that if m divides $b - a$, then m divides $b^n - a^n$. (Hint: Write b as $c + a$, where $c = b - a$, and calculate $b^n = (c + a)^n$ by means of the binomial theorem.)

Exercise 12.

(a) Verify that for each r in the set $\{0, 1, 2, 3, 4, 5\}$, we have $r^3 \equiv r \mod 6$.

(b) Explain how it follows from part (a) and Remark 4.65 and and the result of Exercise 7 that for each $x \in \mathbf{Z}$, $x^3 \equiv x \mod 6$.

(c) In Section 5, you were asked to prove that for each $x \in \mathbf{Z}$, 6 divides $x^3 - x$. Explain how this follows from part (b). (You should learn the earlier method as well as the method suggested here. The present method is more enlightening, but the previous method provides a proof that is self-contained and short.)

More About Divisibility and Congruences (*Optional*).

You may have learned in school that a number is divisible by 9 if and only if the sum of its digits is divisible by 9. For instance, the sum of the digits in 36 is $3 + 6 = 9$, and this is divisible by 9, so 36 is divisible by 9. Of course it is not news that 36 is divisible by 9, but if we apply this test to larger numbers, we can save some work. For instance, the sum of the digits in 1386 is $1 + 3 + 8 + 6 = 18$, and this is divisible by 9, so 1386 is divisible by 9. In the next exercise, you are asked to justify this test for divisibility by 9. The two exercises after that deal with some other tests for divisibility which can be justified in a similar way.

Exercise 13. Let x be a whole number. Prove that x is divisible by 9 iff the sum of its digits is divisible by 9. (Hint: x can be expressed in the form $x = d_n 10^n + d_{n-1} 10^{n-1} + \cdots + d_1 10^1 + d_0$, where $d_0, d_1, \ldots, d_n \in \{0, 1, 2, \ldots, 9\}$ are the digits of x. Notice that $10 \equiv 1 \mod 9$. Then apply the result of Exercise 7 with $a = 10$ and $b = 1$ to show that $x \equiv d_n + d_{n-1} + \cdots + d_1 + d_0 \mod 9$.)

Exercise 14. Let x be a whole number. Prove that x is divisible by 3 iff the sum of its digits is divisible by 3.

Exercise 15. Let x be a whole number. Prove that x is divisible by 11 iff the alternating sum of its digits is divisible by 11. (By the alternating sum of the digits of x, we mean the first digit, minus the second digit, plus the third digit, and so on. For instance, 143 is divisible by 11 because $1 - 4 + 3 = 0$, which is divisible by 11. Hint: $10 \equiv -1 \mod 11$.)

More on Sums of Powers (*Optional*).

In Remark 6.7, we suggested a general method to evaluate sums of powers of natural numbers. Now you will be asked to develop this suggestion in detail. As preparation, you may find it helpful to do the following exercise on how to work with summation notation.

Exercise 16. Consider a rectangular array

$$\begin{array}{cccc} a(1,0) & a(1,1) & \cdots & a(1,r) \\ a(2,0) & a(2,1) & \cdots & a(2,r) \\ \vdots & \vdots & & \vdots \\ a(n,0) & a(n,1) & \cdots & a(n,r) \end{array}$$

of numbers. By writing the sums out in long form, show that

$$\sum_{k=1}^{n} \sum_{q=0}^{r} a(k,q) = \sum_{q=0}^{r} \sum_{k=1}^{n} a(k,q).$$

Now here is the exercise in which you are asked to develop in detail the method to evaluate sums of powers of natural numbers that was suggested in Remark 6.7.

Exercise 17. For all $r \in \boldsymbol{\omega}$ and $n \in \mathbf{N}$, let

$$S_r(n) = \sum_{k=1}^{n} k^r.$$

Observe that for each $n \in \mathbf{N}$, $S_0(n) = n$. Expressions for $S_1(n)$, $S_2(n)$, $S_3(n)$, and $S_4(n)$ were considered in earlier exercises. Let $r \in \mathbf{N}$. Find coefficients $c(r,0), c(r,1), \ldots, c(r,r-1)$ such that for each $n \in \mathbf{N}$,

$$S_r(n) = \frac{n^{r+1}}{r+1} + \sum_{q=0}^{r-1} c(r,q) S_q(n).$$

(Hint: In Example 6.1, we saw how to express $S_1(n)$ in terms of $S_0(n)$. From Exercise 1, you should have learned how to express $S_2(n)$ in terms of $S_1(n)$ and $S_0(n)$. From Exercise 2, you should have learned how to express $S_3(n)$ in terms of $S_2(n)$, $S_1(n)$, and $S_0(n)$. And from Exercise 3, you should have learned how to express $S_4(n)$ in terms of $S_3(n)$, $S_2(n)$, $S_1(n)$, and $S_0(n)$. In this problem, you should use a similar method to express $S_r(n)$ in terms of $S_{r-1}(n), \ldots, S_1(n), S_0(n)$ for a general natural number r. At a certain point, you will need to expand $(k-1)^{r+1}$. Use the binomial theorem to do this. The calculations will go a little more smoothly if you first write $(k-1)^{r+1}$ as $[(-1)+k]^{r+1}$. You may also find that Exercise 16 helps.)

Still More on Sums of Powers (*Optional*).

Here we shall consider yet another way to evaluate the sums $S_r(n) = 1^r + 2^r + \cdots + n^r$. This new method has the advantage that it makes it possible to find the formula for $S_{r+1}(n)$ from the formula for $S_r(n)$ alone. To introduce it, let us begin by recalling these formulas for some small values of r. In each case, we shall expand the right hand side of the formula. We have

$$S_1(n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2} = \frac{n^2}{2} + \frac{n}{2}, \tag{3}$$

$$S_2(n) = 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6} = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6}, \tag{4}$$

and

$$S_3(n) = 1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4} = \frac{n^4}{4} + \frac{n^3}{2} + \frac{n^2}{4}, \tag{5}$$

for instance. Notice that in each of these three examples, $S_r(n)$ is given by a polynomial $P_r(n)$ in which the leading term is $n^{r+1}/(r+1)$, the sum of the coefficients is 1, and the constant term is zero. Note that the leading term $n^{r+1}/(r+1)$ is equal to the integral $\int_0^n t^r\,dt$. This reflects the fact that when n is large, this integral is close to the sum $S_r(n)$. In fact, $S_r(n)$ is the upper Riemann sum for this integral, corresponding to the subdivision $0 < 1 < 2 < \cdots < n$ of the interval from 0 to n. By pursuing these ideas, we get a particularly elegant way to find the expressions for the sums $S_r(n)$ for general whole numbers r. In the next exercise, you are asked to carry this out. This exercise requires calculus, but only for polynomial functions.

Exercise 18. Define a sequence of functions $P_0, P_1, P_2, \ldots$ and a sequence of numbers $B_0, B_1, B_2, \ldots$ inductively as follows. For all $x \in \mathbf{R}$, let $P_0(x) = B_0 x$ where $B_0 = 1$, and for all $r \in \boldsymbol{\omega}$, let

$$P_{r+1}(x) = \int_0^x (r+1) P_r(t)\,dt + B_{r+1} x,$$

where B_{r+1} is a constant that is chosen so that $P_{r+1}(1) = 1$. Notice that $P_0(0) = 0$ and for each $r \in \boldsymbol{\omega}$, $P_{r+1}(0) = 0$. Hence for each $r \in \boldsymbol{\omega}$, $P_r(0) = 0$. As before, for all $r \in \boldsymbol{\omega}$ and all $n \in \mathbf{N}$, let $S_r(n) = \sum_{k=1}^{n} k^r$. Notice that for each $n \in \mathbf{N}$, $S_0(n) = n = P_0(n)$.

(a) Find $P_1(x)$, $P_2(x)$, and $P_3(x)$. Then verify that $P_1(n)$, $P_2(n)$, and $P_3(n)$ agree with the right-hand sides of the formulas for $S_1(n)$, $S_2(n)$, and $S_3(n)$ that are displayed in equations (3), (4), and (5).

(b) Find the derivative

$$\frac{d}{dx}P_{r+1}(x)$$

in terms of $P_r(x)$ and B_{r+1}. (If you do not remember how to do this kind of thing, consult a calculus book to review the fundamental theorem of calculus and related results.)

(c) Prove by induction that for each $r \in \boldsymbol{\omega}$, for each $x \in \mathbf{R}$, $P_r(x) - P_r(x-1) = x^r$. (Hint: In the inductive step, consider the derivative

$$\frac{d}{dx}\big[P_{r+1}(x) - P_{r+1}(x-1) - x^{r+1}\big]$$

and remember that if the derivative of a function on $\mathbf{R}$ is zero, then the function is constant.)

(d) Deduce from part (c) that for each $r \in \boldsymbol{\omega}$, for each $n \in \mathbf{N}$, $S_r(n) = P_r(n)$.

(e) Use the result of part (d) to find expressions for $S_4(n), S_5(n), \ldots, S_{10}(n)$, valid for all $n \in \mathbf{N}$.

6.13 Remark. In Exercise 18, we had $B_0 = 1$ by definition and in the course of your calculations you should have found that $B_1 = 1/2$, $B_2 = 1/6$, $B_4 = -1/30$, $B_6 = 1/42$, $B_8 = -1/30$, $B_{10} = 5/66$, and B_3, B_5, B_7, and B_9 are all zero. You can use this information as a check on your work.

Exercise 19. Let $P_0, P_1, P_2, \ldots$ and $B_0, B_1, B_2, \ldots$ be as in Exercise 18. Prove by induction that for each $r \in \boldsymbol{\omega}$, for each $x \in \mathbf{R}$, we have

$$P_r(x) = \sum_{q=0}^{r} \frac{1}{r+1}\binom{r+1}{q} B_q x^{r+1-q}.$$

6.14 Remark. The numbers $B_0, B_1, B_2, B_3, B_4, \ldots$ from Exercise 18 are called *Bernoulli numbers*,[18] after the Swiss mathematician Jakob Bernoulli (1654–1705), also known as James Bernoulli, who called attention to them in his book *Ars Conjectandi*, published posthumously in 1713. These numbers occur in many other places in mathematics. For instance, the Bernoulli numbers with even indices figure in the power series for $\tan x$ and also in the exact sums for the series

$$\sum_{n=1}^{\infty} \frac{1}{n^2}, \qquad \sum_{n=1}^{\infty} \frac{1}{n^4}, \qquad \sum_{n=1}^{\infty} \frac{1}{n^6}, \quad \ldots.$$

(In contrast, the exact sums for the series

$$\sum_{n=1}^{\infty} \frac{1}{n^3}, \qquad \sum_{n=1}^{\infty} \frac{1}{n^5}, \qquad \sum_{n=1}^{\infty} \frac{1}{n^7}, \quad \ldots$$

are unknown.)

[18] Different authors give different definitions for the Bernoulli numbers. For instance, the Bernoulli number with index 1 is often taken to be $-1/2$ instead of $B_1 = 1/2$. While there is no obvious general pattern to the Bernoulli numbers, it can be shown that $B_3, B_5, B_7, \ldots$ are all zero and that $B_2, B_4, B_6, \ldots$ alternate in sign. For this reason, some authors take the Bernoulli numbers to be just the numbers $B_2, -B_4, B_6, -B_8, \ldots$. When reading any discussion involving Bernoulli numbers, it is wise to check which definition of these numbers is in use.

Section 7. Complete Induction

In Section 5, we discussed the principle of mathematical induction. In this section we shall discuss the following refinement of the principle of mathematical induction.

7.1 The Principle of Complete Mathematical Induction. Let $P(n)$ be any statement about n. Suppose we have proved that

$$P(1) \text{ is true} \tag{1}$$

and that

$$\text{for each natural number } n, \text{ if } P(1), \ldots, P(n) \text{ are all true, then } P(n+1) \text{ is true.} \tag{2}$$

Then we may conclude that for each natural number n, $P(n)$ is true.

The principle of complete mathematical induction may be explained in a way that is similar to the way we explained the ordinary principle of mathematical induction, as follows. For each natural number n, let us say that n is *good* if $P(n)$ is true and let us say that n is *bad* if $P(n)$ is false. It conceivable that some natural numbers are good and some are bad. Suppose that we have proved (1) and (2), as stated in the principle of complete mathematical induction. By (1), the natural number 1 is good. Notice that (2) means that

if 1 is good, then 2 is good;
if 1 and 2 are good, then 3 is good;
if 1, 2, and 3 are good, then 4 is good;
and so on.

So since 1 is good, 2 must also be good. But then since 1 and 2 are good, 3 must also be good. Next, since 1, 2, and 3 are good, 4 must also be good. Continuing in this manner, we see that 1 is good, 2 is good, 3 is good, 4 is good, and so on. In other words, $P(1)$ is true, $P(2)$ is true, $P(3)$ is true, $P(4)$ is true, and so on. In other words, for each $n \in \mathbf{N}$, $P(n)$ is true.

Of course, the explanation in the preceding paragraph is not a proof of the principle of complete mathematical induction. Rather, it is a discussion of it and to some extent a reformulation of it in different words, as was the case for the explanation that we gave for the ordinary principle of mathematical induction.

It is worth remarking that we do not need to assume the principle of complete mathematical induction in addition to the ordinary principle of mathematical induction. This is because the principle of complete mathematical induction can be deduced from the ordinary principle of mathematical induction, as follows. Consider any sentence $P(n)$. Suppose we have proved that $P(1)$ is true and that for each natural number n, if $P(1), \ldots, P(n)$ are all true, then $P(n+1)$ is true. We wish to deduce that for each natural number n, $P(n)$ is true. We shall do this by applying the ordinary principle of mathematical induction to another sentence $Q(n)$, where $Q(n)$ is the sentence

$$\text{For each } k \in \{1, \ldots, n\},\ P(k) \text{ is true.}$$

Notice that for each given natural number n, to say that $Q(n)$ is true means the same thing as to say that $P(1), \ldots, P(n)$ are all true. Now $Q(1)$ is true because $P(1)$ is true. Let n be a natural number such that $Q(n)$ is true. Since $Q(n)$ is true, $P(1), \ldots, P(n)$ are all true. Hence $P(n+1)$ is true. Thus $P(1), \ldots, P(n), P(n+1)$ are all true. In other words, $Q(n+1)$ is true too. Therefore, by induction, for each natural number n, $Q(n)$ is true. In other words, for each natural number n, $P(1), \ldots, P(n)$ are all true. In particular, for each natural number n, $P(n)$ is true. This completes the proof that the principle of complete mathematical induction follows from the ordinary principle of mathematical induction.

We shall illustrate the principle of complete mathematical induction by using it to prove some results from elementary number theory. Clearly it is not essential to start from 1 in applying complete induction. Sometimes it may be more appropriate to start from 0. In our first illustration, it is most convenient to start from 2.

7.2 The Theorem on Existence of Prime Factorization. *Each natural number greater than or equal to* 2 *either is a product of prime numbers or is itself a prime number.*

Proof. Let $A = \{2, 3, 4, \dots\}$ be the set of all natural numbers that are greater than or equal to 2 and let $P(n)$ be the sentence

$$n \text{ is prime or is a product of primes.}$$

We wish to show that for each $n \in A$, $P(n)$ is true. We shall do this by complete induction.

BASE CASE: Note that $P(2)$ is true because 2 is prime.

INDUCTIVE STEP: Let $n \in A$ such that $P(2), \dots, P(n)$ are all true.[19] We wish to show that $P(n+1)$ is true too. Now either $n+1$ is prime or it is not prime.

Case 1. Suppose $n+1$ is prime. Then obviously $P(n+1)$ is true.

Case 2. Suppose $n+1$ is not prime. Then we can pick $a, b \in A$ such that $n+1 = ab$. Since $a > 1$, we have $b < n+1$. Since $b > 1$, we have $a < n+1$. Hence $a, b \in \{2, \dots, n\}$, so by the inductive hypothesis, $P(a)$ and $P(b)$ are both true. Thus a is prime or is a product of primes and b is prime or is a product of primes. Hence ab is a product of primes. In other words, $n+1$ is a product of primes. Thus $P(n+1)$ is true.

Thus in either case, $P(n+1)$ is true too.

CONCLUSION: Therefore, by complete induction, for each $n \in A$, $P(n)$ is true. In other words, each natural number greater than or equal to 2 is prime or is a product of primes. ■

Notice that in the preceding proof, there is no obvious way to show that $n+1$ is prime or is a product of primes just from the assumption that n is prime or is a product of primes. However, if we assume that each of the numbers $2, \dots, n$ is prime or is a product of primes, then it is easy to show that $n+1$ is prime or is a product of primes. This is why we used complete induction instead of just ordinary induction.

7.3 Corollary. *Each integer, except* 1 *and* -1*, is divisible by some prime number.*

Proof. Consider any integer x such that $x \neq 1$ and $x \neq -1$. Then $x \geq 2$ or $x = 0$ or $x \leq -2$.

Case 1. Suppose $x \geq 2$. Then by Theorem 7.2, x is either a product of prime numbers or is itself a prime number. If x is a product of prime numbers, then any of the prime numbers in this product is a prime number that divides x. If x is itself a prime number, then x itself is a prime number that divides x. Either way, there is a prime number that divides x.

Case 2. Suppose $x = 0$. Then any prime number divides x. For instance, 2 is a prime number that divides x.

Case 3. Suppose $x \leq -2$. Then $-x \geq 2$, so by Case 1 applied to $-x$ instead of x, there is a prime number p that divides $-x$. Then p divides x too.

Thus in any case, there is a prime number that divides x. ■

As our next illustration of complete induction, we shall show that if a prime number divides the product of two integers, then it divides at least one of these integers.[20]

7.4 The Theorem on Division by a Prime. *Let p be a prime number. Then for all integers x and y, if p divides xy, then p divides x or p divides y.*

Proof. Let y be an integer. Let $P(x)$ be the sentence

$$\text{If } p \text{ divides } xy, \text{ then } p \text{ divides } x \text{ or } p \text{ divides } y.$$

We wish to show that for each integer x, $P(x)$ is true. Observe that for each integer x, $P(x)$ has the same truth value as $P(-x)$, because p divides xy iff p divides $(-x)y$, and p divides x iff p divides $-x$. Hence it suffices to show that for each whole number x, $P(x)$ is true. We shall prove this by complete induction.

[19] It is this assumption that is referred to as *the inductive hypothesis*, in a proof by complete induction.

[20] Some people call this *Euclid's lemma*. It is Proposition 30 in Book VII of Euclid's *Elements*, written around 300 B.C.

BASE CASE: Observe that $P(0)$ is true, because p divides 0.

INDUCTIVE STEP: Let x be a whole number such that $P(0), \dots, P(x)$ are all true. We wish to show that $P(x+1)$ is true too. In other words, we wish to show that if p divides $(x+1)y$, then p divides $x+1$ or p divides y. Suppose p divides $(x+1)y$. Now either $x+1 < p$ or $x+1 \geq p$.

Case 1. Suppose $x+1 < p$. Dividing $x+1$ into p, we get

$$p = q(x+1) + r$$

for some natural number q and some $r \in \{0, \dots, x\}$. Now $ry = py - q(x+1)y$, so p divides ry. Hence, by the inductive hypothesis, p divides r or p divides y. Suppose p divides r. Then $r = 0$, because $0 \leq r < p$. Hence $p = q(x+1)$. But then $q = 1$ or $x+1 = 1$, because p is prime and q and $x+1$ are natural numbers. But $q \neq 1$, because $p \neq x+1$. Hence $x+1 = 1$, so $(x+1)y = y$, so p divides y after all.

Case 2. Suppose $x+1 \geq p$. Let $w = x+1-p$. Then $w \in \{0, \dots, x\}$ and $wy = (x+1)y - py$, so p divides wy, so by the inductive hypothesis, p divides w or p divides y. But $x+1 = w+p$, so if p divides w, then p divides $x+1$.

Thus in either case, p divides $x+1$ or p divides y. Hence $P(x+1)$ is true too.

CONCLUSION: Therefore, by complete induction, for each $x \in \boldsymbol{\omega}$, $P(x)$ is true. ■

7.5 Corollary. *Let p be a prime number. Then for each $n \in \mathbf{N}$, for all $x_1, \dots, x_n \in \mathbf{Z}$, if p divides the product $x_1 \cdots x_n$, then p divides at least one of the factors $x_1, \dots, x_n$.*

Proof. Let $P(n)$ be the sentence

> for all $x_1, \dots, x_n \in \mathbf{Z}$, if p divides the product $x_1 \cdots x_n$, then p divides at least one of the factors $x_1, \dots, x_n$.

We wish to show that for each $n \in \mathbf{N}$, $P(n)$ is true. We shall do this by (ordinary) induction.

BASE CASE: Clearly $P(1)$ is true.

INDUCTIVE STEP: Let $n \in \mathbf{N}$ such that $P(n)$ is true. To show that $P(n+1)$ is true too, consider any $x_1, \dots, x_n, x_{n+1} \in \mathbf{Z}$. Suppose p divides the product $x_1 \cdots x_n x_{n+1}$. Then by the theorem on division by a prime, p divides $x_1 \cdots x_n$ or p divides x_{n+1}. If p divides $x_1 \cdots x_n$, then by the inductive hypothesis, p divides at least one of $x_1, \dots, x_n$. Thus in either case, p divides at least one of $x_1, \dots, x_n, x_{n+1}$. Thus $P(n+1)$ is true too.

CONCLUSION: Therefore, by induction, for each $n \in \mathbf{N}$, $P(n)$ is true. ■

As we have seen, each natural number greater than or equal to 2 is either a product of prime numbers or is itself a prime number. It is convenient to regard a prime number p as the product consisting of the single factor p. Then we may say that each natural number greater than or equal to 2 is a product of prime numbers. We now wish to show that this prime factorization of such a natural number is unique up to the order of the factors.[21] For instance $6 = 2 \cdot 3$ and $6 = 3 \cdot 2$, but 6 cannot be expressed as a product of prime numbers in any other ways than these. Another way to put this is that the only way to express 6 as a product of primes with the factors written in order from smallest to largest is as $6 = 2 \cdot 3$. To take another example, the only way to express 12 as a product of primes with the factors written in order from smallest to largest is as $12 = 2 \cdot 2 \cdot 3$.

7.6 The Theorem on Uniqueness of Prime Factorization. *Each natural number greater than or equal to 2 can be expressed as a product of prime numbers in at most one way with the factors written in order from smallest to largest.*

Proof. Let $A = \{2, 3, 4, \dots\}$ be the set of all natural numbers greater than or equal to 2 and let $P(n)$ be the sentence

> n can be expressed as a product of prime numbers in at most one way with the factors written in order from smallest to largest.

[21] This is essentially Proposition 14 in Book IX of Euclid's *Elements*, written around 300 B.C.

We wish to show that for each $n \in A$, $P(n)$ is true. We shall do this by complete induction.

BASE CASE: Clearly $P(2)$ is true because the only way to express 2 as a product of primes is as the product consisting of the single factor 2.

INDUCTIVE STEP: Let $n \in A$ such that that $P(2), \ldots, P(n)$ are all true. Under this inductive hypothesis, we wish to show that $P(n+1)$ is true too. So suppose $r, s \in \mathbf{N}$, $p_1, \ldots, p_r, q_1, \ldots, q_s$ are primes, $n+1 = p_1 \cdots p_r = q_1 \cdots q_s$, $p_1 \leq \cdots \leq p_r$, and $q_1 \leq \cdots \leq q_s$. We wish to show that $r = s$ and for each $k \in \{1, \ldots, r\}$, $p_k = q_k$. If $r = 1$ or $s = 1$, then this is clear, since then $n+1$ is prime. Suppose $r \geq 2$ and $s \geq 2$. Now p_r divides the product $q_1 \cdots q_s$, so for some $k \in \{1, \ldots, s\}$, p_r divides q_k, since p_r is prime. Hence $p_r = q_k$, since q_k is prime. But $q_k \leq q_s$. Hence $p_r \leq q_s$. Similarly, q_s divides the product $p_1 \cdots p_r$, so q_s is one of $p_1, \ldots, p_r$, so $q_s \leq p_r$. Thus $p_r = q_s$. Let $m = p_1 \cdots p_{r-1}$. Then $m = q_1 \cdots q_{s-1}$ too. But $m \in \{2, \ldots, n\}$, so by the inductive hypothesis, $P(m)$ is true. In particular, $r - 1 = s - 1$ and for each $k \in \{1, \ldots, r-1\}$, $p_k = q_k$. It follows that $r = s$. But we also know that $p_r = q_s$. Hence for each $k \in \{1, \ldots, r\}$, $p_k = q_k$. Thus $P(n+1)$ is true too.

CONCLUSION: Therefore, by complete induction, for each $n \in A$, $P(n)$ is true. ■

A Second Proof of the Theorem on Uniqueness of Prime Factorization (*Optional*). We shall now present another proof of the uniqueness of prime factorization. This proof is more elementary than the one we have just given, but more intricate, since it starts almost from scratch. It uses the theorem on existence of prime factorization but not the theorem on division by a prime (and not even the division lemma, Lemma 5.21). It is surprisingly recent, having been discovered by Ernst Zermelo around 1912 (but not published by him until 1934). It was rediscovered by F. A. Atkinson (later Lord Cherwell),[22] who published it in 1933. Here it is.

Second Proof of Uniqueness of Prime Factorization. Let $A = \{2, 3, 4, \ldots\}$ be the set of all natural numbers greater than or equal to 2 and let $P(n)$ be the sentence

> n can be expressed as a product of prime numbers in at most one way with the factors written in order from smallest to largest.

We wish to show that for each $n \in A$, $P(n)$ is true. We shall do this by complete induction.

First let us make an observation. Suppose $x \in A$ such that $P(x)$ happens to be true. Let y be a prime number that divides x. By the theorem on existence of prime factorization, applied to x/y, we see that x may be expressed as a product of primes including y. Since $P(x)$ is true, this is the unique way to express x as a product of primes (except that the order of the factors may be varied). It follows that in any way of expressing x as a product of primes, each prime y that divides x must be one of the factors in this product.

Now let us show by complete induction that for each $n \in A$, $P(n)$ is true.

BASE CASE: Clearly $P(2)$ is true because the only way to express 2 as a product of primes is as the product consisting of the single factor 2.

INDUCTIVE STEP: Let $n \in A$ such that that $P(2), \ldots, P(n)$ are all true. Under this inductive hypothesis, we wish to show that $P(n+1)$ is true too. So suppose $r, s \in \mathbf{N}$, $p_1, \ldots, p_r, q_1, \ldots, q_s$ are primes, $n+1 = p_1 \cdots p_r = q_1 \cdots q_s$, $p_1 \leq \cdots \leq p_r$, and $q_1 \leq \cdots \leq q_s$. We wish to show that $r = s$ and for each $k \in \{1, \ldots, r\}$, $p_k = q_k$. If $r = 1$ or $s = 1$, then this is clear, since then $n+1$ is prime. Suppose $r \geq 2$ and $s \geq 2$. Now either $p_1 < q_1$ or $p_1 = q_1$ or $p_1 > q_1$. Suppose $p_1 < q_1$. (We shall derive a contradiction from this assumption.) Let $a = n + 1 - p_1 q_2 \cdots q_s$. Then $a < n+1$. Also, $a = (q_1 - p_1)q_2 \cdots q_s \geq (q_1 - p_1)2 \geq 2$. Thus $a \in \{2, \ldots, n\}$, so $P(a)$ is true. Now the prime p_1 divides a, because p_1 divides $n+1$. Hence by the observation that we made earlier in the proof, in any way of expressing a as a product of primes, the prime p_1 must be one of the factors in this product. But one way to express a as a product of primes is as $a = d_1 \cdots d_\ell q_2 \cdots q_s$ where $d_1, \ldots, d_m$ are primes such that $d_1 \cdots d_\ell = q_1 - p_1$. (In case $q_1 - p_1 = 1$, there are no d_k's needed and we just have $a = q_2 \cdots q_s$.) Now for each $k \in \{1, \ldots, \ell\}$, we have $p_1 \neq d_k$, because

[22] Lord Cherwell was a physicist. It is interesting to mention some details of his career. In 1914, he worked out mathematically how to recover an aircraft from a spin and made the first tests of his solution himself. It is lucky for him that his calculations were correct — before his work on this problem, spins often led to fatal crashes. During the second world war, he was scientific advisor to Churchill, and after it, he played a central role in establishing the Atomic Energy Authority in Britain.

if $p_1 = d_k$, then p_1 divides $q_1 - p_1$, so p_1 divides q_1, so $p_1 = q_1$ (because q_1 is prime), which contradicts our assumption that $p_1 < q_1$. Also, for each $k \in \{2, \ldots, s\}$, we have $p_1 \neq q_k$, because $p_1 < q_1 \leq q_k$. Thus p_1 is not one of the factors $d_1, \ldots, d_\ell, q_2, \ldots, q_m$. Thus we have reached a contradiction. Hence it must not be the case that $p_1 < q_1$. Similarly, it is not the case that $p_1 > q_1$. Thus $p_1 = q_1$. Let $m = p_2 \cdots p_r$. Then $m = q_2 \cdots q_s$ too. But $m \in \{2, \ldots, n\}$, so by the inductive hypothesis, $P(m)$ is true. In particular, $r = s$ and for each $k \in \{2, \ldots, r\}$, $p_k = q_k$. But we also know that $p_1 = q_1$. Hence for each $k \in \{1, \ldots, r\}$, $p_k = q_k$. Thus $P(n+1)$ is true too.

CONCLUSION: Therefore, by complete induction, for each $n \in A$, $P(n)$ is true. ■

7.7 The Fundamental Theorem of Arithmetic. *Each natural number greater than or equal to 2 is expressible as a product of primes in exactly one way with the factors written in order from smallest to largest.*

Proof. Consider any natural number $n \geq 2$. By the theorem on existence of prime factorization, n can be expressed as a product of primes. It is intuitively clear that the primes in this product can be written in order from smallest to largest. (In fact, this can be proved, by induction on the number of factors in this product, but we omit the details.) Finally, by the theorem on uniqueness of prime factorization, there is no other way to express n as a product of primes with the factors written in order from smallest to largest. ■

The object of the next two exercises is to help you see that the theorem on division by a prime and the theorem on uniqueness of prime factorization are neither trivial nor obvious. But first, here is an an example to help you with the first of these two exercises.

7.8 Example. Let $y_1, y_2 \in \mathbf{Z}$. As we have seen, if $y_1 y_2$ is even, then y_1 is even or y_2 is even. In other words, if 2 divides $y_1 y_2$, then 2 divides y_1 or 2 divides y_2. Let us consider an alternative way to prove this. Suppose 2 divides $y_1 y_2$. We wish to show that 2 divides y_1 or 2 divides y_2. By the division lemma, Lemma 5.21, there exist $q_1, q_2 \in \mathbf{Z}$ and $r_1, r_2 \in \{0, 1\}$ such that $y_1 = 2q_1 + r_1$ and $y_2 = 2q_2 + r_2$. Then $r_1 = y_1 - 2q_1$ and $r_2 = y_2 - 2q_2$, so

$$\begin{aligned} r_1 r_2 &= (y_1 - 2q_1)(y_2 - 2q_2) = y_1 y_2 - 2y_1 q_2 - 2q_1 y_2 + 4q_1 q_2 \\ &= y_1 y_2 - 2(y_1 q_2 + q_1 y_2 - 2q_1 q_2). \end{aligned}$$

By assumption, 2 divides $y_1 y_2$. Obviously, 2 divides $2(y_1 q_2 + q_1 y_2 - 2q_1 q_2)$, because $y_1 q_2 + q_1 y_2 - 2q_1 q_2$ is an integer. Thus 2 divides $y_1 y_2 - 2(y_1 q_2 + q_1 y_2 - 2q_1 q_2)$. In other words, 2 divides $r_1 r_2$. But the possible values for r_1 are 0 and 1, as are the possible values for r_2, so the possible values for $r_1 r_2$ are $(0)(0) = 0$, $(0)(1) = 0$, $(1)(0) = 0$, and $(1)(1) = 1$. Of these possible values for $r_1 r_2$, only 0 is divisible by 2. Thus $r_1 r_2$ must be 0, so at least one of r_1 and r_2 must be 0. If $r_1 = 0$, then $y_1 = 2q_1 + r_1 = 2q_1$, so 2 divides y_1. If $r_2 = 0$, then $y_2 = 2q_2 + r_2 = 2q_2$, so 2 divides y_2. Thus 2 divides y_1 or 2 divides y_2, as we wished to show.

Exercise 1. Let $y_1, y_2 \in \mathbf{Z}$.

- **(a)** Without using the theorem on division by a prime, or any of its consequences (such as Remark 4.50) show that if 3 divides $y_1 y_2$, then 3 divides y_1 or 3 divides y_2. (Hint: Adapt the argument of Example 7.8, replacing the divisor 2 there by the divisor 3 that we are considering here. By the division lemma, Lemma 5.21, there exist $q_1, q_2 \in \mathbf{Z}$ and $r_1, r_2 \in \{0, 1, 2\}$ such that $y_1 = 3q_1 + r_1$ and $y_2 = 3q_2 + r_2$. Suppose 3 divides $y_1 y_2$. Show that 3 divides $r_1 r_2$. Then, by examining all the $3 \times 3 = 9$ possibilities for r_1 and r_2, show that at least one of r_1 and r_2 must be 0. To write out the possible values for $r_1 r_2$ efficiently, you may find it helpful to show them in the form of a multiplication table.)
- **(b)** Do the same as in part (a), but with 3 replaced by 5. (Then $\{0, 1, 2\}$ must be replaced by $\{0, 1, 2, 3, 4\}$.) How many possibilities for r_1 and r_2 are there to examine this time?
- **(c)** If the 3 in part (a) were replaced by p, where p is a prime number, then what should $\{0, 1, 2\}$ be replaced by and how many possibilities for r_1 and r_2 would there be to examine if the method of part (a) were followed?

Incidentally, you should not have to use complete induction (or even ordinary induction) in this exercise.

Exercise 2. Let $S = \{\, 3k+1 : k \in \boldsymbol{\omega} \,\}$. In other words, let $S = \{\, 1, 4, 7, 10, \dots \,\}$.

(a) Show that S is closed under multiplication. In other words, show that for all $x, y \in S$, we have $xy \in S$.

For the purposes of the remainder of this exercise, let us agree that to say x *is S-prime* means $x \in S$ and $x \neq 1$ and for each $a \in S$, for each $b \in S$, if $x = ab$, then $a = 1$ or $b = 1$. (For instance, 4 is S-prime, because even though $4 = (2)(2)$, the factor 2 does not belong to S.)

(b) List all elements of S that are less than or equal to 25 and determine which of them are S-prime.

(c) Find an element of S that can be written in two different ways as a product of S-primes with the factors written in order from smallest to largest. Hence the analog for S of the theorem on uniqueness of prime factorization is not true.

(d) Find $p, x, y \in S$ such that p is S-prime and p divides xy, but p does not divide x and p does not divide y. Hence the analog for S of the theorem on division by a prime is not true.

7.9 Remark. It is worth noticing that the set S in Exercise 2 is $\{\, x \in \mathbf{N} : x \equiv 1 \mod 3 \,\}$.

7.10 Remark. The example treated in Exercise 2 is due to the great German mathematician David Hilbert (1862–1943). Later, when we study infinite sets, we shall encounter another example of Hilbert's.

Exercise 3. Let S be as in Exercise 2 and let "S-prime" have the same meaning as in that exercise. Use complete induction to show that each element of S greater than or equal to 4 either is a product of S-primes or is itself S-prime. Hence the analog for S of the theorem on existence of prime factorization is true. (Suggestion: Let $P(k)$ be the sentence "$3k+1$ is S-prime or is a product of S-primes." Then what you are asked to prove by complete induction is that for each $k \in \mathbf{N}$, $P(k)$ is true.)

7.11 Definitions. Let S be a subset of $\mathbf{R}$.

(a) To say that a *is the least element of* S means that $a \in S$ and for each $x \in S$, $a \leq x$.

(b) To say that S *has a least element* means that there exists $a \in S$ such that a is the least element of S.

7.12 Examples. $\mathbf{N}$ has a least element, namely 1. $\mathbf{Z}$ does not have a least element and neither does $(0, 1]$.

7.13 Remark. In Definition 7.11, it makes sense to speak of "the least element of S" rather than "a least element of S" because if a, a' are two least elements of S, then $a \leq a'$ (since $a' \in S$) and $a' \leq a$ (since $a \in S$), so $a = a'$.

Exercise 4.

(a) Suppose S is a subset of $\mathbf{N}$ and S does not have a least element. Show that S is empty. (Hint: Prove, by complete induction, that for each $n \in \mathbf{N}$, we have $n \notin S$.)

(b) Suppose S is a nonempty subset of $\mathbf{N}$. Show that S has a least element.

7.14 Remark (*Optional*). The *well-ordering principle* states that each nonempty subset of $\mathbf{N}$ has a least element. Thus in Exercise 4, we saw that the principle of complete mathematical induction implies the well-ordering principle. Near the beginning of this section, we saw that the ordinary principle of mathematical induction implies the principle of complete mathematical induction. Now in fact, the ordinary principle of mathematical induction, the principle of complete mathematical induction, and the well-ordering principle are all equivalent. To complete the proof of this equivalence, it remains only to show that the well-ordering principle implies the principle of mathematical induction. To show this, assume the well-ordering principle but do not assume the principle of mathematical induction. Consider any sentence $P(n)$ such that $P(1)$ is true and for each $n \in \mathbf{N}$, if $P(n)$ is true, then $P(n+1)$ is true. We wish to show that for each $n \in \mathbf{N}$, $P(n)$ is true. Suppose not. Let S be the set of all natural numbers b such that $P(b)$ is not true. Then S is not empty. Hence by the well-ordering principle, S has a least element, say a. Since $a \in S$, $P(a)$ is not true. Hence $a \neq 1$. Thus a is a natural number different from 1, so $a = k+1$ where $k = a - 1 \in \mathbf{N}$. Then $k \notin S$, because a is the least element of S. Hence $P(k)$ is true. But then $P(k+1)$ is true. In other words, $P(a)$ is true. But $P(a)$ is not true. This contradiction shows that it must be the case that for each $n \in \mathbf{N}$, $P(n)$ is true.

7.15 Remark. Similarly to Exercise 4(b), each nonempty subset of ω has a least element. More generally, let S be a nonempty subset of $\mathbf{Z}$ which has a lower bound in $\mathbf{Z}$. Then it follows from Exercise 4(b) that S

has a least element. For let b be a lower bound for S in $\mathbf{Z}$. (This means that $b \in \mathbf{Z}$ and for each $n \in S$, we have $b \leq n$.) Let $T = \{ n - b : n \in S \}$. Then T is a nonempty subset of $\boldsymbol{\omega}$, so T has a least element. Let x be the least element of T. Since $x \in T$, there exists $n \in S$ such that $x = n - b$. It is easy to check that n is the least element of S. Similarly, if S is a nonempty subset of $\mathbf{Z}$ which has an upper bound in $\mathbf{Z}$, then S has a largest element. (The formulation of the definitions of "upper bound in $\mathbf{Z}$" and "largest element of S" is left to you.)

Exercise 5. Recall that the sequence of Fibonacci numbers $F_1, F_2, F_3, \ldots$ is defined by $F_1 = 1$, $F_2 = 1$, and for all $n \in \{ 3, 4, 5, \ldots \}$, $F_n = F_{n-2} + F_{n-1}$. Notice that 1, 2, and 3 are Fibonacci numbers, $4 = 1 + 3$, 5 is a Fibonacci number, $6 = 1 + 5$, $7 = 2 + 5$, 8 is a Fibonacci number, $9 = 1 + 8$, $10 = 2 + 8$, $11 = 3 + 8$, $12 = 1 + 3 + 8$, and so on. This suggests that for each $n \in \mathbf{N}$, either n is a Fibonacci number or n is a sum of distinct nonconsecutive Fibonacci numbers. Prove that this is true. (Hint: Use complete induction. For $n = 1$, n is a Fibonacci number. Suppose $n \in \mathbf{N}$ such that each natural number less than or equal to n is either a Fibonacci number or a sum of distinct nonconsecutive Fibonacci numbers. Consider $n + 1$. Let m be the largest $k \in \{ 1, \ldots, n + 1 \}$ such that k is a Fibonacci number.[23] If $m = n + 1$, then $n + 1$ is a Fibonacci number. Suppose $m \neq n + 1$. Then $m \leq n$ and $n + 1$ is the sum of the natural number $n + 1 - m$ and the Fibonacci number m. Apply the inductive hypothesis to $n + 1 - m$. Explain why it follows that $n + 1$ is a sum of Fibonacci numbers and why they are distinct and nonconsecutive.)

Exercise 6. Let a be a nonzero real number. Find the mistake in the following argument which purports to prove that for each $n \in \mathbf{N}$, $a^{n-1} = 1$. Let $P(n)$ be the sentence

$$a^{n-1} = 1.$$

BASE CASE: Then $P(1)$ is true, because $a^{1-1} = a^0 = 1$.

INDUCTIVE STEP: Let $n \in \mathbf{N}$ such that $P(1), \ldots, P(n)$ are all true. Then

$$a^{(n+1)-1} = a^n = \frac{a^{n-1} \times a^{n-1}}{a^{n-2}} = \frac{1 \times 1}{1} = 1.$$

Thus $P(n + 1)$ is true too.

CONCLUSION: Therefore, by complete induction, for each $n \in \mathbf{N}$, $P(n)$ is true. ■

Exercise 7. Find the mistake in the following argument which purports to prove that for each $n \in \mathbf{N}$, either n is prime or there exist $r, s \in \boldsymbol{\omega}$ such that $n = 2^r 3^s$. Let $P(n)$ be the sentence

$$\text{Either } n \text{ is prime or there exist } r, s \in \boldsymbol{\omega} \text{ such that } n = 2^r 3^s.$$

BASE CASE: Then $P(1)$ is true because $1 = 2^0 3^0$.

INDUCTIVE STEP: Let $n \in \mathbf{N}$ such that $P(1), \ldots, P(n)$ are all true. If $n + 1$ is prime, then clearly $P(n + 1)$ is true. Suppose $n + 1$ is not prime. Then $n + 1 = a_1 a_2$ for some $a_1, a_2 \in \{ 1, \ldots, n \}$. By the inductive hypothesis, $a_1 = 2^{r_1} 3^{s_1}$ and $a_2 = 2^{r_2} 3^{s_2}$ for some $r_1, s_1, r_2, s_2 \in \boldsymbol{\omega}$. Then $n + 1 = 2^{r_1 + r_2} 3^{s_1 + s_2}$, so $P(n + 1)$ is true in this case as well. Thus in either case, $P(n + 1)$ is true too.

CONCLUSION: Therefore, by complete induction, for each $n \in \mathbf{N}$, $P(n)$ is true. ■

Exercise 8. (*More about Bernoulli numbers.*) Let $P_0, P_1, P_2, \ldots$ and $B_0, B_1, B_2, \ldots$ be as in Exercise 18 in Section 6.

(a) Show that for each $r \in \mathbf{N}$, we have

$$B_r = 1 - \sum_{q=0}^{r-1} \frac{1}{r+1} \binom{r+1}{q} B_q.$$

[23] You may take it for granted that m exists but it is worth mentioning that this can easily be deduced from Exercise 4.

(Hint: Consider $P_r(1)$.)

(b) Show that for each $r \in \mathbf{N}$, $P_r(-1) = 0$.

(c) Deduce from part (b) that for each $r \in \mathbf{N}$, we have

$$B_r = \sum_{q=0}^{r-1} \frac{1}{r+1} \binom{r+1}{q} (-1)^{r+1-q} B_q.$$

(d) Show that for each even number $r \geq 2$, we have

$$B_r = \frac{1}{2} - \frac{1}{r+1} - \sum_{\substack{q=2 \\ q \text{ even}}}^{r-2} \frac{1}{r+1} \binom{r+1}{q} B_q.$$

Note that this formula gives a method for finding each of the numbers $B_2, B_4, B_6, \ldots$ in terms of the preceding ones and that when $r = 2$, it reduces to $B_2 = 1/2 - 1/(2+1) = 1/6$. (Hint: Add the expressions for B_r from parts (a) and (c).)

(e) Show by complete induction that for each odd number $r \geq 3$, we have $B_r = 0$. (Hint: Use the method suggested in the hint for part (d) to derive a formula that gives a method for finding each of the numbers $B_3, B_5, B_7, \ldots$ in terms of the preceding ones.)

A Generalization of the Theorem on Division by a Prime.

The next result, which we used in Example 4.52 and in the series of exercises following that example, reduces to the theorem on division by a prime in the special case where d is a prime number.

7.16 Theorem. *Let n be a natural number. Then for each natural number d, for all integers $x_1, \ldots, x_n$, if d divides the product $x_1 \cdots x_n$, then there exist natural numbers $d_1, \ldots, d_n$ such that d_k divides x_k for $k = 1, \ldots, n$ and $d = d_1 \cdots d_n$*

Proof. To save writing, let $I = \{1, \ldots, n\}$. Let $P(d)$ be the sentence

> for all integers $x_1, \ldots, x_n$, if d divides the product $x_1 \cdots x_n$, then there exist natural numbers $d_1, \ldots, d_n$ such that d_k divides x_k for each $k \in I$ and $d = d_1 \cdots d_n$.

We shall show by complete induction that for each natural number d, $P(d)$ is true.

BASE CASE: Clearly $P(1)$ is true because if $d = 1$, we may take $d_1 = 1, \ldots, d_n = 1$.

INDUCTIVE STEP: Let d be a natural number such that $P(1), \ldots, P(d)$ are all true. Under this inductive hypothesis, we wish to show that $P(d+1)$ is true too. Consider any integers $x_1, \ldots, x_n$. Suppose $d+1$ divides the product $x_1 \cdots x_n$. We wish to show that there exist natural numbers $d_1, \ldots, d_n$ such that d_k divides x_k for each $k \in I$ and $d+1 = d_1 \cdots d_n$. Now $d+1$ is a natural number greater than or equal to 2, so there is a prime number p such that p divides $d+1$. Let $d' = (d+1)/p$. Then $d' \in \{1, \ldots, d\}$. Hence $P(d')$ is true by the inductive hypothesis. Now p divides the product $x_1 \cdots x_n$, because p divides $d+1$ and $d+1$ divides $x_1 \cdots x_n$. Hence by Corollary 7.5, p divides x_{k_0} for some $k_0 \in I$. Let $x'_{k_0} = x_{k_0}/p$ and for all other $k \in I$, let $x'_k = x_k$. The $x'_1, \ldots, x'_n$ are integers and d' divides the product $x'_1 \cdots x'_n$. Since $P(d')$ is true, there exist natural numbers $d'_1, \ldots, d'_n$ such that d'_k divides x'_k for each $k \in I$ and $d' = d'_1 \cdots d'_n$. Let $d_{k_0} = pd'_{k_0}$ and for all other $k \in I$, let $d_k = d'_k$. Then $d_1, \ldots, d_n$ are natural numbers, d_k divides x_k for each $k \in I$, and $d+1 = d_1 \cdots d_n$. Thus $P(d+1)$ is true too.

CONCLUSION: Therefore, by complete induction, for each natural number d, $P(d)$ is true. ■

7.17 Corollary. *Let n be a natural number, let $d, x_1, \ldots, x_n$ be integers, and suppose d divides the product $x_1 \cdots x_n$. Then there exist natural numbers $d_1, \ldots, d_n$ such that d_k divides x_k for each $k \in \{1, \ldots, n\}$ and $d = \operatorname{sgn}(d) d_1 \cdots d_n$.*

Proof. Once again, to save writing, let $I = \{1, \ldots, n\}$. Now either $d \in \mathbf{N}$ or $-d \in \mathbf{N}$ or $d = 0$. If $d \in \mathbf{N}$, then $\operatorname{sgn}(d) = 1$, so the desired conclusion follows from Theorem 7.16. Consider the case where $-d \in \mathbf{N}$.

Then $-d$ also divides $x_1 \cdots x_n$, so by Theorem 7.16, since $-d \in \mathbf{N}$, there exist natural numbers $d_1, \ldots, d_n$ such that d_k divides x_k for each $k \in I$ and $-d = d_1 \cdots d_n$. Then $\operatorname{sgn}(d) d_1 \cdots d_n = (-1) d_1 \cdots d_n = (-1)(-d) = d$. Finally consider the case where $d = 0$. Let $d_k = 1$ for each $k \in I$. Then d_k divides x_k for each $k \in I$. Furthermore, $d = \operatorname{sgn}(d) d_1 \cdots d_n$, because $\operatorname{sgn}(d) = 0$. ■

7.18 Remark. Let d be a natural number and let a and b be integers. By Theorem 7.16 with $n = 2$, if d divides the product ab, then there exist natural numbers d_1 and d_2 such that d_1 divides a, d_2 divides b, and $d = d_1 d_2$.

7.19 Remark. Let d, a, and b be integers. By Corollary 7.17 with $n = 2$, if d divides the product ab, then there exist natural numbers d_1 and d_2 such that d_1 divides a, d_2 divides b, and $d = \operatorname{sgn}(d) d_1 d_2$.

Common Factors and Relative Primality (*Optional*).

7.20 Definition. Let $a, b, f \in \mathbf{Z}$. To say that f *is a common factor of* a *and* b means that f divides a and f divides b.

For instance, the common factors of 12 and 30 are 1, 2, 3, 6, −1, −2, −3, and −6. A somewhat silly example is that any integer f is a common factor of 0 and 0. A common factor is also called a *common divisor*.

7.21 Definition. Let $a, b \in \mathbf{Z}$. To say that a *and* b *are relatively prime* means that for each $f \in \mathbf{Z}$, if f is a common factor of a and b, then $f = 1$ or $f = -1$.

7.22 Remark. Let $a, b \in \mathbf{Z}$. Then 1 and −1 are always common factors of a and b. Thus a and b are relatively prime exactly when 1 and −1 are the only common factors of a and b. Sometimes one says that a *and* b *have no common factors* to mean that a and b are relatively prime. Of course this is illogical, since a and b always have at least the common factors 1 and −1, but these may be regarded as trivial common factors.

Exercise 9. Let x be a rational number. Show that we can find an integer a and a natural number b such that $x = a/b$ and the fraction a/b is in lowest terms. (Hint: As we know, we can find an integer m_0 and a natural number n_0 such that $x = m_0/n_0$. Hence it suffices to show that for each natural number n, for each integer m, we can find an integer a and a natural number b such that $m/n = a/b$ and the fraction a/b is in lowest terms. Prove the latter statement by complete induction on n. Note that if a and b are integers, with $b \neq 0$, then to say that the fraction a/b is in lowest terms means that a and b are relatively prime. This is the definition of *lowest terms*. It is not the definition of *relatively prime*. The definition of *relatively prime* is Definition 7.21.)

Exercise 10. Let $d, a, b \in \mathbf{Z}$. Suppose d and a are relatively prime and d divides ab. Show that d divides b. (Hint: Use Remark 7.19.)

Exercise 11. Let $n \in \mathbf{N}$ and let $a, b_1, \ldots, b_n \in \mathbf{Z}$. Suppose that for each $k \in \{1, \ldots, n\}$, a and b_k are relatively prime. Let $b = b_1 \cdots b_n$. Show that a and b are relatively prime. (Hint: Use Corollary 7.17.)

Exercise 12. Let $a, b \in \mathbf{Z}$. Show that a and b are relatively prime iff for each prime number p, p divides at most one of a and b.

The Euclidean Algorithm and Related Topics (*Optional*).

In the remainder of this section we discuss highest common factors and lowest common multiples, the Euclidean algorithm, and two more ways to prove the theorem on division by a prime.[24] This material may be omitted without serious loss of continuity.

7.23 Definition. Let $a, b, h \in \mathbf{Z}$. To say that h *is a highest common factor of* a *and* b means that h is a common factor of a and b, and for each $f \in \mathbf{Z}$, if f is a common factor of a and b, then f divides h.

[24] The first of these other ways is more or less the way that Euclid proved this theorem in his *Elements*, written around 300 B.C.

For instance, the highest common factors of 12 and 30 are 6 and -6. As another example, 0 is the only highest common factor of 0 and 0. It is a fact that any two integers a and b have a highest common factor, but this requires proof.

Exercise 13. Let a be a nonzero integer.

(a) What are the highest common factors of a and 0?

(b) What are the highest common factors of a and a?

(c) Let b be an integer such that a divides b. What are highest common factors of a and b?

It was mentioned above that 0 is the only highest common factor of 0 and 0. This is the only case where a highest common factor is unique. Whenever a, b, h are integers and h is a highest common factor of a and b, then $-h$ is also a highest common factor of a and b. However this is the extent of the possible nonuniqueness of highest common factors. Whenever a, b, h_1, h_2 are integers and h_1 and h_2 are both highest common factors of a and b, then h_1 divides h_2 and h_2 divides h_1, so $h_2 = h_1$ or $h_2 = -h_1$.

A highest common factor is also called a *greatest common divisor*. When a and b are integers that are not both zero, then the highest common factors of a and b are largest in absolute value among the common divisors of a and b. However this is not the definition of highest common factors.

When we speak of *the* highest common factor of two integers a and b, we mean the nonnegative highest common factor. For instance, *the* highest common factor of 12 and 30 is 6, not -6.

The fundamental theorem of arithmetic makes it possible to read off the highest common factor of two natural numbers a and b from their prime factorizations. For instance, the prime factorizations of 12 and 30 are $12 = 2 \cdot 2 \cdot 3$ and $30 = 2 \cdot 3 \cdot 5$, so the highest common factor of 12 and 30 is the product of the factors that are common to these two factorizations, namely $2 \cdot 3 = 6$. When a and b are large, this method becomes cumbersome. A more efficient method, which is called *the Euclidean algorithm*, is based on the following exercise.

Exercise 14. Let a, b, q, r be integers such that $a = bq + r$. Show that for each integer d, d is a common factor of a and b iff d is a common factor of b and r.

We illustrate the Euclidean algorithm by using it to find the highest common factor of 2747 and 871. For each $d \in \mathbf{Z}$,

	d is a common factor of 2747 and 871	
iff	d is a common factor of 871 and 134	(because $2747 = 3 \times 871 + 134$)
iff	d is a common factor of 134 and 67	(because $871 = 6 \times 134 + 67$)
iff	d is a common factor of 67 and 0	(because $134 = 2 \times 67 + 0$)
iff	d divides 67.	

It follows that 67 is the highest common factor of 871 and 2747.

As the preceding example illustrates, the Euclidean algorithm for finding the highest common factor of two given natural numbers consists in dividing the smaller into the larger, replacing the larger by the smaller and the smaller by the remainder, and repeating this process until a remainder of 0 is obtained. Then the final dividend is the highest common factor of the original two numbers.

Exercise 15. Use the Euclidean algorithm to find the highest common factor of 7200 and 3132.

Remark. It is a fact, sometimes known as *Bézout's identity*,[25] that not only do any two integers a and b have a highest common factor, but the highest common factor of a and b turns out to be of the form $ma + nb$ for suitable integers m and n. In the next exercise, you are asked to show this.

Exercise 16.

[25] The French mathematician Etienne Bézout (1730 – 1783) proved an analog of this identity for polynomials. It is included in his 1779 book *Théorie générale des équations algébrique*. For integers it can be found earlier in the work of another French mathematician, Claude Gaspard Bachet de Méziriac (1581 – 1638). See `https://en.wikipedia.org/wiki/B%C3%A9zout%27s_identity`. Still, it is fair to say that the identity for integers is almost implicit in Propositions 1 and 2 of Book VII of Euclid's *Elements*, written around 300 B.C., and these propositions almost certainly predate Euclid.

(a) Show that for each $a \in \mathbf{Z}$, for each $b \in \mathbf{Z}$, there exist $m, n \in \mathbf{Z}$ such that $ma + nb$ is a common factor of a and b. (Hint: Let $P(a)$ be the sentence

> for each $b \in \mathbf{Z}$, there exist $m, n \in \mathbf{Z}$ such that $ma + nb$ is a common factor of a and b.

Use complete induction on a to show that for each $a \in \mathbf{N}$, $P(a)$ is true. In the inductive step, reason as in a single step of the Euclidean algorithm. Finally, use the fact that $P(a)$ is true for each $a \in \mathbf{N}$ to deduce that actually $P(a)$ is true for each $a \in \mathbf{Z}$.)

(b) Let $a, b, m, n \in \mathbf{Z}$ and suppose $ma + nb$ is a common factor of a and b. Show that $ma + nb$ is a highest common factor of a and b.

(c) Deduce from parts (a) and (b) that any two integers a and b have a highest common factor and that any highest common factor of a and b is of the form $ma + nb$ for suitable integers m and n.

7.24 Theorem. *Let $k, a, b, c \in \mathbf{Z}$. Suppose c is a highest common factor of a and b. Then kc is a highest common factor of ka and kb.*

Proof. The case where $k = 0$ or $c = 0$ is trivial. Suppose $k \neq 0$ and $c \neq 0$. Let d be a highest common factor of ka and kb. Clearly kc is a common factor of ka and kb, so kc divides d. Hence $d = kc\delta$ for some $\delta \in \mathbf{Z}$. Now since d is a common factor of ka and kb, we have $ka = d\alpha$ and $kb = d\beta$ for some $\alpha, \beta \in \mathbf{Z}$. Since $d = kc\delta$, we have $ka = kc\delta\alpha$ and $kb = kc\delta\beta$. Cancelling k, we get $a = c\delta\alpha$ and $b = c\delta\beta$, so $c\delta$ is a common factor of a and b. But c is a highest common factor of a and b. Hence $c\delta$ divides c, so $c = c\delta\delta'$ for some $\delta' \in \mathbf{Z}$. Cancelling c, we get $1 = \delta\delta'$. As δ and δ' are integers, it follows that $\delta = 1$ or $\delta = -1$. Since $d = kc\delta$, it follows that $d = kc$ or $d = -kc$. Hence kc is a highest common factor of ka and kb. ■

The proof of the preceding theorem uses only the existence of highest common factors but is somewhat intricate. By using what we know about the special form of highest common factors, a simpler proof of this theorem can be given. In the next exercise, you are asked to do this.

Exercise 17. Use the results of Exercise 16 to give an alternative proof of Theorem 7.24.

Exercise 18.

(a) Use the result of Theorem 7.24 to give an alternative solution of Exercise 10.

(b) By part (a), it is possible to give a solution of Exercise 10 that does not depend on the theorem on division by a prime. Show that the theorem on division by a prime can be deduced from the result of Exercise 10.

Exercise 19. Since our second proof of the theorem on uniqueness of prime factorization does not use the theorem on division by a prime, it is of interest to point out that the theorem on uniqueness of prime factorization can be used to prove the theorem on division by a prime. Work out such a proof. (Hint: Use the observation from the second paragraph of our second proof of the uniqueness of prime factorization, together with the theorem on existence of prime factorization.)

7.25 Definition. Let $a, b, m \in \mathbf{Z}$. To say that m *is a common multiple of a and b* means that a divides m and b divides m.

For instance, the common multiples of 4 and 6 are 0, 12, −12, 24, −24, 36, −36, and so on; note that these are precisely the integers that are divisible by 12. As another example, if a and b are integers and at least one of them is 0, then the only common multiple of a and b is 0.

7.26 Definition. Let $a, b, \ell \in \mathbf{Z}$. To say that ℓ *is a lowest common multiple of a and b* means that ℓ is a common multiple of a and b, and for each $m \in \mathbf{Z}$, if m is a common multiple of a and b, then ℓ divides m.

For instance, the lowest common multiples of 4 and 6 are 12 and −12. As another example, if a and b are integers and at least one of them is 0, then the lowest common multiple of a and b is 0, the only common multiple of a and b. This is the only case where a lowest common multiple is unique. Whenever a, b, ℓ are integers and ℓ is a lowest common multiple of a and b, then $-\ell$ is also a lowest common multiple of a and b. However, this is the extent of the possible nonuniqueness of lowest common multiples. Whenever

a, b, ℓ_1, ℓ_2 are integers and ℓ_1 and ℓ_2 are both lowest common multiples of a and b, then ℓ_1 divides ℓ_2 and ℓ_2 divides ℓ_1, so $\ell_2 = \ell_1$ or $\ell_2 = -\ell_1$.

A lowest common multiple is also called a *least common multiple*. When a and b are nonzero integers, the lowest common multiples of a and b are smallest in absolute value among the nonzero common multiples of a and b. However this is not the definition of lowest common multiples.

When we speak of *the* lowest common multiple of two integers a and b, we mean the nonnegative lowest common multiple of a and b. For instance, *the* lowest common multiple of 4 and 6 is 12, not -12.

Exercise 20. Let α, β, and n be integers. Suppose α divides n, β divides n, and α and β are relatively prime. Prove that $\alpha\beta$ divides n.

Exercise 21. Let a and b be nonzero integers and let h be a highest common factor of a and b. (Then $h \neq 0$.)

(a) Let $\alpha = a/h$ and $\beta = b/h$. Prove that α and β are relatively prime.

(b) Let $\ell = ab/h$. Prove that ℓ is a lowest common multiple of a and b. In particular, a and b have a lowest common multiple.

Section 8. Order Properties of the System of Real Numbers

As usual, for all real numbers a and b, we write $a < b$ to mean that a is strictly less than b, we write $b > a$ to mean $a < b$, we write $a \leq b$ to mean $a < b$ *or* $a = b$, and we write $b \geq a$ to mean $a \leq b$. We shall now state the basic properties of the order relation on $\mathbf{R}$.

8.1 Basic Order Properties of R.

(a) For all $a, b, c \in \mathbf{R}$, if $a < b$ and $b < c$, then $a < c$.

(b) For each $a \in \mathbf{R}$, it is not the case that $a < a$.

(c) For all $a, b \in \mathbf{R}$, if $a \neq b$, then $a < b$ or $b < a$.

(d) For all $a, b, c \in \mathbf{R}$, if $a < b$, then $a + c < b + c$.

(e) For all $a, b \in \mathbf{R}$, if $a > 0$ and $b > 0$, then $ab > 0$.

Certainly all of the properties just stated are familiar, but there are many other familiar elementary order properties of $\mathbf{R}$ besides the five just stated. As will become clear, these other familiar elementary properties are all consequences of the five basic ones.[26]

At first it might seem like a waste of time to prove these other familiar properties, since we already believe that they are true. However, there are a number of reasons for proving them. To do so is a good exercise in logic. It is easy to make mistakes in working with inequalities. If you have worked through the proofs of a fair number of the familiar properties of order in terms of the basic properties, you will be less likely to make such mistakes because you will have learned how to figure out for yourself what is true and what isn't.

Also, there are other mathematical structures besides the system of real numbers, in which properties similar to some or all of the basic order properties of $\mathbf{R}$ hold. For now, let us just mention the names of some of these structures, without explaining what they mean: *partially ordered sets*, *totally ordered sets*, *ordered groups*, *ordered fields*. If you pay attention to which basic order properties the other familiar order properties of $\mathbf{R}$ depend on, it will prepare you to study the more general structures just mentioned.

8.2 Proposition. *For all $a, b \in \mathbf{R}$, at most one of the following three conditions holds:*

$$a < b, \qquad a = b, \qquad b < a.$$

(Remark: Soon we shall show that in fact, for all $a, b \in \mathbf{R}$, exactly one of these conditions holds. To prove this however, we shall have to use property 8.1(c). To prove that at most one of them holds, it suffices to use properties 8.1(a) and 8.1(b).)

[26] We should mention that by "elementary order properties of $\mathbf{R}$," we mean those order properties of $\mathbf{R}$ which do not involve infinite sets of real numbers. The significance of this distinction will become clear later, when we discuss the completeness property of $\mathbf{R}$.

Proof of Proposition 8.2. Consider any $a, b \in \mathbf{R}$. For each of the three conditions mentioned, we must show that if that condition holds, then the other two do not.

Suppose $a < b$. We wish to show that $a \neq b$ and that it is not the case that $b < a$. We shall show each of these things by contradiction. Suppose $a = b$. Then in the inequality $a < b$, we may replace b by a to get $a < a$. But by 8.1(b), it is not the case that $a < a$. Thus we have reached a contradiction. Hence it must not be the case that $a = b$. Suppose $b < a$. Then by 8.1(a) (specialized to the case where $c = a$), from $a < b$ and $b < a$, we get $a < a$. But as before, it is not the case that $a < a$. Therefore it must not be the case that $b < a$.

Similarly, if $b < a$, then $b \neq a$ (so $a \neq b$) and it is not the case that $a < b$.

Finally, suppose $a = b$. As we just saw, if $a < b$, then $a \neq b$. Hence it must not be the case that $a < b$. Similarly, it is not the case that $b < a$. ■

8.3 Corollary. *Let $a, b \in \mathbf{R}$. Then $a < b$ iff $a \leq b$ and $a \neq b$.*

Proof. First, suppose $a < b$. Then $a < b$ or $a = b$ (since an "or" sentence is true when at least one of its parts is true). In other words, $a \leq b$. Also, $a \neq b$ by Proposition 8.2. Hence $a \leq b$ and $a \neq b$.

Conversely, suppose $a \leq b$ and $a \neq b$. In other words, suppose $a < b$ or $a = b$, and $a \neq b$. Then $a < b$, since if an "or" sentence is true and one of its parts is false, then its other part must be true. ■

8.4 Proposition. *Let $a, b, c \in \mathbf{R}$. Then:*

(a) *If $a \leq b$ and $b \leq c$, then $a \leq c$.*

(b) *$a \leq a$.*

(c) *If $a \leq b$ and $b \leq a$, then $a = b$.*

Proof. (a) Suppose $a \leq b$ and $b \leq c$. We wish to prove that $a \leq c$. Since $a \leq b$, either $a = b$ or $a < b$.

Case 1. Suppose $a = b$. Then in the inequality $b \leq c$, we may replace b by a to get $a \leq c$.

Case 2. Suppose $a < b$. Since $b \leq c$, either $b = c$ or $b < c$.

Subcase (a). Suppose $b = c$. Then in the inequality $a < b$, we may replace b by c to get $a < c$.

Subcase (b). Suppose $b < c$. Then since $a < b$ and $b < c$, by 8.1(a) we get $a < c$.

Thus in either subcase, $a < c$. Hence $a < c$ or $a = c$. In other words, $a \leq c$.

Thus in either case, $a \leq c$.

(b) Since $a = a$, we have $a = a$ or $a < a$. In other words, $a \leq a$.

(c) Suppose that $a \leq b$ and $b \leq a$. We wish to show that $a = b$. We shall show this by contradiction. Suppose $a \neq b$. Since $a \leq b$ and $a \neq b$, we have $a < b$ by Corollary 8.3. Similarly, since $b \leq a$ and $b \neq a$, we have $b < a$. But by Proposition 8.2, it is not possible to have both $a < b$ and $b < a$ at the same time. Hence it must not be the case that $a \neq b$. Therefore $a = b$. ■

Of the properties 8.1(a–e), so far we have used only 8.1(a) and 8.1(b). Next we shall use 8.1(c). Notice that properties 8.1(a–c) do not mention addition or multiplication.

8.5 Proposition. (The Trichotomy Property.) *For all $a, b \in \mathbf{R}$, exactly one of the following three conditions holds:*

$$a < b, \qquad a = b, \qquad b < a.$$

Proof. Consider any $a, b \in \mathbf{R}$. In Proposition 8.2, we saw that at most one of the specified conditions holds. It remains only to show that at least one of them holds. But either $a = b$ or $a \neq b$. Furthermore, if $a \neq b$, then either $a < b$ or $b < a$ by 8.1(c). ■

Next we shall use 8.1(d) for the first time. This is the property that links the order relation on $\mathbf{R}$ with operation of addition.

8.6 Proposition. *Let $a, b \in \mathbf{R}$. Then $a < b$ iff $b - a > 0$.*

Proof. Suppose $a < b$. Then by 8.1(d) (specialized to the case where $c = -a$), in the inequality $a < b$, we may add $-a$ to both sides to get $0 < b - a$. In other words, $b - a > 0$.

Conversely, suppose $b - a > 0$. In other words, suppose $0 < b - a$. Adding a to both sides in this inequality, we get $a < b$, by 8.1(d) again. ■

8.7 Proposition. *Let $a, b \in \mathbf{R}$. Then $a < b$ iff $-b < -a$.*

Proof. By Proposition 8.6, $a < b$ iff $b - a > 0$. Now $b - a = (-a) - (-b)$. Hence $a < b$ iff $(-a) - (-b) > 0$. But by Proposition 8.6 again, $(-a) - (-b) > 0$ iff $-b < -a$. ■

Exercise 1. Let $a \in \mathbf{R}$. Prove that:
(a) $a < 0$ iff $-a > 0$.
(b) $a > 0$ iff $-a < 0$.
For the sake of practice, give proofs that are based directly on 8.1(d), rather than using Proposition 8.6 or Proposition 8.7. In each part, remember to prove both the forward implication and the reverse implication.

Exercise 2. Let $a, b, c, d \in \mathbf{R}$. Prove that:
(a) If $a < b$ and $c < d$, then $a + c < b + d$. (Hint: Use 8.1(d) twice.)
(b) If $a > 0$ and $b > 0$, then $a + b > 0$.
(c) $a < b$ iff $a + c < b + c$.

Exercise 3. Let $a, b, c, d \in \mathbf{R}$.
(a) Suppose $a \leq b$. Prove that $a + c \leq b + c$. (You will need to consider two cases.)
(b) Suppose $a \leq b$ and $c \leq d$. Prove that $a + c \leq b + d$.

Next we shall use 8.1(e) for the first time. This is the property that links the order relation on $\mathbf{R}$ with the operation of multiplication.

8.8 Proposition. *Let $a, b \in \mathbf{R}$. Then:*
(a) *If $a < 0$ and $b < 0$, then $ab > 0$.*
(b) *If $a < 0$ and $b > 0$, then $ab < 0$.*
(c) *If $a > 0$ and $b < 0$, then $ab < 0$.*

Proof. (a) Suppose $a < 0$ and $b < 0$. Then $-a > 0$ and $-b > 0$ by Exercise 1(a). Hence $(-a)(-b) > 0$ by 8.1(e). But $(-a)(-b) = ab$. Hence $ab > 0$.

(b) Suppose $a < 0$ and $b > 0$. From $a < 0$ we get $-a > 0$ by Exercise 1(a). From $-a > 0$ and $b > 0$, we get $(-a)b > 0$. In other words, $-(ab) > 0$. Hence by Exercise 1(a) again, we get $ab < 0$.

(c) Since $ab = ba$, (c) may be deduced from (b) by interchanging the roles of a and b. ■

Exercise 4. Let $a, b \in \mathbf{R}$. Prove that:
(a) If $a \geq 0$ and $b \geq 0$, then $ab \geq 0$.
(b) If $a \leq 0$ and $b \leq 0$, then $ab \geq 0$.
(c) If $a \leq 0$ and $b \geq 0$, then $ab \leq 0$.
(d) If $a \geq 0$ and $b \leq 0$, then $ab \leq 0$.
(To avoid having to consider an unwieldy number of cases, note that either a and b are both nonzero, or at least one of them is zero. In the former case, the inequalities in the antecedents of the four conditional sentences (a)–(d) become strict. In the latter case, $ab = 0$, so all four conditional sentences are true because the consequents in them are true.)

8.9 Proposition. *Let $a, b \in \mathbf{R}$. Suppose $ab > 0$. Then either $a > 0$ and $b > 0$, or $a < 0$ and $b < 0$.*

Proof. First note that $a \neq 0$, because if $a = 0$, then $ab = 0$, which is not possible by Proposition 8.2 since $ab > 0$. Similarly $b \neq 0$. Since $a \neq 0$, either $a > 0$ or $a < 0$, by 8.1(c).

Case 1. Suppose $a > 0$. Since $b \neq 0$, either $b > 0$ or $b < 0$, by 8.1(c). But if $b < 0$, then by Proposition 8.8(c), $ab < 0$ which is not possible (by Proposition 8.2) since by assumption, $ab > 0$. Hence it must be that $b > 0$. Thus in this case, $a > 0$ and $b > 0$.

Case 2. Suppose $a < 0$. Then, by an argument similar to the one given in case 1, it follows that $b < 0$. Thus in this case, $a < 0$ and $b < 0$.

Thus either $a > 0$ and $b > 0$, or $a < 0$ and $b < 0$. ■

Exercise 5. Let $a, b \in \mathbf{R}$. Prove that:
(a) If $ab < 0$, then either $a < 0$ and $b > 0$, or $a > 0$ and $b < 0$.
(b) If $ab \geq 0$, then either $a \geq 0$ and $b \geq 0$, or $a \leq 0$ and $b \leq 0$.
(c) If $ab \leq 0$, then either $a \leq 0$ and $b \geq 0$, or $a \geq 0$ and $b \leq 0$.

8.10 Proposition. *Let $a \in \mathbf{R}$. Suppose $a \neq 0$. Then $a^2 > 0$.*

Proof. Since $a \neq 0$, either $a > 0$ or $a < 0$, by 8.1(c). If $a > 0$, then $a^2 = aa > 0$ by 8.1(e). If $a < 0$, then $-a > 0$ by Exercise 1(a), so $a^2 = (-a)(-a) > 0$ by 8.1(e) again. Thus in either case, $a^2 > 0$. ■

So far, we have not proved that there are any strictly positive real numbers. But this too follows from 8.1(a–e), as we shall now show.

8.11 Lemma. $1 > 0$.

Proof. Since $1 \neq 0$, we have $1^2 > 0$ by Proposition 8.10. But $1^2 = 1$. Hence $1 > 0$. ■

8.12 Proposition. *For each $n \in \mathbf{N}$, we have $n > 0$.*

Proof. We shall use induction. Let $P(n)$ be the sentence "$n > 0$".

BASE CASE: By Lemma 8.11, $1 > 0$. Hence $P(1)$ is true.

INDUCTIVE STEP: Let $n \in \mathbf{N}$ such that $P(n)$ is true. Then $n > 0$. As we just saw, $1 > 0$. Since $n > 0$ and $1 > 0$, we have $n + 1 > 0$ by Exercise 2(b). Thus $P(n + 1)$ is true.

CONCLUSION: Therefore, by induction, for each $n \in \mathbf{N}$, $P(n)$ is true. In other words, for each $n \in \mathbf{N}$, we have $n > 0$. ■

Exercise 6. Let $a \in \mathbf{R}$. Prove that:

(a) $a^2 \geq 0$.
(b) If $a < 0$, then $a^3 < 0$.
(c) If $a > 0$, then for each $n \in \mathbf{N}$, $a^n > 0$. (Use induction.)
(d) If $a < 0$, then for each $n \in \mathbf{N}$, if n is odd, then $a^n < 0$, and if n is even, then $a^n > 0$. (You should not need to use induction again. Instead, apply part (c) to $-a$.)

8.13 Proposition. *Let $a, b, c \in \mathbf{R}$. Suppose $a < b$. Then:*

(a) *If $c > 0$, then $ac < bc$.*
(b) *If $c < 0$, then $ac > bc$.*

Proof. (a) Suppose $c > 0$. Since $a < b$, we have $b - a > 0$ by Proposition 8.6. Since $b - a > 0$ and $c > 0$, it follows that $(b - a)c > 0$ by 8.1(e). Hence $bc - ac > 0$. In other words, $0 < bc - ac$. Hence $ac < bc$, again by Proposition 8.6.

(b) may be proved in a similar way, but Proposition 8.8(c) should be used instead of 8.1(e). ■

Exercise 7. Prove that for all $a, b, c, d \in \mathbf{R}$, if $0 \leq a < b$ and $0 \leq c < d$, then $ac < bd$. (Hint: This is similar to Exercise 2(a) but you should use Proposition 8.13(a) instead of 8.1(d).)

Exercise 8. Prove that it is not the case that for all $a, b, c, d \in \mathbf{R}$, if $a < b$ and $c < d$, then $ac < bd$.

Exercise 9. Let $a, b \in \mathbf{R}$. Suppose $a \geq 0$ and $b \geq 0$. Prove that:

(a) If $a < b$, then $a^2 < b^2$.
(b) If $a^2 \leq b^2$, then $a \leq b$. (Do not use square roots.)
(c) If $a^2 < b^2$, then $a < b$. (Again, do not use square roots.)
(d) If $a < b$, then $\sqrt{a} < \sqrt{b}$. (Apply part (c) to a different a and b.)

Exercise 10. Let $a, b \in \mathbf{R}$. Prove that if $0 < a < b$, then $a < \sqrt{ab} < b$.

Exercise 11. Let $a, b \in \mathbf{R}$. Suppose $a > 0$ and $b > 0$. Prove that $\sqrt{a + b} < \sqrt{a} + \sqrt{b}$.

Exercise 12. Let $a, b \in \mathbf{R}$. Suppose $a \geq 0$ and $b \geq 0$. Prove that:

(a) For each $n \in \mathbf{N}$, if $a < b$, then $a^n < b^n$. (Use induction.)
(b) For each $n \in \mathbf{N}$, if $a^n \leq b^n$, then $a \leq b$. (Do not use n-th roots.)
(c) For each $n \in \mathbf{N}$, if $a^n < b^n$, then $a < b$. (Do not use n-th roots.)
(d) For each $n \in \mathbf{N}$, if $a < b$, then $a^{1/n} < b^{1/n}$. (Apply part (c) to a different a and b.)

Exercise 13. Let $a, b \in \mathbf{R}$ and let $n \in \mathbf{N}$. Suppose $a < b \leq 0$. Prove that:

(a) If n is even, then $a^n > b^n$.
(b) If n is odd, then $a^n < b^n$.

(You should not need to use induction again. Just apply Exercise 12(a) to a different a and b.)

Exercise 14. Let $a, b, x \in \mathbf{R}$. Suppose $a < b$. Prove that exactly one of the following five conditions holds:

$$x < a, \qquad x = a, \qquad a < x < b, \qquad x = b, \qquad x > b$$

(Use the trichotomy property twice.)

Exercise 15. Let $a, b \in \mathbf{R}$ and let $n \in \mathbf{N}$. Suppose $a < b$ and n is odd. Prove that $a^n < b^n$. (You will need to consider several cases. You should need not to use induction again.)

8.14 Proposition. *Let $a \in \mathbf{R}$. Then:*
(a) *If $a > 0$, then $1/a > 0$.*
(b) *If $a < 0$, then $1/a < 0$.*

Proof. (a) Suppose $a > 0$. Then $a \neq 0$, by Proposition 8.2. Hence $1/a$ is defined and $1/a \neq 0$. Since $1/a \neq 0$, either $1/a < 0$ or $1/a > 0$, by 8.1(c). Hence if we can show that it is not the case that $1/a < 0$, then it will follow that $1/a > 0$. Suppose $1/a < 0$. We shall get a contradiction from this assumption. Since $a > 0$ and $1/a < 0$, it follows that $a(1/a) < 0$ by Proposition 8.8(c). But $a(1/a) = 1$. Hence $1 < 0$. Hence it is not the case that $1 > 0$, by Proposition 8.2. But $1 > 0$ by Lemma 8.11. Thus we have reached a contradiction. Hence it must not be the case that $1/a < 0$.

(b) may be proved in a similar way. ■

8.15 Corollary. *For all $m, n \in \mathbf{N}$, the rational number m/n is strictly positive.*

Proof. Consider any $m, n \in \mathbf{N}$. By Proposition 8.12, $m > 0$ and $n > 0$. Then by Proposition 8.14(a), $1/n > 0$. Hence by 8.1(e), $m(1/n) > 0$. In other words, $m/n > 0$. ■

Exercise 16. Let $a, b, c \in \mathbf{R}$. Prove that:
(a) If $c > 0$, then $a < b$ iff $ac < bc$.
(b) If $c < 0$, then $a < b$ iff $ac > bc$.
(In each part, the forward implication has already been proved, so you need only refer to the appropriate result, but you must supply a proof for the reverse implication.)

Exercise 17. Let $a, b \in \mathbf{R}$. Suppose $a \geq 0$ and $b \geq 0$. Prove that:
(a) $\sqrt{ab} \leq (a + b)/2$.
(b) If $\sqrt{ab} = (a + b)/2$, then $a = b$.
(Hint for both parts: Consider $(\sqrt{a} - \sqrt{b})^2$.)

8.16 Remark. The quantity $(a + b)/2$ is the average of a and b, also called the *arithmetic mean* of a and b. The quantity $\sqrt{ab}$ is called the *geometric mean* of a and b. The inequality in Exercise 17(a) is called the *inequality between the arithmetic and geometric means* of a and b. This inequality can be generalized to more than two numbers and also to weighted means. For instance, if $p, q, r \geq 0$ and $p + q + r = 1$, then for all $a, b, c \geq 0$, $a^p b^q c^r \leq pa + qb + rc$.

8.17 Proposition. *Let $a, b \in \mathbf{R}$. Then:*
(a) *If $0 < a < b$, then $1/a > 1/b$.*
(b) *If $a < b < 0$, then $1/a > 1/b$.*

Proof. (a) Suppose $0 < a < b$. Then $a > 0$ and by 8.1(a), $b > 0$. Hence by 8.1(e), $ab > 0$. Therefore, by Proposition 8.14(a), $1/(ab) > 0$. Hence by Proposition 8.13, in the inequality $a < b$, we may multiply both sides by $1/(ab)$ to get $a/(ab) < b/(ab)$. In other words, $1/b < 1/a$.

(b) may be proved similarly but Proposition 8.8(a) should be used instead of 8.1(e). ■

Exercise 18. Let $a \in \mathbf{R}$. Suppose $a > 1$. Prove that:
(a) For each $n \in \mathbf{N}$, $a^n > 1$. (Use induction.)
(b) For all $j, k \in \mathbf{Z}$, if $j < k$, then $a^j < a^k$. (Apply part (a).)

Exercise 19. Let $a \in \mathbf{R}$. Prove that:
(a) If $a > 1$, then $0 < 1/a < 1$.
(b) If $0 < a < 1$, then $1/a > 1$.

Exercise 20. Let $a \in \mathbf{R}$. Suppose $0 < a < 1$. Prove that:

(a) For each $n \in \mathbf{N}$, $0 < a^n < 1$. (You should be able to prove this without induction. Combine Exercise 19 with Exercise 18(a).)

(b) For all $j, k \in \mathbf{Z}$, if $j < k$, then $a^j > a^k$.

8.18 Lemma. *Let $c \in \mathbf{R}$. Suppose $c > 0$. Then $0 < \frac{1}{2}c < c$.*

Proof. By Lemma 8.11, $1 > 0$. Hence $1 + 1 > 0 + 1$ by 8.1(d). In other words, $2 > 1$. Hence $0 < 1/2 < 1$ by Exercise 19(a). Since $1/2 > 0$ and $c > 0$, we have $(1/2)c > 0$ by 8.1(e). Since $1/2 < 1$ and $c > 0$, we have $(1/2)c < (1)c$ by Proposition 8.13(a). Therefore $0 < (1/2)c < c$. ■

The next result implies that the system of real numbers is *densely ordered*; in other words, for all $a, b \in \mathbf{R}$, if $a < b$, then there exists $c \in \mathbf{R}$ such that $a < c < b$. (In contrast, the integers are not densely ordered. For instance, there is no integer between 2 and 3.)

8.19 Proposition. *Let $a, b \in \mathbf{R}$. Suppose $a < b$. Then $a < \frac{1}{2}(a + b) < b$.*

Proof. Let $c = b - a$. Since $a < b$, we have $c > 0$ by Proposition 8.6. Hence $0 < (1/2)c < c$ by Lemma 8.18. Thus $a + 0 < a + (1/2)c < a + c$ by 8.1(d). But $a + 0 = a$, $a + c = b$, and $a + (1/2)c = a + (1/2)b - (1/2)a = (1/2)(a + b)$. Thus $a < \frac{1}{2}(a + b) < b$. ■

8.20 Proposition. *Let $a, b \in \mathbf{R}$. The following are equivalent:*

(a) $a \leq b$.

(b) *For each $\varepsilon > 0$, $a \leq b + \varepsilon$.*

(c) *For each $\varepsilon > 0$, $a < b + \varepsilon$.*

Proof. We shall show that (a)⇒(b), (b)⇒(c), and (c)⇒(a). (From this it follows that if any one of (a), (b), (c) is true, then so are the other two.)

(a)⇒(b): Suppose $a \leq b$. Consider any $\varepsilon > 0$. Then $b + 0 < b + \varepsilon$ by 8.1(d), so $b \leq b + \varepsilon$, so by Proposition 8.4(a), $a \leq b + \varepsilon$. Now ε is an arbitrary real number > 0. Hence for each $\varepsilon > 0$, $a \leq b + \varepsilon$.

(b)⇒(c): Suppose for each $\varepsilon > 0$, $a \leq b + \varepsilon$. Consider any $\varepsilon_2 > 0$. Let $\varepsilon_1 = (1/2)\varepsilon_2$. Then $0 < \varepsilon_1 < \varepsilon_2$ by Lemma 8.18. Since $\varepsilon_1 > 0$, $a \leq b + \varepsilon_1$ because by assumption, for each $\varepsilon > 0$, $a \leq b + \varepsilon$. Since $\varepsilon_1 < \varepsilon_2$, we have $b + \varepsilon_1 < b + \varepsilon_2$ by 8.1(d). Thus $a \leq b + \varepsilon_1$ and $b + \varepsilon_1 < b + \varepsilon_2$. It follows that $a < b + \varepsilon_2$. But ε_2 is an arbitrary real number > 0. Hence for each $\varepsilon > 0$, $a < b + \varepsilon$.

(c)⇒(a): Suppose for each $\varepsilon > 0$, $a < b + \varepsilon$. Assume that $b < a$. We shall get a contradiction from this assumption. Since $b < a$, we have $a - b > 0$ by 8.1(d). Let $\varepsilon = a - b$. Then $\varepsilon > 0$. Hence $a < b + \varepsilon$. But $b + \varepsilon = b + (a - b) = a$. Thus $a < a$. But this is impossible by 8.1(b). Hence it must not be the case that $b < a$. Therefore $a \leq b$ by the trichotomy property (Proposition 8.5). ■

We have now shown how to deduce many of the familiar elementary order properties of $\mathbf{R}$ from the basic properties 8.1(a–e). In future, we shall be less pedantic in justifying manipulations with inequalities. When in doubt, though, you should try to trace any order properties that you use back to the basic ones.

8.21 Theorem. (Bernoulli's Inequality.) *Let $x \in \mathbf{R}$. Suppose $x \geq -1$. Then for each $n \in \boldsymbol{\omega}$,*

$$(1 + x)^n \geq 1 + nx \tag{1}$$

.

Proof. We shall use induction. Let $P(n)$ be the sentence (1) above.

BASE CASE: Then $P(0)$ is true, because $(1 + x)^0 = 1$ and $1 + 0 \cdot x = 1$.

INDUCTIVE STEP: Now let $n \in \boldsymbol{\omega}$ such that $P(n)$ is true. Then $(1 + x)^n \geq 1 + nx$. Since $1 + x \geq 0$, it follows that

$$(1 + x)^n(1 + x) \geq (1 + nx)(1 + x).$$

In other words,

$$(1 + x)^{n+1} \geq 1 + (n + 1)x + nx^2.$$

But $nx^2 \geq 0$, so $1 + (n+1)x + nx^2 \geq 1 + (n+1)x$. Hence

$$(1+x)^{n+1} \geq 1 + (n+1)x.$$

Thus $P(n+1)$ is true.

CONCLUSION: Therefore, by induction, for each $n \in \boldsymbol{\omega}$, $P(n)$ is true. In other words, for each $n \in \boldsymbol{\omega}$, $(1+x)^n \geq 1 + nx$. ■

8.22 Example. For each $n \in \mathbf{N}$, we have $2^{n-1} \geq n$, because by Bernoulli's inequality, since $n - 1 \in \boldsymbol{\omega}$, we have $2^{n-1} = (1+1)^{n-1} \geq 1 + (n-1) \cdot 1 = 1 + (n-1) = n$.

8.23 Example. Use Bernoulli's inequality to prove that for each $n \in \boldsymbol{\omega}$, $1.01^n \geq 0.01n$.

Solution. Consider any $n \in \boldsymbol{\omega}$. By Bernoulli's inequality (with $x = 0.01$), we have $1.01^n \geq 1 + 0.01n$. But $1 + 0.01n \geq 0.01n$. Hence $1.01^n \geq 0.01n$. ■

8.24 Remark. In working with equations, one cannot normally throw away terms as this will usually lead to a false equation. But as we saw in the proof of Bernoulli's inequality and in the solution of Example 8.23, in working with inequalities, one may sometimes throw away terms, so long as the resulting inequality is still true. If $a \geq b + c$ where b is positive, then $a \geq c$. This can be a very useful trick, as it often leads to a simpler inequality. (Note however that the new inequality is usually not equivalent to the original one. It is just a consequence of the original inequality. In other words, if the original inequality is true, then so is the new one, but not conversely.)

8.25 Example. Prove that for each $n \in \boldsymbol{\omega}$, $1.01^n \geq 0.000016n^2$.

Solution. . Notice that $1.004^2 = 1.008016 < 1.01$. Hence for each $n \in \boldsymbol{\omega}$, $1.01^n \geq (1.004^2)^n = 1.004^{2n} = (1.004^n)^2 = ((1 + 0.004)^n)^2 \geq (1 + 0.004n)^2 \geq (0.004n)^2 = 0.004^2 n^2 = 0.000016n^2$, where we have used Bernoulli's inequality in the fifth step. ■

8.26 Example. Without using square roots, show that for each $a > 1$, there exists $b > 1$ such that $a \geq b^2$.

Solution. For each $b \in \mathbf{R}$, we have $b^2 = [1 + (b-1)]^2 = 1 + 2(b-1) + (b-1)^2 = 1 + [2 + (b-1)](b-1)$. Now for each b such that $1 < b \leq 2$, we have $2 + (b-1) \leq 3$ and $b - 1 > 0$, so $[2 + (b-1)](b-1) \leq 3(b-1)$, so $1 + [2 + (b-1)](b-1) \leq 1 + 3(b-1)$, so $b^2 \leq 1 + 3(b-1)$. Let β be such that $1 + 3(\beta - 1) = a$. In other words, let $\beta = [(a-1)/3] + 1$. Then $\beta > 1$. Now either $\beta \leq 2$ or $\beta > 2$.

Case 1. Suppose $\beta \leq 2$. Let $b = \beta$. Then $1 < b \leq 2$, so $b^2 \leq 1 + 3(b-1)$. But $1 + 3(b-1) = 1 + 3(\beta - 1) = a$. Hence $b^2 \leq a$.

Case 2. Suppose $\beta > 2$. Let $b = 2$. Then $1 < b \leq 2$, so $b^2 \leq 1 + 3(b-1)$. But $b < \beta$, so $1 + 3(b-1) < 1 + 3(\beta - 1) = a$. Hence $b^2 \leq a$.

Thus in either case, there exists $b > 1$ such that $b^2 \leq a$. ■

Exercise 21. Without using r-th roots, show that for each $r \in \mathbf{N}$, for each $a > 1$, there exists $b > 1$ such that $a \geq b^r$. (Hint: Rewrite b^r as $[1 + (b-1)]^r$, use the binomial theorem to expand this, and generalize what we did in Example 8.26.)

Exercise 22. Use Bernoulli's inequality to prove the following results:

- **(a)** For each $a > 1$, there exists $\varepsilon > 0$ such that for each $n \in \boldsymbol{\omega}$, $a^n \geq \varepsilon n$. (Hint: Generalize what we did in Example 8.23.)
- **(b)** For each $a > 1$, there exists $\varepsilon > 0$ such that for each $n \in \boldsymbol{\omega}$, $a^n \geq \varepsilon n^2$. (Hint: Use Example 8.26 to generalize what we did in Example 8.25.)
- **(c)** For each $r \in \mathbf{N}$, for each $a > 1$, there exists $\varepsilon > 0$ such that for each $n \in \boldsymbol{\omega}$, $a^n \geq \varepsilon n^r$. (Hint: Use Exercise 21 to generalize what you did in part (b).)

We conclude this section with some material on solving inequalities.

8.27 Example. Solve the inequality $5 - 2x < 11$.

Solution. For each $x \in \mathbf{R}$, we have $5 - 2x < 11$ iff $-2x < 6$ iff $x > 6/(-2)$ iff $x > -3$. ■

8.28 Example. Solve the inequality $x^2 \geq 9$.

Solution. Consider any $x \in \mathbf{R}$. We have $x^2 \geq 9$ iff $x^2 - 9 \geq 0$. But $x^2 - 9 = (x+3)(x-3)$. Now either $x \leq -3$ or $-3 < x < 3$ or $x \geq 3$.

Case 1. Suppose $x \leq -3$. Then $x + 3 \leq 0$ and $x - 3 \leq -6 < 0$, so $(x+3)(x-3) \geq 0$, so $x^2 \geq 9$.

Case 2. Suppose $-3 < x < 3$. Then $x + 3 > 0$ and $x - 3 < 0$ so $(x+3)(x-3) < 0$, so $x^2 < 9$.

Case 3. Suppose $x \geq 3$. Then $x + 3 \geq 6 > 0$ and $x - 3 \geq 0$, so $(x+3)(x-3) \geq 0$, so $x^2 \geq 9$.

Thus for each $x \in \mathbf{R}$, $x^2 \geq 9$ iff $x \leq -3$ or $x \geq 3$. ■

Let us remark that it is poor style to say, for instance, that $x \geq 3$ is a solution of the inequality $x^2 \geq 9$. By definition, a solution of this inequality is a number x for which the inequality is true. The expression $x \geq 3$ is not a number, it is a sentence. (It has a subject, namely x, and a predicate, namely "is greater than or equal to 3.") It would be correct to say that if $x \geq 3$, then x is a solution of the inequality $x^2 \geq 9$. But this is unnecessarily wordy and yet does not tell us all we want to know about solutions of the inequality $x^2 \geq 9$. What we want is to know exactly when $x^2 \geq 9$. To say "$x^2 \geq 9$ iff $x \leq -3$ or $x \geq 3$" is shorter and tells us exactly what we want to know. Similar remarks apply in general to the process of solving inequalities.

Exercise 23. Solve the inequality $x^2 \leq x + 2$.

8.29 Example. Solve the inequality $x^2 + 2x \leq -2$.

Solution. Consider any $x \in \mathbf{R}$. We have $x^2 + 2x \leq -2$ iff $x^2 + 2x + 2 \leq 0$. But $x^2 + 2x + 2 = (x+1)^2 + 1 \geq 0 + 1 = 1 > 0$. Hence for each $x \in \mathbf{R}$, the inequality $x^2 + 2x \leq -2$ is false. ■

Exercise 24. Solve the inequality $x^2 \leq 6(x - 2)$.

Exercise 25. Solve the inequality $x^2 \geq 8(x - 3)$.

8.30 Example. Solve the inequality $\dfrac{3x-1}{x+2} \leq 2$.

Solution. Consider any $x \in \mathbf{R}$. Either $x = -2$ or $x \neq -2$. If $x = -2$, then $(3x+1)/(x+2)$ is undefined, so the inequality $(3x+1)/(x+2) \leq 2$ is false. If $x \neq -2$, then

$$\frac{3x+1}{x+2} \leq 2 \text{ iff } \frac{3x+1}{x+2} - 2 \leq 0 \text{ iff } \frac{3x+1-2(x+2)}{x+2} \leq 0 \text{ iff } \frac{x-3}{x+2} \leq 0.$$

If $x < -2$, then $x + 2 < 0$ and $x - 3 < -5 < 0$, so $(x-3)/(x+2) > 0$. If $-2 < x \leq 3$, then $x + 2 > 0$ and $x - 3 \leq 0$, so $(x-3)/(x+2) \leq 0$. Finally, if $x \geq 3$, then $x + 2 \geq 5 > 0$ and $x - 3 \geq 0$, so $(3x-1)/(x+2) \geq 0$. Thus $(3x+1)/(x+2) \leq 2$ iff $-2 < x \leq 3$. ■

Exercise 26. Solve the inequality $\dfrac{3x-5}{x-2} \leq 4$.

Exercise 27. Solve the inequality $\dfrac{x^2-6x+4}{2x^2-5x+2} \geq 1$.

Exercise 28. Solve the inequality $\dfrac{3x^2-4x-5}{x^2-4} \leq 2$.

Section 9. Absolute Value

9.1 Definition. Let a be a real number. Then the *absolute value of* a is denoted by $|a|$ and is defined by

$$|a| = \begin{cases} a & \text{if } a \geq 0; \\ -a & \text{if } a < 0. \end{cases}$$

For example, $|2| = 2$ and $|-3| = -(-3) = 3$. We remark that for each $a \in \mathbf{R}$, if $a \leq 0$, then $|a| = -a$. (Proof: Consider any $a \in \mathbf{R}$. Suppose $a \leq 0$. Then either $a < 0$ or $a = 0$. If $a < 0$, then $|a| = -a$ by definition. If $a = 0$, then $a \geq 0$, so $|a| = a$ by definition, so $|a| = 0 = -0 = -a$. Thus in either case, $|a| = -a$.)

9.2 Proposition. *Let* $a \in \mathbf{R}$. *Then:*

(a) $|a| \geq 0$.
(b) $|a| = 0$ *iff* $a = 0$.
(c) $|-a| = |a|$.
(d) $|a|^2 = a^2$.
(e) $-|a| \leq a \leq |a|$.

Proof. (a) Either $a \geq 0$ or $a < 0$. If $a \geq 0$, then $|a| = a$, so $|a| \geq 0$. If $a < 0$, then $|a| = -a$ and $-a > 0$, so $|a| > 0$, so $|a| \geq 0$. Thus in either case, $|a| \geq 0$.

(b) If $a = 0$, then $a \geq 0$, so $|a| = a$, so $|a| = 0$. We shall prove the converse by contraposition. Suppose $a \neq 0$. We wish to show that $|a| \neq 0$. Now either $a > 0$ or $a < 0$. If $a > 0$, then $|a| = a$, so $|a| > 0$, so $|a| \neq 0$. If $a < 0$, then $|a| = -a$, so $|a| > 0$, so $|a| \neq 0$. Thus in either case, $|a| \neq 0$.

(c) Either $a \geq 0$ or $a < 0$. If $a \geq 0$, then $|a| = a$, and $-a \leq 0$ so $|-a| = -(-a) = a$, so $|-a| = |a|$. If $a < 0$, then $|a| = -a$, and $-a > 0$ so $|-a| = -a$, so $|-a| = |a|$. Thus in either case, $|-a| = |a|$.

(d) Either $a \geq 0$ or $a < 0$. If $a \geq 0$, then $|a| = a$, so $|a|^2 = a^2$. If $a < 0$, then $|a| = -a$, so $|a|^2 = (-a)^2 = a^2$. Thus in either case, $|a|^2 = a^2$.

(e) Either $a \geq 0$ or $a < 0$. If $a \geq 0$, then $|a| = a$, so $-|a| = -a \leq 0 \leq a = |a|$, so $-|a| \leq a \leq |a|$. If $a < 0$, then $|a| = -a$, so $-|a| = a < 0 < -a = |a|$, so $-|a| \leq a \leq |a|$. Thus in either case, $-|a| \leq a \leq |a|$. ■

9.3 Proposition. *Let* $a, b \in \mathbf{R}$. *Then* $|ab| = |a||b|$.

Proof. Either $a \geq 0$ or $a < 0$.

Case 1. Suppose $a \geq 0$. Then $|a| = a$. Now either $b \geq 0$ or $b < 0$.

Subcase (a). Suppose $b \geq 0$. Then $|b| = b$. Also $ab \geq 0$, so $|ab| = ab = |a||b|$.

Subcase (b). Suppose $b < 0$. Then $|b| = -b$. Also $ab \leq 0$, so $|ab| = -ab = a(-b) = |a||b|$. (Remark: We cannot say that $ab < 0$, because a might be 0.)

Thus in either subcase, $|ab| = |a||b|$.

Case 2. Suppose $a < 0$. Then by an argument similar to the one in case 1, we can show that $|ab| = |a||b|$.

Thus in either case, $|ab| = |a||b|$. ■

Exercise 1. Let $a, b \in \mathbf{R}$. Suppose $b \neq 0$. Prove that:

(a) $|1/b| = 1/|b|$.
(b) $|a/b| = |a|/|b|$. (Combine part (a) with Proposition 9.3.)

9.4 Theorem. (The Triangle Inequality.) *Let* $x, y \in \mathbf{R}$. *Then* $|x + y| \leq |x| + |y|$.

Proof. We have $|x + y| \geq 0$ and $|x| + |y| \geq 0$, so by Exercise 9(b) in Section 8, it suffices to show that $|x+y|^2 \leq (|x|+|y|)^2$. Now $|x+y|^2 = (x+y)^2 = x^2+2xy+y^2 = |x|^2+2xy+|y|^2$ by Proposition 9.2(d). Next, $-|xy| \leq xy \leq |xy|$ by Proposition 9.2(e). In particular, $xy \leq |xy|$. But $|xy| = |x||y|$ by Proposition 9.3. Hence $xy \leq |x||y|$. Therefore $|x + y|^2 \leq |x|^2 + 2|x||y| + |y|^2 = (|x| + |y|)^2$. ■

Exercise 2. Let $x, y \in \mathbf{R}$. Prove that $|x + y| = |x| + |y|$ iff $xy \geq 0$.

Exercise 3. Let $a, b \in \mathbf{R}$. Prove that $|a - b| \leq |a| + |b|$.

If $a, b \in \mathbf{R}$, then $|b - a|$ is equal to the distance from a to b. For instance, the distance from -2 to 3 is 5 and $|3 - (-2)| = |5| = 5$. Of course the distance between two points does not depend on the order in which they are considered. The distance from 3 to -2 is also 5, and $|(-2) - 3| = |-5| = 5$. The next result tells us that if $a, b, c \in \mathbf{R}$, then the distance from a to c is less than or equal to the distance from a to b, plus the distance from b to c. This result is also often called the triangle inequality.

9.5 Proposition. *Let $a, b, c \in \mathbf{R}$. Then $|a - c| \leq |a - b| + |b - c|$.*

Proof. We use the common trick of subtracting something away and adding it back. We have $|a - c| = |a - b + b - c| = |(a - b) + (b - c)| \leq |a - b| + |b - c|$, where we have used Theorem 9.4 in the last step. ■

If A, B, C are points in the plane, then the distance from A to C is less than or equal to the distance from A to B, plus the distance from B to C. This is because the length of one side a triangle, say the side AC of the triangle ABC, is smaller than the sum of the lengths of the other two sides, namely the sides AB and BC. Proposition 9.5 is called the triangle inequality by analogy with this fact about triangles. Theorem 9.4 is called the triangle inequality because it essentially just an alternative version of Proposition 9.5. We have just seen how to deduce Proposition 9.5 from Theorem 9.4. But it is just as easy to deduce Theorem 9.4 from Proposition 9.5. Just let $a = x$, $b = 0$, and $c = -y$.

Exercise 4. Let $a, b, c \in \mathbf{R}$. Suppose $a \leq c$. Prove that $|a - c| = |a - b| + |b - c|$ iff $a \leq b \leq c$. Explain the geometrical meaning of this equivalence.

Exercise 5. Prove the following generalized triangle inequalities:

(a) For each $n \in \mathbf{N}$, for each $x_1, \ldots, x_n \in \mathbf{R}$, $|x_1 + \cdots + x_n| \leq |x_1| + \cdots + |x_n|$. (Use induction and apply Theorem 9.4.)

(b) For each $n \in \mathbf{N}$, for each $a_1, \ldots, a_n, a_{n+1} \in \mathbf{R}$, $|a_1 - a_{n+1}| \leq |a_1 - a_2| + |a_2 - a_3| + \cdots + |a_n - a_{n+1}|$. (Apply part (a).)

9.6 Proposition. *Let $a, b \in \mathbf{R}$. Then $|a| \leq b$ iff $-b \leq a \leq b$.*

Proof. ($\Rightarrow$) Suppose $|a| \leq b$. Then $-b \leq -|a|$. But by Proposition 9.2(e), $-|a| \leq a \leq |a|$. Hence $-b \leq a \leq b$.

($\Leftarrow$) Conversely, suppose $-b \leq a \leq b$. Now either $a \geq 0$ or $a < 0$. If $a \geq 0$, then $|a| = a$, so $|a| \leq b$. If $a < 0$, then $|a| = -a$, so $a = -|a|$, so $-b \leq -|a|$, so $|a| \leq b$. Thus in either case, $|a| \leq b$. ■

Exercise 6.

(a) Let $a, b \in \mathbf{R}$. Prove that $|a| < b$ iff $-b < a < b$.

(b) Let $x, c, \varepsilon \in \mathbf{R}$. Prove that $|x - c| < \varepsilon$ iff $c - \varepsilon < x < c + \varepsilon$. Also, draw a picture to illustrate the geometrical meaning of this result in the case where $\varepsilon > 0$.

(c) Let $x, c, \varepsilon \in \mathbf{R}$ again. When is $|x - c| \geq \varepsilon$? Prove your answer. Also, draw a picture to illustrate the geometrical meaning of your answer in the case where $\varepsilon > 0$.

The next result tells us that the distance between $|a|$ and $|b|$ is less than or equal to the distance between a and b.

9.7 Proposition. *Let $a, b \in \mathbf{R}$. Then $\big||a| - |b|\big| \leq |a - b|$.*

Proof. We have $a = (a - b) + b$, so $|a| \leq |a - b| + |b|$ by Theorem 9.4. Hence $|a| - |b| \leq |a - b|$. Similarly, $|b| - |a| \leq |b - a|$. But $|b - a| = |a - b|$. Hence $|b| - |a| \leq |a - b|$, so $-|a - b| \leq |a| - |b|$. Thus $-|a - b| \leq |a| - |b| \leq |a - b|$. Therefore $\big||a| - |b|\big| \leq |a - b|$ by Proposition 9.6. ■

Exercise 7. Let $a, b \in \mathbf{R}$. Prove that $\big||a| - |b|\big| = |a - b|$ iff $ab \geq 0$.

Exercise 8. The statement of Theorem 9.4 (the triangle inequality) does not involve multiplication but the proof that we gave did involve multiplication. Give a proof of Theorem 9.4 that does not involve multiplication. (Use Proposition 9.6. Note that our proof of Proposition 9.6 did not depend on Theorem 9.4.)

9.8 Definition. Let $a, b \in \mathbf{R}$. Then the *minimum of a and b* is denoted by $\min\{a, b\}$ and is defined by

$$\min\{a, b\} = \begin{cases} a & \text{if } a < b; \\ b & \text{if } a \geq b. \end{cases}$$

For example, $\min\{3,7\}=3$, $\min\{3,-7\}=-7$, and $\min\{6,6\}=6$. We remark that for all $a,b\in\mathbf{R}$, if $a\le b$, then $\min\{a,b\}=a$. (Proof: Consider any $a,b\in\mathbf{R}$. Suppose $a\le b$. Then either $a<b$ or $a=b$. If $a<b$, then $\min\{a,b\}=a$, by definition. If $a=b$, then $a\ge b$, so $\min\{a,b\}=b=a$.)

Exercise 9. Let $a,b\in\mathbf{R}$. Prove that $\min\{a,b\}=\frac{1}{2}(a+b-|a-b|)$.

Exercise 10. Formulate a definition for *the maximum of a and b*, where $a,b\in\mathbf{R}$. Then prove that for each $a,b\in\mathbf{R}$,

$$\max\{a,b\}=\tfrac{1}{2}(a+b+|a-b|),$$

where of course $\max\{a,b\}$ denotes the maximum of a and b.

Exercise 11. In Exercise 9 and Exercise 10, we saw that the minimum and maximum can be expressed in terms of the absolute value. Prove that the absolute value can be expressed in terms of the maximum or minimum, in the sense that for each $a\in\mathbf{R}$, $|a|=\max\{a,-a\}=-\min\{a,-a\}$.

Exercise 12. Prove that each of the minimum and maximum can be expressed in terms of the other, in the sense that for each $a,b\in\mathbf{R}$, $\min\{a,b\}=-\max\{-a,-b\}$ and $\max\{a,b\}=-\min\{-a,-b\}$.

9.9 Example. Solve the inequality $|x+2|\ge|2x-3|$.

Solution. Note that $2x-3=2(x-3/2)$. Now either $x<-2$ or $-2\le x<3/2$ or $x\ge 3/2$.

Case 1. Suppose $x<-2$. Then $x+2<0$ and $x-3/2<0$, so $|x+2|=-x-2$ and $|2x-3|=3-2x$. Hence $|x+2|\ge|2x-3|$ iff $-x-2\ge 3-2x$ iff $x\ge 5$. Thus the inequality $|x+2|\ge|2x-3|$ is always false in this case.

Case 2. Suppose $-2\le x<3/2$. Then $x+2\ge 0$ and $x-3/2<0$ so $|x+2|=x+2$ and $|2x-3|=3-2x$. Hence $|x+2|\ge|2x-3|$ iff $x+2\ge 3-2x$ iff $3x\ge 1$ iff $x\ge 1/3$. Thus in this case, $|x+2|\ge|2x-3|$ iff $1/3\le x<3/2$.

Case 3. Suppose $x\ge 3/2$. Then $x+2\ge 0$ and $x-3/2\ge 0$, so $|x+2|=x+2$ and $|2x-3|=2x-3$. Hence $|x+2|\ge|2x-3|$ iff $x+2\ge 2x-3$ iff $5\ge x$. Thus in this case, $|x+2|\ge|2x-3|$ iff $3/2\le x\le 5$.

Therefore for each $x\in\mathbf{R}$, $|x+2|\ge|2x-3|$ iff $1/3\le x\le 5$. ■

Exercise 13. Solve the inequality $|x-3|+|3x+2|>4$.

Exercise 14. Solve the inequality $|1-x|+|x-5|<4$. (This can be done by a case analysis as in Example 9.9, but if you use the right one of the results proved in this section, you should be able to do it in about one line. Think about the geometrical meaning of the inequality.)

9.10 Example. Solve the inequality $\dfrac{|2x-1|}{x+1}\le 2$.

Solution. Unlike what happened in Example 8.30, it would not be simpler here to subtract 2 from both sides. Instead, we shall multiply both sides by $x+1$. Of course, when we do this, we must consider whether $x+1$ is positive or negative, because the direction of the resulting inequality will depend on this. Consider any $x\in\mathbf{R}$. Note that $2x-1=2(x-1/2)$, so $2x-1\ge 0$ iff $x\ge 1/2$. Note also that $x+1=0$ iff $x=-1$. Now either $x<-1$ or $x=-1$ or $-1<x<1/2$ or $1/2\le x$.

Case 0. Suppose $x=-1$. Then $|2x-1|/(x+1)$ is undefined, so the inequality $|2x-1|/(x+1)\le 2$ is false.

Case 1. Suppose $x<-1$. Then $x+1<0$, so $|2x-1|/(x+1)\le 0$ (since $|2x-1|\ge 0$), so the inequality $|2x-1|/(x+1)\le 2$ is always true in this case.

Case 2. Suppose $-1<x<1/2$. Then $x+1>0$, so $|2x-1|/(x+1)\le 2$ iff $|2x-1|\le 2x+2$. Also, $x-1/2<0$, so $2x-1<0$, so $|2x-1|=1-2x$. Hence $|2x-1|/(x+1)\le 2$ iff $1-2x\le 2x+2$ iff $1-2\le 4x$ iff $-1/4\le x$. Thus in this case, $|2x-1|/(x+1)\le 2$ iff $-1/4\le x<1/2$.

Case 3. Suppose $1/2\le x$. Then $x+1>0$ and $2x-1\ge 0$, so $|2x-1|/(x+1)\le 2$ iff $2x-1\le 2x+2$ iff $-1\le 2$. Thus the inequality $|2x-1|/(x+1)\le 2$ is always true in this case.

Therefore for each $x\in\mathbf{R}$, $|2x-1|/(x+1)\le 2$ iff $x<-1$ or $-1/4\le x$. ■

Exercise 15. Solve the inequality $\dfrac{|3x-2|}{2x-3}\ge 5$.

Chapter 3

Sets, Functions, and Relations

Section 10. Sets

In earlier sections, we have made a small amount of informal use of sets. In this section, we shall take a closer look at sets. We begin by stating that a *set* is a collection of objects, considered as an object in its own right.

As we mentioned near the beginning of Section 3, if A is a set and x is an object, we write $x \in A$ to mean x is one of the objects in the collection A, and we write $x \notin A$ to mean x is not in the collection A. The notation $x \in A$ may be read "x is an element of A" or "x belongs to A" or "x is a member of A" or "x is in A."

Occasionally the notation $A \ni x$ is used to mean the same thing as $x \in A$. The notation $A \ni x$ may be read "A owns x."

Denoting a Set by Listing Its Elements.

Sometimes we denote a set by listing its elements between braces. For instance, $\{\,2, 3, 5\,\}$ is the set whose elements are the numbers 2, 3, and 5. To give another example, $\{\,2\,\}$ is the set whose only element is the number 2. Let us emphasize that 2 is not the same thing as $\{\,2\,\}$. The difference between them is like the difference a potato and a sack with a potato in it. By the way, the notation $\{\,2\,\}$ is read "singleton 2."

There is another important way to denote sets. It is called set-builder notation. We shall discuss it shortly. Before we do that, let us discuss the concept of equality for sets.

Sets Having the Same Elements Are Equal.

It is more or less inherent in the notion of "set" that a set is completely determined by saying which objects belong to it. Thus if A and B are sets that have the same elements (in other words, if for each x, we have $x \in A$ iff $x \in B$), then $A = B$. It follows that the order in which the elements of a set are listed does not matter. For example, $\{\,1, 2\,\} = \{\,2, 1\,\}$ because for each x, we have $x \in \{\,1, 2\,\}$ iff $x = 1$ or $x = 2$ iff $x = 2$ or $x = 1$ iff $x \in \{\,2, 1\,\}$. (Remember that an "or" statement is true exactly when at least one of the parts is true.) Likewise, repetitions do not count in the description of a set. For instance, $\{\,3, 3\,\} = \{\,3\,\}$ because for each x, we have $x \in \{\,3, 3\,\}$ iff $x = 3$ or $x = 3$ iff $x = 3$ iff $x \in \{\,3\,\}$.

Equal Sets Have the Same Elements.

As we have just discussed, sets that have the same elements are equal. Now since equals may be replaced by equals, it is also true that equal sets have the same elements (in other words, for all sets A and B, if $A = B$, then for each x, we have $x \in A$ iff $x \in B$) and that equal objects are elements of the same sets (in other words, for all x and y, if $x = y$, then for each set A, we have $x \in A$ iff $y \in A$).

Set-Builder Notation.

Now let us discuss *set-builder notation*, which is the second main way to denote sets. In set-builder notation, we describe a set in terms of a property that is characteristic of the elements of the set. Thus if S is a set whose elements are precisely the objects x that have a certain property $P(x)$, then we may write $\{\, x : P(x) \,\}$ for the set S. The notation $\{\, x : P(x) \,\}$ is read "the set of all x such that $P(x)$." For example, the notation $\{\, x : x \text{ is prime and } x \leq 6 \,\}$ is read "the set of all x such that x is prime and $x \leq 6$." We have

$$\{\, x : x \text{ is prime and } x \leq 6 \,\} = \{\, 2, 3, 5 \,\}.$$

We also have

$$\{\, y : y \text{ is prime and } y \leq 6 \,\} = \{\, 2, 3, 5 \,\}.$$

This illustrates the fact that in the set-builder notation $\{\, x : P(x) \,\}$, the variable x is a dummy variable. Similarly, in the following example, the variables a and b are both dummy variables:

$$\begin{aligned}\{\, a \in \mathbf{N} : a \text{ is even} \,\} &= \text{the set of even natural numbers} \\ &= \{\, 2, 4, 6, 8, \ldots \,\} = \{\, b \in \mathbf{N} : b \text{ is even} \,\}.\end{aligned}$$

Here we have used a variation on set-builder notation, namely: $\{\, x \in A : P(x) \,\}$ is another way to write $\{\, x : x \in A \text{ and } P(x) \,\}$. (For instance, $\{\, a \in \mathbf{N} : a \text{ is even} \,\} = \{\, a : a \in \mathbf{N} \text{ and } a \text{ is even} \,\}$.) The notation $\{\, x \in A : P(x) \,\}$ is read "the set of all x in A such that $P(x)$." For example, the notation $\{\, a \in \mathbf{N} : a \text{ is even} \,\}$ is read "the set of all a in $\mathbf{N}$ such that a is even."

By the way, to be completely honest, we should admit that a notation such as $\{\, 2, 4, 6, 8, \ldots \,\}$ must be considered informal. Its interpretation depends on our making a reasonable assumption about the pattern it suggests. It is not our purpose here to be completely formal. Strict formality before we are ready for it can interfere with understanding. But it is good to be conscious of when we are being informal.

Here is another variation on set-builder notation: if $f(x)$ denotes an object that depends on x and $P(x)$ is a property of x, then

$$\{\, f(x) : P(x) \,\} \text{ denotes } \{\, y : y = f(x) \text{ for some } x \text{ such that } P(x) \,\}.$$

The notation $\{\, f(x) : P(x) \,\}$ is read "the set of all $f(x)$ such that $P(x)$." For instance,

$$\begin{aligned}\{\, 2x : x \in \mathbf{N} \,\} &= \{\, y : y = 2x \text{ for some } x \in \mathbf{N} \,\} \\ &= \{\, 2, 4, 6, 8, \ldots \,\}.\end{aligned}$$

It follows that $\{\, 2x : x \in \mathbf{N} \,\} = \{\, x \in \mathbf{N} : x \text{ is even} \,\}$. To understand the preceding sentence properly, it is important to realize that the x in the notation $\{\, 2x : x \in \mathbf{N} \,\}$ is a dummy variable, as is the x in the notation $\{\, x \in \mathbf{N} : x \text{ is even} \,\}$, so that the former x has nothing to do with the latter x. Thus it does not matter whether we write $\{\, 2x : x \in \mathbf{N} \,\} = \{\, x \in \mathbf{N} : x \text{ is even} \,\}$, or whether we write $\{\, 2a : a \in \mathbf{N} \,\} = \{\, b \in \mathbf{N} : b \text{ is even} \,\}$; they both mean the same thing.

By the way, $\{\, y : y = 2x \text{ for each } x \in \mathbf{N} \,\}$ is not equal to $\{\, 2, 4, 6, 8, \ldots \,\}$. Rather, the set

$$\{\, y : y = 2x \text{ for each } x \in \mathbf{N} \,\}$$

is empty. The reason is that if $y = 2x$ for each $x \in \mathbf{N}$, then for instance, $y = 2 \cdot 1 = 2$ and $y = 2 \cdot 2 = 4$, which is impossible.

Summary of Ways to Denote Sets.

Here is an example to illustrate the various ways we have discussed to denote sets:

$$\begin{aligned}\left\{\, x^2 : x \in \{\, -1, 0, 1 \,\} \,\right\} &= \left\{\, (-1)^2, 0^2, 1^2 \,\right\} \\ &= \{\, 1, 0, 1 \,\} = \{\, 0, 1 \,\} = \{\, x \in \boldsymbol{\omega} : x \leq 1 \,\}.\end{aligned}$$

Exercise 1. Which of the sets A, B, C, D, and E below are the same?

$$\begin{aligned}&A = \{\, 3 \,\}, \quad B = \{\, 2, 4 \,\}, \quad C = \{\, x : x \text{ is prime, } x \text{ is odd, and } x < 5 \,\}, \\ &D = \{\, x - 1 : x \text{ is prime, } x \text{ is odd, and } x \leq 5 \,\}, \quad E = \left\{\, x^2 + 2 : x \in \{\, -1, 1 \,\} \,\right\}.\end{aligned}$$

Also, how many different sets are named here?

The Number of Elements in Some Simple Sets.

To better understand how set notation works, let us consider how many elements the set $\{a, b\}$ has. It is tempting to say that it has two elements, namely a and b. However, the correct answer is that $\{a, b\}$ has two elements if $a \neq b$, but only one if $a = b$. The set $\{a, b\}$ is not the set whose elements are the letters a and b; rather, it is the set whose elements are the objects that the variables a and b stand for. Different variables may stand for the same object. For instance, at the start of a discussion, we might choose to use two different variables because we are not sure whether the objects they stand for are the same or different. Then in the course of the discussion, it might turn out that actually they are the same.

10.1 Remark. Let a, b, and c be objects.

To say that $a \neq b \neq c$ means that $a \neq b$ and $b \neq c$. Note that from this it does not follow that $a \neq c$. (For instance, $1 \neq 2 \neq 3^2 - 8$ but $1 = 3^2 - 8$.) If you wish to express in detail the idea that a, b, and c are distinct, you need to say that $a \neq b$, $a \neq c$, and $b \neq c$.

Note also that if $a = b$, it does not follow that $b \neq c$. If you wish to express the idea that a and b are the same but c is distinct from them, you need to say that $a = b$ and $b \neq c$.

Exercise 2. How many elements does the set $\{a, b, c\}$ have? Answer as completely and precisely as possible. Remark 10.1 should alert you to some of the things you need to pay attention to.

Sets as Elements of other Sets.

Recall that we said that a set is a collection of objects, *considered as an object in its own right.* Since sets are objects, it is natural that they can be elements of other sets. For instance, if $A = \{1, 2, \{3, 4\}\}$, then A has three elements, namely 1, 2, and the set $\{3, 4\}$. Note that $3 \notin A$ and $4 \notin A$. Instead, 3 is an element of an element of A. Similarly for 4. Here is an example of a set with one element, that element being an infinite set:

$$\{\{1, 2, 3, \dots\}\} = \{\mathbf{N}\}.$$

Now here is an example of a set with infinitely many elements, each element being a set with one element:

$$\{\{1\}, \{2\}, \{3\}, \dots\}.$$

And here is an example of a set with infinitely many elements, each element being a set that itself has infinitely many elements:

$$\{\{1, 2, 3, \dots\}, \{2, 4, 6, \dots\}, \{3, 6, 9, \dots\}, \dots\}.$$

Exercise 3. Use set-builder notation to describe the sets in the last two examples in the previous paragraph. (Of course, you will need to make reasonable assumptions about the patterns in those examples.)

10.2 Remark. It is common to use lower case letters such as $a, b, c, \dots$ to denote objects, upper case letters such as $A, B, C, \dots$ to denote sets of objects, and upper case script letters such as $\mathscr{A}, \mathscr{B}, \mathscr{C}, \dots$ to denote sets of sets.[1] For instance, in a particular situation, we might consider a set of objects $S = \{a, b, c\}$, some other sets of these objects, say $U = \{a, b\}$, $V = \{a, c\}$ and $W = \{b, c\}$, and the set of sets $\mathscr{M} = \{U, V, W\}$. However, this notational convention is not intended to be adhered to rigidly, but rather only when it is helpful. After all, sets are objects too, so in some contexts it may be quite natural to use a lower case letter such as x to denote a set.

[1] When reading script letters aloud, it is customary to say that they are script letters. For instance, $\mathscr{A}$ would be read "script ay."

The Empty Set.

The empty set is the set that has no elements. It is usually denoted by $\emptyset$. (Occasionally, it is denoted by $\{\ \}$.) By the way, the symbol $\emptyset$ is not a Greek letter "phi." It is an upper case "oh" with a slash through it, one of the letters of the Scandinavian alphabet.[2] (See the difference: $\emptyset$ is the empty set; ϕ is a Greek letter "phi.")

The reason why there should be an empty set is that given a property $P(x)$, if there are no values of x for which $P(x)$ is true, then $\{\, x : P(x) \,\}$ is the empty set. For instance,

$$\{\, x : x \text{ is prime, } x \text{ is even, and } x > 2 \,\} = \emptyset.$$

There is only one empty set. To see this, suppose $\emptyset'$ is another set with no elements. Then for each object x, the sentence $x \in \emptyset$ and the sentence $x \in \emptyset'$ are both false, so the sentence $x \in \emptyset \Leftrightarrow x \in \emptyset'$ is true. Hence $\emptyset$ and $\emptyset'$ have the same elements (namely, none), so $\emptyset = \emptyset'$.

The preceding paragraph reveals the usual way to show that a given set A is equal to the empty set. Namely, show that for each object x, we have $x \notin A$. If we show this, then it follows that for each object x, the sentence $x \in A$ and the sentence $x \in \emptyset$ are both false, so the sentence $x \in A \Leftrightarrow x \in \emptyset$ is true. Hence A and $\emptyset$ have the same elements (namely, none), so $A = \emptyset$.

By the way, the empty set is even more empty than empty space. Empty space is empty only in the sense that it contains no material objects. But in empty space, we can conceive of regions, surfaces, curves, and points. These are not material objects. They are conceptual objects. But the empty set is truly empty. It does not even have any points in it.

Exercise 4. Which of the following set notations denote the empty set?

(a) $\{\, z : z \text{ is a horse and } z \text{ has 6 legs} \,\}$.

(b) $\{\, a \in \mathbf{R} : a^2 + 2a + 2 = 0 \,\}$.

(c) $\{\, n \in \mathbf{N} : n^2 + n + 11 \text{ is not prime} \,\}$.

Subsets.

10.3 Definition. Let A and B be sets. To say that A *is a subset of* B (denoted $A \subseteq B$) means that for each x, if $x \in A$, then $x \in B$.

In other words, A is a subset of B when each element of A is an element of B. For example, $\{\, 3, 5 \,\}$ and $\{\, 2, 3, 5 \,\}$ are subsets of $\{\, 2, 3, 5 \,\}$. For another example, $\{\, 2, \{\, 3, 5 \,\} \,\}$ is not a subset of $\{\, 2, 3, 5 \,\}$, because $\{\, 3, 5 \,\}$ is not an element of $\{\, 2, 3, 5 \,\}$. By the way, the relation $\subseteq$ is usually called *set inclusion*.

To say that A *is a proper subset of* B means that $A \subseteq B$ and $A \neq B$. For example, $\{\, 3, 5 \,\}$ is a proper subset of $\{\, 2, 3, 5 \,\}$.

By analogy with the notations $\leq$ and $<$, since we write $A \subseteq B$ to mean A is a subset of B, it is tempting to write $A \subset B$ to mean A is a proper subset of B. Unfortunately, this convention is followed in very few books. There is no widely accepted notation that means A is a proper subset of B. Worse than that, in most books, the notation $A \subset B$ is used instead of $A \subseteq B$ to mean A is a subset of B. I have chosen to use the notation $A \subseteq B$ to mean A is a subset of B in part because I think it is better in handwritten work, since it is less likely to look like "$A\ C\ B$." But you should be aware that usually $A \subset B$ means the same thing as $A \subseteq B$.

Occasionally the notation $B \supseteq A$ (or $B \supset A$) is used to mean the same thing as $A \subseteq B$. The notation $B \supseteq A$ may be read "B is a superset of A." To say that B *is a proper superset of* A means that $B \supseteq A$ and $B \neq A$.

---

[2] This symbol for the empty set was introduced in one of the early textbooks on set theory, written in the 1930's by a group of distinguished French mathematicians who published under the pseudonym *Nicolas Bourbaki*. One of these mathematicians, André Weil, revealed in his autobiography that much later, his own part in this writing "earned me the respect of my daughter Nicolette, when she learned the symbol $\emptyset$ for the empty set at school and I told her that I had been personally responsible for its adoption. The symbol came from the Norwegian alphabet, with which I alone among the Bourbaki group was familiar."

10.4 Proposition. *Set inclusion is reflexive, antisymmetric, and transitive. In other words,*

(a) *For each set A, we have $A \subseteq A$.* (Reflexivity.)

(b) *For all sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.* (Antisymmetry.)

(c) *For all sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.* (Transitivity.)

Proof. (a) Consider any set A. Then obviously, for each x, if $x \in A$, then $x \in A$. In other words, $A \subseteq A$.

(b) Consider any sets A and B. Suppose $A \subseteq B$ and $B \subseteq A$. If $x \in A$, then $x \in B$, because $A \subseteq B$. Conversely, if $x \in B$, then $x \in A$, because $B \subseteq A$. Thus for each x, we have $x \in A$ iff $x \in B$. In other words, A and B have the same elements. Hence $A = B$.

(c) Consider any sets A, B, and C. Suppose $A \subseteq B$ and $B \subseteq C$. Let $x \in A$. Then $x \in B$, because $A \subseteq B$. But then $x \in C$, because $B \subseteq C$. Thus for each x, if $x \in A$, then $x \in C$. In other words, $A \subseteq C$. ■

10.5 Proposition. *For each set A, we have $\emptyset \subseteq A$.*

Proof. Consider any set A. We wish to show that for each x, if $x \in \emptyset$, then $x \in A$. Consider any object x. Then the conditional sentence

$$\text{if } x \in \emptyset, \text{ then } x \in A$$

is true because the antecedent in it, namely $x \in \emptyset$, is false. Since x is arbitrary, it follows that for each x, if $x \in \emptyset$, then $x \in A$. In other words, $\emptyset \subseteq A$. ■

10.6 Remark. The idea of the preceding proof may be briefly expressed as follows: every element of $\emptyset$ is an element of A because $\emptyset$ has no elements. This is a special case of the following general fact: If $P(x)$ is any statement about x, then the universal sentence $(\forall x \in \emptyset)P(x)$ is true, because $P(x)$ is true for every value of x that is an element of $\emptyset$, since $\emptyset$ has no elements. We describe this situation by saying that the universal sentence $(\forall x \in \emptyset)P(x)$ is vacuously true, as we already mentioned in Section 3.

Exercise 5. Let A be a set such that for each set B, we have $A \subseteq B$. Show that $A = \emptyset$.

The Difference between Elements and Subsets.

It is important to realize that $\in$ and $\subseteq$ are different notions. For instance, the elements of the set $\{1, 2\}$ are the numbers 1 and 2 but the subsets of $\{1, 2\}$ are the sets $\emptyset$, $\{1\}$, $\{2\}$, and $\{1, 2\}$.

In general, neither of the sentences "$A \in B$" and "$A \subseteq B$" implies the other.

10.7 Example. Let $A = \emptyset$ and let $B = \emptyset$. Then $A \subseteq B$, by Proposition 10.5, but $A \notin B$, because B has no elements.

10.8 Example. Let $A = \{\emptyset\}$ and let $B = \{\{\emptyset\}\}$. Then $A \in B$ but $A \not\subseteq B$. That $A \in B$ is obvious. To see that $A \not\subseteq B$, let us suppose that $A \subseteq B$ and let us derive a contradiction. Since $\emptyset \in A$ and $A \subseteq B$, we have $\emptyset \in B$. But the only element of B is $\{\emptyset\}$. Hence $\emptyset = \{\emptyset\}$. Thus $\emptyset$ and $\{\emptyset\}$ have the same elements. But $\emptyset$ has no elements, whereas $\{\emptyset\}$ has an element (namely $\emptyset$). Hence $\emptyset$ and $\{\emptyset\}$ do not have the same elements. Thus we have reached a contradiction. Hence A must not be a subset of B after all.

It is worth noticing that in this example, our proof that $A \not\subseteq B$ was completely from first principles. This reflects the profoundly fundamental nature of set theory.

Exercise 6.

(a) Find a set A and a set B such that $A \notin B$ and $A \not\subseteq B$.

(b) Find a set A and a set B such that $A \in B$ and $A \subseteq B$.

(Hint for both parts: Reflect on what we know about the empty set.)

Set Operations: Unions, Intersections, and Relative Complements.

10.9 Definition. Let A and B be sets. The *union of A and B* (denoted $A \cup B$) is the set of all things that belong to at least one of the sets A and B; in other words, $A \cup B = \{\, x : x \in A \text{ or } x \in B \,\}$.

10.10 Definition. Let A and B be sets. The *intersection of A and B* (denoted $A \cap B$) is the set of all things that belong to both of the sets A and B; in other words, $A \cap B = \{\, x : x \in A \text{ and } x \in B \,\}$.

10.11 Definition. Let A and B be sets. The *relative complement of B in A* (denoted $A \setminus B$) is the set of all things that belong to A but not to B; in other words, $A \setminus B = \{\, x : x \in A \text{ and } x \notin B \,\}$.

10.12 Remark. It might seem natural to try to define the "absolute complement" of a set A to be $B = \{\, x : x \notin A \,\}$, the set of all things that do not belong to the set A. But if we could do this, then $U = A \cup B$ would be the set of all things. Everything would be an element of U. In particular, U would belong to itself, which is strange, although perhaps not impossible. But as we shall see later, the notion of a set to which every object belongs leads to even more serious difficulties. It turns out that there is no such thing as the set of all objects. For this reason, the absolute complement of a set is not defined. If A is a set, then there is no such thing as the set $B = \{\, x : x \notin A \,\}$. Only the relative complement of a set with respect to another set is defined.

10.13 Remark. The short ways to read $A \cup B$, $A \cap B$, and $A \setminus B$ are "A union B," "A intersect B," and "A less B" respectively.

10.14 Example. Let $A = \{\, 2, 3, 5, 6 \,\}$ and $B = \{\, 4, 5, 8 \,\}$. Then $A \cup B = \{\, 2, 3, 4, 5, 6, 8 \,\}$, $A \cap B = \{\, 5 \,\}$, $A \setminus B = \{\, 2, 3, 6 \,\}$, and $B \setminus A = \{\, 4, 8 \,\}$.

Exercise 7. Let $A = \big\{\, 1, \{\, 4, 7 \,\}, 9 \,\big\}$ and $B = \big\{\, \{\, 1, 4 \,\}, 7, 9 \,\big\}$. Find $A \cup B$, $A \cap B$, $A \setminus B$, and $B \setminus A$.

10.15 Remark. $A \cup B$ should not be read "A or B." One reason is that this could cause you to misunderstand a sentence such as $x \notin A \cup B$. (I have often seen students read $x \notin A \cup B$ as "x is not in A or B," and then mistakenly construe this to mean "x is not in A or x is not in B". In fact, as we shall explain shortly, the sentence $x \notin A \cup B$ is logically equivalent to "x is not in A and x is not in B.".) Likewise, $A \cap B$ should not be read "A and B." Symbols for sets, such as "A" and "B" above, denote objects and so are nouns, not sentences. The logical connectives "and" and "or" should connect sentences, not nouns.

Similarly, the notations "$A \cup B$", "$A \cap B$", and "$A \setminus B$" are nouns, not sentences. Hence, for instance, it would be nonsense to write something like "$A \cup B$ iff $x \in A$ or $x \in B$." It would be correct instead to write "$x \in A \cup B$ iff $x \in A$ or $x \in B$."

Connections between Set Inclusion and Set Operations.

As we have already mentioned, the relation $\subseteq$ is usually called *set inclusion*. Next we shall consider some connections between this relation and the set operations $\cup$, $\cap$, and $\setminus$.

10.16 Example. Let A and B be sets. Show that $A \subseteq A \cup B$ and $B \subseteq A \cup B$.

Solution. We shall write two versions of the proof. The first version will include several extra sentences that would not normally be written but that we have included to illustrate what you should read "between the lines" when you study even a simple proof such as this, or what should be in the back of your mind when you write a proof like this. The second version of the proof will be written in the way you should normally write it.

Here is the first version of the proof. Recall that an "or" statement is true when at least one of the parts is true. Suppose $x \in A$. Then it is true that $x \in A$ or $x \in B$. In other words, $x \in A \cup B$. Thus if $x \in A$, then $x \in A \cup B$. Now x is arbitrary, because the assumption that $x \in A$ has been discharged. Hence for each x, if $x \in A$, then $x \in A \cup B$. In other words, $A \subseteq A \cup B$. Similarly, $B \subseteq A \cup B$.

Now here is the second version of the proof, to illustrate how you should normally write such a proof. Let $x \in A$. Then $x \in A$ or $x \in B$. Hence $x \in A \cup B$. Thus $A \subseteq A \cup B$. Similarly, $B \subseteq A \cup B$. ■

Exercise 8. Let A and B be sets. Show that $A \cap B \subseteq A$ and $A \cap B \subseteq B$.

10.17 Example. Let A, B, and C be sets. Suppose $A \subseteq C$ and $B \subseteq C$. Show that $A \cup B \subseteq C$.

Solution. Let $x \in A \cup B$. Then $x \in A$ or $x \in B$. In the case where $x \in A$, we have $x \in C$, because $A \subseteq C$. In the case where $x \in B$, we have $x \in C$, because $B \subseteq C$. Thus in either case, $x \in C$. Hence $A \cup B \subseteq C$. ■

Exercise 9. Let A, B, and C be sets. Suppose $C \subseteq A$ and $C \subseteq B$. Show that $C \subseteq A \cap B$.

10.18 Example. Let A and B be sets. Show that $A \subseteq B$ iff $A \cup B = B$.

Solution. Suppose $A \subseteq B$. Under this assumption, we wish to show that $A \cup B = B$. We know that $B \subseteq A \cup B$, by Example 10.16. Next, $A \subseteq B$ by assumption and $B \subseteq B$ by the reflexivity of set inclusion. Hence $A \cup B \subseteq B$, by Example 10.17. Thus $A \cup B \subseteq B$ and $B \subseteq A \cup B$, so $A \cup B = B$.

Conversely, suppose $A \cup B = B$. Now by Example 10.16, we have $A \subseteq A \cup B$. Since $A \subseteq A \cup B$ and $A \cup B = B$, we have $A \subseteq B$. ■

Exercise 10. Let A and B be sets. Show that $A \subseteq B$ iff $A \cap B = A$.

Exercise 11. Let A and B be sets. Show that $A \subseteq B$ iff $A \setminus B = \emptyset$.

Basic Algebra of Set Operations.

10.19 Proposition. *Let A and B be sets and let x be any object. Then:*
(a) *$x \notin A \cup B$ iff $x \notin A$ and $x \notin B$.*
(b) *$x \notin A \cap B$ iff $x \notin A$ or $x \notin B$.*

Proof. (a) Recall that by one of De Morgan's laws from propositional calculus, $\neg(P \vee Q)$ is logically equivalent to $\neg P \wedge \neg Q$. Bearing this in mind, we have

$$\begin{array}{ll} & x \notin A \cup B \\ \text{iff} & \text{it is not the case that } x \in A \cup B \\ \text{iff} & \text{it is not the case that } x \in A \text{ or } x \in B \\ \text{iff} & x \notin A \text{ and } x \notin B. \end{array}$$

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

Exercise 12. Prove Proposition 10.19(b).

Exercise 13. Let A and B be sets and let x be any object. Prove that $x \notin A \setminus B$ iff $x \notin A$ or $x \in B$.

10.20 Theorem. (De Morgan's Laws for Sets.) *Let S, A, and B be sets. Then:*
(a) *$S \setminus (A \cup B) = (S \setminus A) \cap (S \setminus B)$.*
(b) *$S \setminus (A \cap B) = (S \setminus A) \cup (S \setminus B)$.*

Proof. (a) For each object x, we have

$$\begin{array}{ll} & x \in S \setminus (A \cup B) \\ \text{iff} & x \in S \text{ and } x \notin A \cup B \\ \text{iff} & x \in S \text{ and } (x \notin A \text{ and } x \notin B) \qquad \text{(by Proposition 10.19(a))} \\ \text{iff} & (x \in S \text{ and } x \notin A) \text{ and } (x \in S \text{ and } x \notin B) \\ \text{iff} & x \in S \setminus A \text{ and } x \in S \setminus B \\ \text{iff} & x \in (S \setminus A) \cap (S \setminus B). \end{array}$$

Thus the set $S \setminus (A \cup B)$ has the same elements as the set $(S \setminus A) \cap (S \setminus B)$, so these two sets are equal. This proves (a). The proof of (b) is left as an exercise. ■

Exercise 14. Prove Theorem 10.20(b).

Exercise 15. Let S, A, and B be sets.
(a) Prove that $S \setminus (A \setminus B) = (S \setminus A) \cup (S \cap B)$.
(b) Deduce that $A \setminus (A \setminus B) = A \cap B$.

10.21 Theorem. (The Distributive Laws for Unions and Intersections.) *Let S, A, and B be sets. Then:*

(a) $S \cap (A \cup B) = (S \cap A) \cup (S \cap B)$.

(b) $S \cup (A \cap B) = (S \cup A) \cap (S \cup B)$.

Proof. (a) Recall that by one of the distributive laws for propositional calculus, $P \wedge (Q \vee R)$ is logically equivalent to $(P \wedge Q) \vee (P \wedge R)$. Bearing this in mind, for each object x, we have

$$\begin{array}{ll} & x \in S \cap (A \cup B) \\ \text{iff} & x \in S \text{ and } x \in A \cup B \\ \text{iff} & x \in S \text{ and } (x \in A \text{ or } x \in B) \\ \text{iff} & (x \in S \text{ and } x \in A) \text{ or } (x \in S \text{ and } x \in B) \\ \text{iff} & x \in S \cap A \text{ or } x \in S \cap B \\ \text{iff} & x \in (S \cap A) \cup (S \cap B). \end{array}$$

Thus the set $S \cap (A \cup B)$ has the same elements as the set $(S \cap A) \cup (S \cap B)$, so these two sets are equal. This proves (a). The proof of (b) is left as an exercise. ■

Exercise 16. Prove Theorem 10.21(b).

10.22 Proposition. (The Associative Laws for Unions and Intersections.) *Let A, B, and C be sets. Then:*

(a) $(A \cup B) \cup C = A \cup (B \cup C)$.

(b) $(A \cap B) \cap C = A \cap (B \cap C)$.

Proof. (a) Recall that by one of the associative laws for propositional calculus, $(P \vee Q) \vee R$ is logically equivalent to $P \vee (Q \vee R)$. Bearing this in mind, for each x, we have

$$\begin{array}{ll} & x \in (A \cup B) \cup C \\ \text{iff} & x \in A \cup B \text{ or } x \in C \\ \text{iff} & (x \in A \text{ or } x \in B) \text{ or } x \in C) \\ \text{iff} & x \in A \text{ or } (x \in B \text{ or } x \in C) \\ \text{iff} & x \in A \text{ or } x \in B \cup C \\ \text{iff} & x \in A \cup (B \cup C). \end{array}$$

Thus the set $(A \cup B) \cup C$ has the same elements as the set $A \cup (B \cup C)$, so these two sets are equal. This proves (a). The proof of (b) is similar but is based on the other associative law of propositional calculus, according to which $(P \wedge Q) \wedge R$ is logically equivalent to $P \wedge (Q \wedge R)$. ■

It follows from Proposition 10.22 that it makes sense to write $A \cup B \cup C$ and $A \cap B \cap C$ without parentheses. Notice that $A \cup B \cup C$ is the set of all things which belong to at least one of the three sets A, B, and C. Also, $A \cap B \cap C$ is the set of all things that belong to all three of the sets A, B, and C. Similar remarks apply to unions and intersections involving four or more sets.

Exercise 17. Give an example of three sets A, B, and C such that

$$(A \cup B) \cap C \neq A \cup (B \cap C).$$

(Thus it does not make sense to write $A \cup B \cap C$ without parentheses.)

10.23 Proposition. (The Commutative Laws for Unions and Intersections.) *Let A and B be sets. Then:*

(a) $A \cup B = B \cup A$.

(b) $A \cap B = B \cap A$.

Proof. This is similar to the proof of Proposition 10.22 but is based on the commutative laws for propositional calculus, according to which $P \vee Q$ is logically equivalent to $Q \vee P$ and $P \wedge Q$ is logically equivalent to $Q \wedge P$. ■

More about Algebra of Set Operations.

10.24 Remark. If all of the sets we are dealing with in a particular discussion are subsets of a fixed set T, then one often shortens the notation $T \setminus A$ to A^c, which may be read "A complement."[3] Notice that when A and B are subsets of a fixed set T, then $(A^c)^c = A$, $A \setminus B$ may be written as $A \cap B^c$, and De Morgan's laws, in the special case where the set S in Theorem 10.20 is equal to the set T here, may be stated as follows:

(a) $(A \cup B)^c = A^c \cap B^c$.
(b) $(A \cap B)^c = A^c \cup B^c$.

10.25 Example. Let us use the observations from Remark 10.24 to give an alternative solution to Exercise 15(a).[4] Let S, A, and B be sets. Let T be any set such that each of S, A, and B is a subset of T. (For instance, $T = S \cup A \cup B$ would do.) For each subset $E \subseteq T$, write E^c for $T \setminus E$. Then

$$\begin{aligned} S \setminus (A \setminus B) &= S \cap (A \cap B^c)^c = S \cap (A^c \cup (B^c)^c) \\ &= S \cap (A^c \cup B) = (S \cap A^c) \cup (S \cap B) = (S \setminus A) \cup (S \cap B), \end{aligned}$$

where we used one of De Morgan's laws in the second step.

Exercise 18. Let A, B, and C be sets. Use methods of Example 10.25 to prove the following set equations.

(a) $A \cap (B \setminus C) = (A \cap B) \setminus C = (A \setminus C) \cap B$.
(b) $A \cup (B \setminus C) = (A \cup B) \setminus (C \setminus A)$.
(c) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$.
(d) $(A \cap B) \setminus C = A \cap (B \setminus C) = (A \setminus C) \cap B$.
(e) $(A \setminus B) \setminus C = A \setminus (B \cup C)$.

10.26 Remark. If you survey the results and exercises from Theorem 10.20 through Exercise 18 and take into account the commutative laws for unions and intersections, you will find that we have obtained rules for manipulating all expressions of the forms $A \star (B \diamond C)$ and $(A \star B) \diamond C$, where A, B, and C are sets and where $\star$ and $\diamond$ can each be any one of $\cap$, $\cup$, and $\setminus$.

More Connections between Set Inclusion and Set Operations.

Exercise 19. Let A, B and X be sets.

(a) Prove that if $A \subseteq B$, then $X \setminus B \subseteq X \setminus A$.
(b) Prove that $A \subseteq X$ iff $A = X \setminus (X \setminus A)$. (Hint: Use the result of an earlier exercise to express $X \setminus (X \setminus A)$ in a simpler form.)
(c) Suppose $A \subseteq X$. Prove that if $X \setminus B \subseteq X \setminus A$, then $A \subseteq B$.

Disjointness.

To say that two sets A and B are *disjoint* means that A and B have no elements in common; in other words, $A \cap B = \emptyset$. To say that several sets $A, B, C, \ldots$ are *pairwise disjoint* means that each two of them are disjoint. For instance, three sets A, B, and C are said to be pairwise disjoint when $A \cap B = \emptyset$, $A \cap C = \emptyset$ and $B \cap C = \emptyset$. To say that a set of sets $\mathscr{M}$ is *pairwise disjoint* means that each two distinct elements of $\mathscr{M}$ are disjoint; in other words, for each $S \in \mathscr{M}$, for each $T \in \mathscr{M}$, if $S \neq T$, then $S \cap T = \emptyset$.

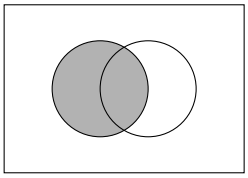
Exercise 20. Let A and B be sets. Let $C = A \setminus B$, $D = A \cap B$, and $E = B \setminus A$. Let $\mathscr{M} = \{ C, D, E \}$. Show that the set of sets $\mathscr{M}$ is pairwise disjoint and that $A \cup B = C \cup D \cup E$.

---

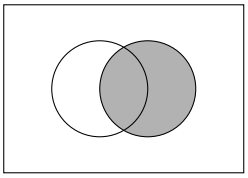
[3] Other common notations for "A complement" are A', $\overline{A}$ and $\widetilde{A}$. But these may mean other things too, so you should check what notation whatever book you are reading uses.

[4] Of course you should not copy this alternative solution as your answer to Exercise 15(a)! There, you should write a solution based on methods already developed at that point.

Venn Diagrams. There is a pictorial way of checking set identities such as De Morgan's laws, the distributive laws, and so on. The sorts of pictures used in this method are called *Venn diagrams*.[5] In these diagrams, the universe of discourse is represented by a rectangle, and subsets of the universe of discourse are represented by regions drawn within the rectangle. The region representing the set in the caption is shaded. Thus, the two Venn diagrams

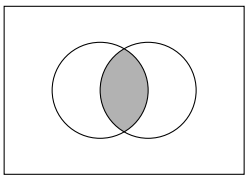


A

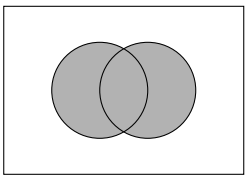


B

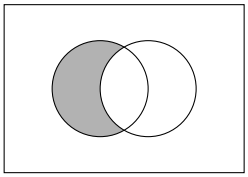
indicate that the interior of the left circle in each diagram represents the set A and the interior of the right circle represents the set B. Then in the following Venn diagrams



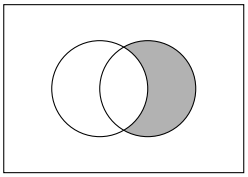
$A \cap B$



$A \cup B$

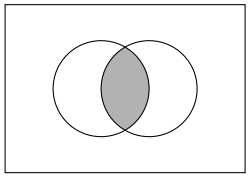


$A \setminus B$



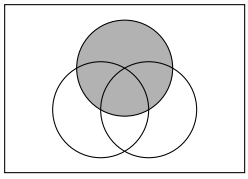
$B \setminus A$

the shaded regions represent the sets $A \cap B$, $A \cup B$, $A \setminus B$, and $B \setminus A$ respectively. From the Venn diagrams labeled A and $A \setminus B$, we can see that the Venn diagram for $A \setminus (A \setminus B)$ is as follows.

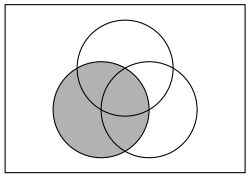


$A \setminus (A \setminus B)$

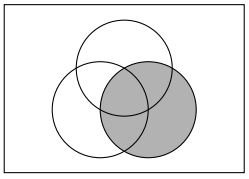
Notice that the shaded region in this Venn diagram is the same as the shaded region in the Venn diagram for $A \cap B$. In this way we have verified the set identity $A \setminus (A \setminus B) = A \cap B$ by means of Venn diagrams. This method works equally well for set identities involving three sets. For instance, we may verify the set identity $S \setminus (A \cup B) = (S \setminus A) \cap (S \setminus B)$ (one of De Morgan's laws for sets) by drawing the following Venn diagrams.



S

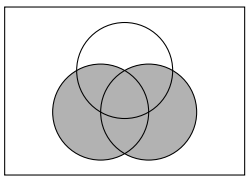


A

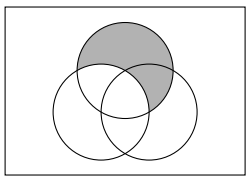


B

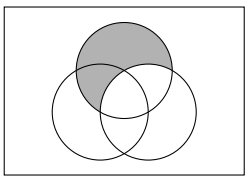
[5] Around 1880, the English logician John Venn introduced similar diagrams to illustrate various patterns of logical reasoning. His diagrams were refinements of diagrams that had been used earlier by Leibniz and by Euler.



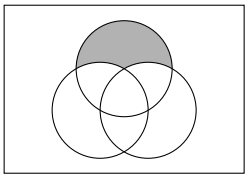
$A \cup B$



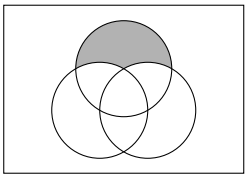
$S \setminus A$



$S \setminus B$

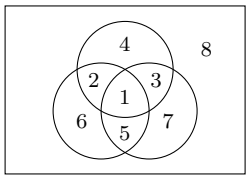


$S \setminus (A \cup B)$



$(S \setminus A) \cap (S \setminus B)$

The reason why the Venn diagram approach works for arbitrary sets, and not just for sets which are circles in the plane, is that it is a pictorial representation of a truth table. For instance, in the case of the Venn diagram verification that we just did for the set identity $S \setminus (A \cup B) = (S \setminus A) \cap (S \setminus B)$, each of the eight numbered regions in this diagram



corresponds to the line with the same number in the following truth table.

	$x \in S$	$x \in A$	$x \in B$	$x \in A \vee x \in B$	$x \in S \wedge x \notin A$	$x \in S \wedge x \notin B$
1.	T	T	T	T	F	F
2.	T	T	F	T	F	T
3.	T	F	T	T	T	F
4.	T	F	F	F	T	T
5.	F	T	T	T	F	F
6.	F	T	F	T	F	F
7.	F	F	T	T	F	F
8.	F	F	F	F	F	F

	$x \in S \wedge \neg(x \in A \vee x \in B)$	$(x \in S \wedge x \notin A) \wedge (x \in S \wedge x \notin B)$
1.	F	F
2.	F	F
3.	F	F
4.	T	T
5.	F	F
6.	F	F
7.	F	F
8.	F	F

Each of the Venn diagrams that we drew to verify the set identity $S \setminus (A \cup B) = (S \setminus A) \cap (S \setminus B)$ corresponds to one of the columns in this truth table. (The table has been broken into two pieces because it would be too wide to fit across the page in one piece.)

Exercise 21. Let S, A, and B be sets. Use Venn diagrams to verify the following set identities.

(a) $S \setminus (A \cap B) = (S \setminus A) \cup (S \setminus B)$.

(b) $S \cap (A \cup B) = (S \cap A) \cup (S \cap B)$.

(c) $S \cup (A \cap B) = (S \cup A) \cap (S \cup B)$.

As will be clear from the discussion above, set identities may be verified quite mechanically, either by means of Venn diagrams (if only two or three sets are involved) or by means of truth tables. Nevertheless, to write proofs in words for set identities furnishes good practice in writing proofs. A picture may be worth a thousand words, but it is also true that sometimes words are more effective than pictures. Advanced mathematics is full of examples where a proof in words is more convincing than any picture could be.

Intervals.

An *interval in* $\mathbf{R}$ is a subset $I \subseteq \mathbf{R}$ that contains all the points between any two of its points. In other words, to say that I is an interval in $\mathbf{R}$ means that $I \subseteq \mathbf{R}$ and for each $u \in I$, for each $v \in I$, for each $x \in \mathbf{R}$, if $u < x < v$, then $x \in I$. Thus the set $\{1, 2, 3, 4\}$ is not an interval in $\mathbf{R}$ because for instance it contains the points 1 and 2 but it does not contain the point 1.5 which lies between the points 1 and 2. If $a, b \in \mathbf{R}$ and $a \leq b$, then clearly the following sets are intervals in $\mathbf{R}$.

$$[a, b] = \{ x \in \mathbf{R} : a \leq x \leq b \}$$
$$(a, b) = \{ x \in \mathbf{R} : a < x < b \}$$
$$[a, b) = \{ x \in \mathbf{R} : a \leq x < b \}$$
$$(a, b] = \{ x \in \mathbf{R} : a < x \leq b \}$$

Notice that brackets indicate included endpoints and parentheses indicate excluded endpoints. The interval $[a, b]$ is called *the closed interval from a to b* and the interval (a, b) is called *the open interval from a to b*. The interval $[a, b)$ is called *the left-closed interval from a to b* or *the right-open interval from a to b*. The interval $(a, b]$ is called *the left-open interval from a to b* or *the right-closed interval from a to b*. Intervals of the four types just described are called *bounded intervals*. If $a = b$, then $[a, b] = \{a\}$ and $(a, b) = [a, b) = (a, b] = \emptyset$. These are called *degenerate intervals*. If $c \in \mathbf{R}$, then the following sets are also intervals in $\mathbf{R}$.

$$[c, \infty) = \{ x \in \mathbf{R} : c \leq x \}$$
$$(c, \infty) = \{ x \in \mathbf{R} : c < x \}$$
$$(-\infty, c] = \{ x \in \mathbf{R} : x \leq c \}$$
$$(-\infty, c) = \{ x \in \mathbf{R} : x < c \}$$

The whole real line

$$(-\infty, \infty) = \mathbf{R}$$

is also an interval in $\mathbf{R}$. Remember that ∞ and $-\infty$ are not elements of $\mathbf{R}$, so they are never included in an interval in $\mathbf{R}$. The intervals $[c, \infty)$ and $(-\infty, c]$ are called *closed half-lines*. The intervals (c, ∞) and $(-\infty, c)$ are called *open half-lines*. Half-lines and the whole real line are *unbounded intervals*. It is a consequence of the completeness property of $\mathbf{R}$ (to be discussed later) that any interval in $\mathbf{R}$ is of one of the nine types displayed above.

Exercise 22.

(a) Find $[1, 3] \cap [2, 4]$, $[1, 2] \cap [3, 4]$, and $[1, 4] \cap [2, 3]$.

(b) Find $[1, 3] \cup [2, 4]$ and $[1, 4] \cup [2, 3]$. Are these intervals in $\mathbf{R}$? Is $[1, 2] \cup [3, 4]$ an interval in $\mathbf{R}$?

(c) Find $(1, 4] \setminus (2, 3]$, $(2, 3] \setminus (1, 4]$, $(1, 3] \setminus (2, 4]$, and $(2, 4] \setminus (1, 3]$. Which of these are intervals in $\mathbf{R}$?

Exercise 23. Let $S = \{ x \in \mathbf{Q} : 1 \leq x \leq 2 \}$. Show that S is not an interval in $\mathbf{R}$.

Unions and Intersections of Sets of Sets.

10.27 Definition. Let $\mathscr{A}$ be a set of sets. Then *the union of* $\mathscr{A}$ (denoted $\bigcup \mathscr{A}$) is the set of all things that belong to at least one of the sets in $\mathscr{A}$; in other words,

$$\bigcup \mathscr{A} = \{\, x : x \in A \text{ for some } A \in \mathscr{A} \,\}.$$

10.28 Example. If A, B, and C are sets, then $\bigcup \{\, A, B \,\} = A \cup B$, $\bigcup \{\, A, B, C \,\} = A \cup B \cup C$, $\bigcup \{\, A \,\} = A$, and $\bigcup \emptyset = \emptyset$.

10.29 Example. If $\mathscr{A} = \{\, [1/n, 5] : n \in \mathbf{N} \,\}$, then $\bigcup \mathscr{A} = (0, 5]$.

10.30 Definition. Let $\mathscr{A}$ be a nonempty set of sets. Then *the intersection of* $\mathscr{A}$ (denoted $\bigcap \mathscr{A}$) is the set of all things that belong to all of the sets in $\mathscr{A}$; in other words,

$$\bigcap \mathscr{A} = \{\, x : x \in A \text{ for each } A \in \mathscr{A} \,\}.$$

10.31 Remark. We have not defined $\bigcap \mathscr{A}$ when $\mathscr{A}$ is empty. The reason is that if $\mathscr{A}$ is empty, then it is no restriction to say that an object belongs to all of the sets in $\mathscr{A}$, since there are no such sets. Hence if $\mathscr{A}$ is empty, then every object belongs to all of the sets in $\mathscr{A}$, so it looks as if $\bigcap \mathscr{A}$ should be the set of all objects. But as we have already mentioned, the notion of a set of all objects leads to serious difficulties. For this reason, it is better to define $\bigcap \mathscr{A}$ only when $\mathscr{A}$ is nonempty.

10.32 Example. If A, B, and C are sets, then $\bigcap \{\, A, B \,\} = A \cap B$, $\bigcap \{\, A, B, C \,\} = A \cap B \cap C$, and $\bigcap \{\, A \,\} = A$.

10.33 Example. If $\mathscr{A} = \{\, (-1/n, 5] : n \in \mathbf{N} \,\}$, then $\bigcap \mathscr{A} = [0, 5]$.

10.34 Proposition. *Let $\mathscr{A}$ be a nonempty set of sets and let $A_0 \in \mathscr{A}$. Then*

$$\bigcap \mathscr{A} \subseteq A_0 \subseteq \bigcup \mathscr{A}.$$

Proof. Consider any $x \in \bigcap \mathscr{A}$. Then for each $A \in \mathscr{A}$, we have $x \in A$. In particular, $x \in A_0$. This shows that $\bigcap \mathscr{A} \subseteq A_0$. Now consider any $x \in A_0$. Then there exists $A \in \mathscr{A}$ such that $x \in A$, because in particular, A_0 is such an A. Thus $x \in \bigcup \mathscr{A}$. This shows that $A_0 \subseteq \bigcup \mathscr{A}$. ■

10.35 Proposition. *Let $\mathscr{A}$ be a nonempty set of sets and let x be any object. Then:*

(a) *$x \notin \bigcup \mathscr{A}$ iff for each $A \in \mathscr{A}$, $x \notin A$.*

(b) *$x \notin \bigcap \mathscr{A}$ iff there exists $A \in \mathscr{A}$ such that $x \notin A$.*

Proof. (a) Recall that by one of the generalized De Morgan's laws from logic, $\neg(\exists A \in \mathscr{A})P(A)$ is logically equivalent to $(\forall A \in \mathscr{A})\neg P(A)$. Bearing this in mind, we have

$$\begin{aligned} & x \notin \bigcup \mathscr{A} \\ \text{iff} \quad & \text{it is not the case that } x \in \bigcup \mathscr{A} \\ \text{iff} \quad & \text{it is not the case that there exists } A \in \mathscr{A} \text{ such that } x \in A \\ \text{iff} \quad & \text{for each } A \in \mathscr{A}, \text{ it is not the case that } x \in A \\ \text{iff} \quad & \text{for each } A \in \mathscr{A}, \ x \notin A. \end{aligned}$$

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

Exercise 24. Prove Proposition 10.35(b).

10.36 Theorem. (The Generalized De Morgan's Laws for Sets of Sets.) *Let S be a set and let $\mathscr{A}$ be a nonempty set of sets. Then:*

(a) $S \setminus \bigcup \mathscr{A} = \bigcap \{\, S \setminus A : A \in \mathscr{A} \,\}$.

(b) $S \setminus \bigcap \mathscr{A} = \bigcup \{\, S \setminus A : A \in \mathscr{A} \,\}$.

Proof. (a) Let $\mathscr{B} = \{\, S \setminus A : A \in \mathscr{A} \,\}$. We wish to show that $S \setminus \bigcup \mathscr{A} = \bigcap \mathscr{B}$. Now for each x, we have

$$x \in S \setminus \bigcup \mathscr{A}$$

$$\begin{aligned}
&\text{iff } \ x \in S \text{ and } x \notin \bigcup \mathscr{A} \\
&\text{iff } \ x \in S \text{ and for each } A \in \mathscr{A},\ x \notin A \\
&\text{iff } \ \text{for each } A \in \mathscr{A},\ x \in S \text{ and } x \notin A \\
&\text{iff } \ \text{for each } A \in \mathscr{A},\ x \in S \setminus A \\
&\text{iff } \ \text{for each } B \in \mathscr{B},\ x \in B \\
&\text{iff } \ x \in \bigcap \mathscr{B},
\end{aligned}$$

where we have used Proposition 10.35 in the second step. Thus the set $S \setminus \bigcup \mathscr{A}$ has the same elements as the set $\bigcap \mathscr{B}$, so these two sets are equal. This proves (a). The proof of (b) is left as an exercise. ■

Exercise 25. Prove Theorem 10.36(b).

10.37 Theorem. (The Generalized Distributive Laws for Sets of Sets.) *Let S be a set and let $\mathscr{A}$ be a nonempty set of sets. Then:*

(a) $S \cap \bigcup \mathscr{A} = \bigcup \{\, S \cap A : A \in \mathscr{A} \,\}$.

(b) $S \cup \bigcap \mathscr{A} = \bigcap \{\, S \cup A : A \in \mathscr{A} \,\}$.

Proof. (a) Let $\mathscr{B} = \{\, S \cap A : A \in \mathscr{A} \,\}$. We wish to show that $S \cap \bigcup \mathscr{A} = \bigcup \mathscr{B}$. For each x, we have

$$\begin{aligned}
&x \in S \cap \bigcup \mathscr{A} \\
&\text{iff } \ x \in S \text{ and } x \in \bigcup \mathscr{A} \\
&\text{iff } \ x \in S \text{ and there exists } A \in \mathscr{A} \text{ such that } x \in A \\
&\text{iff } \ \text{there exists } A \in \mathscr{A} \text{ such that } x \in S \text{ and } x \in A \\
&\text{iff } \ \text{there exists } A \in \mathscr{A} \text{ such that } x \in S \cap A \\
&\text{iff } \ \text{there exists } B \in \mathscr{B} \text{ such that } x \in B \\
&\text{iff } \ x \in \bigcup \mathscr{B}.
\end{aligned}$$

Thus the set $S \cap \bigcup \mathscr{A}$ has the same elements as the set $\bigcup \mathscr{B}$, so these two sets are equal. This proves (a). The proof of (b) is left as an exercise. ■

Exercise 26. Prove Theorem 10.37(b).

Exercise 27. Let A be a set and let $\mathscr{B}$ be a nonempty set of sets. Show that:

(a) $A \cup \bigcup \mathscr{B} = \bigcup \{\, A \cup B : B \in \mathscr{B} \,\}$.

(b) $A \cap \bigcap \mathscr{B} = \bigcap \{\, A \cap B : B \in \mathscr{B} \,\}$.

The Power Set of a Set.

10.38 Definition. Let A be a set. The *power set of A* (denoted $\mathscr{P}(A)$) is the set of all subsets of A; in other words, $\mathscr{P}(A) = \{\, S : S \subseteq A \,\}$.

For instance, the power set of $\{\, 3, 5 \,\}$ is $\mathscr{P}(\{\, 3, 5 \,\}) = \big\{\, \varnothing, \{\, 3 \,\}, \{\, 5 \,\}, \{\, 3, 5 \,\} \big\}$. Note that the empty set is an element of the power set of any set, because the empty set is a subset of any set. Also, for each set A, we have $A \in \mathscr{P}(A)$ because $A \subseteq A$. For instance, notice that $\{\, 3, 5 \,\} \in \mathscr{P}(\{\, 3, 5 \,\})$ in the example above.

If A is a finite set, with n elements, then it turns out that the power set of A has 2^n elements. This is illustrated above with $A = \{\, 3, 5 \,\}$ and $n = 2$. Later we shall see how to prove this in general, by induction on n. By the way, this fact is one of the reasons for the name "power set."

Exercise 28. Find $\mathscr{P}(\{\, 1, 2, 3 \,\})$.

10.39 Example. Starting from the empty set and repeatedly forming power sets we can quickly generate a huge number of sets. Let $V_0 = \varnothing$ and for each $n \in \boldsymbol{\omega}$, let $V_{n+1} = \mathscr{P}(V_n)$. Then, for instance,

$$V_1 = \mathscr{P}(\varnothing) = \{\, \varnothing \,\}, \quad V_2 = \mathscr{P}(\{\, \varnothing \,\}) = \big\{\, \varnothing, \{\, \varnothing \,\} \big\},$$
$$\text{and} \quad V_3 = \mathscr{P}(V_2) = \Big\{\, \varnothing, \{\, \varnothing \,\}, \{\, \{\, \varnothing \,\} \,\}, \{\, \varnothing, \{\, \varnothing \,\} \,\} \Big\}.$$

Note that V_0 has 0 elements, V_1 has $2^0 = 1$ element, V_2 has $2^1 = 2$ elements, and V_3 has $2^2 = 4$ elements. Next, $V_4 = \mathscr{P}(V_3)$, $V_5 = \mathscr{P}(V_4)$, and $V_6 = \mathscr{P}(V_5)$. It would be tedious to write out all of the elements of

V_4: there are $2^4 = 16$ of them. It would be a real chore to write out all $2^{16} = 65536$ elements of V_5. As for V_6, it has $2^{65,536} \approx 2 \times 10^{19,728}$ elements. There is not enough ink in the world to write out all of the elements of V_6. In fact, V_6 has far more elements than there are protons in the known physical universe! In view of this, it boggles the mind to contemplate the fact that the number of elements in V_6 is tiny compared to the number of elements in V_7. And then we have $V_8, V_9, V_{10}, \ldots$ which have even more elements.

Exercise 29.

(a) Calculate a rough upper bound on the number of protons in the known physical universe. (You may use the following facts: the radius of the known physical universe is about 1.5×10^{10} light years; the speed of light is about 3×10^8 meters per second; the diameter of an atom is about 10^{-10} meters; the average density of the known physical universe is (much) less than the density of water.[6])

(b) The number of elements in the set V_6 in Example 10.39 is $2^{65,536}$. Explain how we can determine that this is about $2 \times 10^{19,728}$ and use this to verify that it is much larger than the number of protons in the known physical universe.

The Whole Numbers as Sets.

It is possible to define the whole numbers $0, 1, 2, \ldots$ as sets built up from the empty set, in the following way which was first pointed out[7] by the German logician Gottlob Frege in a book published in 1884. First, define 0 to be the empty set $\emptyset$. Then define 1 to be the set $\{\, 0 \,\}$, define 2 to be the set $\{\, 0, 1 \,\}$, define 3 to be the set $\{\, 0, 1, 2 \,\}$, and so on. Notice that in this way, each whole number n is defined to be a certain set with n elements. Notice also that the operation of adding 1 to a whole number n may be expressed in terms of set operations, since $n + 1 = \{\, 0, 1, 2, \ldots, n-1, n \,\} = \{\, 0, 1, 2, \ldots, n-1 \,\} \cup \{\, n \,\} = n \cup \{\, n \,\}$.

Other Mathematical Objects as Sets.

After one has defined each whole number as a suitable set, one can define each integer as a suitable set, then each rational number, each real number, each complex number, and so on. Indeed it turns out that all of the mathematical objects that are needed can be defined as suitable sets built up from the empty set. The particular way in which mathematical objects are defined as sets is not very important. What is important is the fact that by defining mathematical objects as sets, we can express essentially all of mathematics within set theory. Because of the simplicity of set theory, this increases our confidence in the consistency of mathematics. The possibility of defining all mathematical objects as sets is a striking illustration of the power of set theory.

Ordered Pairs.

We write (a, b) for the ordered pair whose first entry is the object denoted by a and whose second entry is the object denoted by b. (By the way, when a and b are real numbers with $a \leq b$, it is important to distinguish between the ordered pair (a, b) and the open interval (a, b). This is a minor notational conflict which should not lead to misunderstandings.) The fundamental property of ordered pairs is that the ordered pair (a, b) is equal to the ordered pair (a', b') if and only if $a = a'$ and $b = b'$. Note that if the set $\{\, a, b \,\}$ is equal to the set $\{\, a', b' \,\}$, it does not follow that $a = a'$ and $b = b'$. For instance, $\{\, 3, 5 \,\} = \{\, 5, 3 \,\}$. Thus it would not do to define the ordered pair (a, b) to be the set $\{\, a, b \,\}$. But if all mathematical objects that are needed can be defined as suitable sets, as was suggested in the previous paragraph, then it ought to be possible to define the ordered pair (a, b) as a suitable set. This is indeed possible, as was first shown by the American mathematician Norbert Wiener (1914). Wiener's definition has been replaced by a simpler one that was proposed by the Polish mathematician Kasimir Kuratowski (1921). Here is Kuratowski's definition.

10.40 Definition. Let a and b be any objects. The *ordered pair* (a, b) is the set $\big\{\, \{\, a \,\}, \{\, a, b \,\} \,\big\}$.

---

[6] Actually, the average density of the known physical universe is believed to be around 1 hydrogen atom per 10 cubic meters.

[7] See §70 through §83 in Gottlob Frege, *Die Grundlagen der Arithmetik - Eine logisch mathematische Untersuchung über den Begriff der Zahl*, Verlag von Willhelm Koebner, Breslau, 1884, translated into English by J. L. Austin as *The Foundations of Arithmetic - A logico-mathematical enquiry into the concept of number*, Philosophical Library, Inc., New York, 1950.

By the way, both Wiener and Kuratowski made outstanding contributions to twentieth century mathematics. Their definitions of ordered pairs are among their minor contributions. Let us verify that Kuratowski's definition of ordered pairs satisfies the fundamental property of ordered pairs.

10.41 The Fundamental Property of Ordered Pairs. *Let a and b be any objects. We have $(a,b) = (a',b')$ if and only if $a = a'$ and $b = b'$.*

Proof. If $a = a'$ and $b = b'$, then $(a,b) = (a',b')$ simply because equals can be substituted for equals. Thus the reverse implication is trivial. Let us prove the forward implication. Suppose $(a,b) = (a',b')$. In other words, suppose $S = S'$, where $S = \{\{a\},\{a,b\}\}$ and $S' = \{\{a'\},\{a',b'\}\}$. We wish to show that $a = a'$ and $b = b'$. Now $\{a'\} \in S'$, so since $S = S'$, $\{a'\} \in S$. Hence $\{a'\} = \{a\}$ or $\{a'\} = \{a,b\}$. Either way, $a \in \{a'\}$, because $a \in \{a\}$ and $a \in \{a,b\}$. Since $a \in \{a'\}$, $a = a'$. Now $\{a',b'\} \in S'$, so since $S = S'$, $\{a',b'\} \in S$. Thus $\{a',b'\} = \{a\}$ or $\{a',b'\} = \{a,b\}$. Hence $b' \in \{a\}$ or $b' \in \{a,b\}$. Either way, $b' = a$ or $b' = b$. If $b' = b$, then we are done. Suppose $b' = a$. Then since $a = a'$, $b' = a'$ Hence $S' = \{\{b'\}\}$. But $\{a,b\} \in S'$, because $\{a,b\} \in S$ and $S = S'$. Thus $\{a,b\} = \{b'\}$, so $b \in \{b'\}$, so again $b = b'$. This completes the proof of the forward implication. ■

Let us mention that to say that z *is an ordered pair* means that $z = (x,y)$ for some x and some y. (Notice the existential quantification here. To say that z is an ordered pair does not mean that $z = (x,y)$. Rather, it means that $(\exists x)(\exists y)(z = (x,y))$. The phrase "$z$ is an ordered pair" is a statement about z alone, as is the phrase "$(\exists x)(\exists y)(z = (x,y))$," but the phrase "$z = (x,y)$" is a statement about z, x, and y.) To say that S *is a set of ordered pairs* means that for each $z \in S$, z is an ordered pair. Less formally stated, S is a set of ordered pairs when each element of S is an ordered pair.

Ordered triples can be defined in terms of ordered pairs. The ordered triple (a,b,c) can be defined as $((a,b),c)$. If $(a,b,c) = (a',b',c')$, then $a = a'$, $b = b'$, and $c = c'$. To see this, observe that if $(a,b,c) = (a',b',c')$, then $((a,b),c) = ((a',b'),c')$ by the definition of ordered triples, so $(a,b) = (a',b')$ and $c = c'$ by the fundamental property of ordered pairs, so $a = a'$, $b = b'$, and $c = c'$ by a second application of the fundamental property of ordered pairs.

Ordered quadruples can be defined in terms of ordered triples. The ordered quadruple (a,b,c,d) can be defined as $((a,b,c),d)$. Continuing in this way, we can define ordered n-tuples $(a_1,a_2,\ldots,a_n)$ for each natural number $n \geq 2$.

Exercise 30. Show that if $(a,b,c,d) = (a',b',c',d')$, then $a = a'$, $b = b'$, $c = c'$, and $d = d'$.

One could define the ordered triple (a,b,c) as $(a,(b,c))$ rather than as $((a,b),c)$. If this were done, then it would still be true that if $(a,b,c) = (a',b',c')$, then $a = a'$, $b = b'$, and $c = c'$. However, this would really be a different definition of (a,b,c). It is an annoying but inescapable fact is that $((a,b),c)$ is not equal to $(a,(b,c))$ in general. The following exercise deals with this point.

Exercise 31.

(a) Use the fundamental property of ordered pairs, but not Kuratowski's definition, to show that

$$\text{if } ((a,b),a) = (a,(b,a)), \text{ then } a = b.$$

(b) Use the fundamental property of ordered pairs and Kuratowski's definition to show that

$$((\emptyset,\emptyset),\emptyset) \neq (\emptyset,(\emptyset,\emptyset)).$$

Cartesian Products.

10.42 Definition. Let A and B be sets. Then the *Cartesian product of A and B* (denoted $A \times B$) is the set of all ordered pairs (x,y) such that $x \in A$ and $y \in B$; in other words, $A \times B = \{(x,y) : x \in A \text{ and } y \in B\}$.

The Cartesian product of a set A with itself is $A \times A$, which is also denoted A^2. For instance, the coordinate plane in analytic geometry is $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$, the Cartesian product of the real line $\mathbf{R}$ with itself. (The name "Cartesian" refers to the French mathematican and philosopher René Descartes (1596–1650) who was one of the inventors of analytic geometry.) As another example, the Cartesian product $[1,4] \times [2,3]$ is a rectangle in the coordinate plane.

Exercise 32. Sketch the rectangle $[1,4]\times[2,3]$ in the coordinate plane. (Shade the set of points that belong to this rectangle.)

Cartesian products of more than two sets can also be defined. The Cartesian product of three sets A, B, and C (denoted $A\times B\times C$) is the set of all ordered triples (x,y,z) such that $x\in A$, $y\in B$, and $z\in C$. More generally, given n sets $A_1, A_2, \ldots, A_n$, their Cartesian product $A_1\times A_2\times\cdots\times A_n$ is the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$ such that $a_1\in A_1$, $a_2\in A_2$, …, $a_n\in A_n$. The Cartesian product of a set A with itself n times is usually denoted A^n. In other words,

$$\underbrace{A\times A\times\cdots\times A}_{n \text{ times}} = A^n.$$

The three-dimensional space of analytic geometry is $\mathbf{R}^3=\mathbf{R}\times\mathbf{R}\times\mathbf{R}$, the Cartesian product of the real line $\mathbf{R}$ with itself three times. This is the set of all ordered triples of real numbers. Although we cannot visualize spaces of more than three dimensions, we can easily define such spaces by means of Cartesian products such as $\mathbf{R}^4=\mathbf{R}\times\mathbf{R}\times\mathbf{R}\times\mathbf{R}$, $\mathbf{R}^5=\mathbf{R}\times\mathbf{R}\times\mathbf{R}\times\mathbf{R}\times\mathbf{R}$, and so on.

We should point out that there is no requirement for the sets from which we form a Cartesian product to be sets of numbers. They can be sets of arbitrary objects.

Exercise 33. Let A, B, C, and D be sets.

(a) Prove that $(A\times B)\cap(C\times D)=(A\cap C)\times(B\cap D)$.

(b) Prove that $(A\cup B)\times C=(A\times C)\cup(B\times C)$ and $A\times(B\cup C)=(A\times B)\cup(A\times C)$.

(c) Prove that $(C\times D)\setminus(A\times B)=E\cup F$, where $E=(C\setminus A)\times D$ and $F=C\times(D\setminus B)$.

(d) In the special case where $A=[1,3]=B$ and $C=[2,4]=D$, draw a picture to illustrate the result you proved for the general case in part (c).

(e) The sets E and F in part (c) need not be disjoint. Prove that $(C\times D)\setminus(A\times B)=E\cup F_1$, where E is as in part (c) and $F_1=(C\cap A)\times(D\setminus B)$, and prove that E and F_1 are disjoint.

(f) In the special case where $A=[1,3]=B$ and $C=[2,4]=D$, draw a picture to illustrate the result you proved for the general case in part (e).

(g) Prove that $(C\times D)\setminus(A\times B)=E_1\cup F$, where $E_1=(C\setminus A)\times(D\cap B)$ and F is as in part (c), and prove that E_1 and F are disjoint.

(h) In the special case where $A=[1,3]=B$ and $C=[2,4]=D$, draw a picture to illustrate the result you proved for the general case in part (g).

Exercise 34. Let A, B, and C be sets.

(a) Suppose $A\times C=B\times C$ and $C\neq\emptyset$. Prove that $A=B$.

(b) Can we still get the same conclusion in part (a) without the assumption that $C\neq\emptyset$? Either prove that it can be or give an example to show that in general, it cannot be.

Exercise 35. Let A, B, C, and D be sets. Suppose that $A\times B=C\times D\neq\emptyset$. Prove that $A=C$ and $B=D$.

Further Exercises About Set Algebra (*Optional*).

Exercise 36. Let A, B, and C be sets. Prove that

$$A\setminus C\subseteq(A\setminus B)\cup(B\setminus C).$$

10.43 Definition. Let A and B be sets. The *symmetric difference of A and B* (denoted $A\,\Delta\,B$) is the set of all objects that belong to A but not to B or vice versa. In other words,

$$A\,\Delta\,B=(A\setminus B)\cup(B\setminus A).$$

10.44 Remark. The operation of symmetric difference of sets is commutative. In other words, for all sets A and B, we have $A\,\Delta\,B=B\,\Delta\,A$, because $(A\setminus B)\cup(B\setminus A)=(B\setminus A)\cup(A\setminus B)$, by the commutativity of the operation of union of sets.

Exercise 37. Let A, B, and C be sets. Prove that

$$A \,\Delta\, C \subseteq (A \,\Delta\, B) \cup (B \,\Delta\, C).$$

(Hint: Exercise 36 should help.)

Exercise 38. Let A and B be sets. Prove that $A = B$ iff $A \,\Delta\, B = \emptyset$. (Hint: Exercise 11 should help.)

10.45 Remark. Let A, B, and C be sets. Then $A \,\Delta\, B = C$ iff $(A \,\Delta\, B) \,\Delta\, C = \emptyset$. This follows from Exercise 38.

10.46 Remark. Let A_1 and A_2 be sets. Notice that

$$A_1 \,\Delta\, A_2 = \{\, x : x \in A_k \text{ for exactly one value of } k \,\}.$$

Exercise 39. Let A_1, A_2, and A_3 be sets. Let

$$B_1 = A_1 \setminus (A_2 \cup A_3), \qquad B_2 = A_2 \setminus (A_1 \cup A_3), \qquad B_3 = A_3 \setminus (A_1 \cup A_2), \qquad \text{and} \qquad C = A_1 \cap A_2 \cap A_3.$$

(a) Prove that

$$(A_1 \,\Delta\, A_2) \,\Delta\, A_3 = B_1 \cup B_2 \cup B_3 \cup C.$$

(b) Clearly $C = \{\, x : x \in A_k \text{ for all three values of } k \,\}$. Prove that

$$B_1 \cup B_2 \cup B_3 = \{\, x : x \in A_k \text{ for exactly one value of } k \,\}.$$

(c) Prove that

$$(A_1 \,\Delta\, A_2) \,\Delta\, A_3 = \{\, x : x \in A_k \text{ for exactly one value of } k \text{ or for all three values of } k \,\}.$$

10.47 Remark. In Exercise 39, it is easy to check that the sets B_1, B_2, B_3, and C are pairwise disjoint.

Exercise 40. Let A_1, A_2, and A_3 be sets. Prove that

$$(A_1 \,\Delta\, A_2) \,\Delta\, A_3 = A_1 \,\Delta\, (A_2 \,\Delta\, A_3).$$

(Hint: Use Exercise 39 to show that $(A_1 \,\Delta\, A_2) \,\Delta\, A_3 = (A_2 \,\Delta\, A_3) \,\Delta\, A_1$. Then use Remark 10.44. In applying Exercise 39, a key observation is that for each object x, changing the order of A_1, A_2, and A_3 does not change the number of values of k such that $x \in A_k$.)

10.48 Remark. Exercise 40 tells us that the operation of symmetric difference of sets is associative.

Exercise 41. Let D, E, and F be sets. Prove that

$$(D \,\Delta\, E) \,\Delta\, F = (E \,\Delta\, F) \,\Delta\, D = (F \,\Delta\, D) \,\Delta\, E.$$

(Hint: Use Remark 10.44 and Exercise 40.)

Exercise 42. Let D, E, and F be sets. Prove that the following are equivalent.

(a) $D \,\Delta\, E = F$.

(b) $E \,\Delta\, F = D$.

(c) $F \,\Delta\, D = E$.

(Hint: Use Remark 10.45 and Exercise 41.)

10.49 Remark. It is not difficult to prove, by complete induction, that for each integer $n \geq 2$, for all sets $A_1, A_2, \ldots, A_n$, the expression $A_1 \,\Delta\, A_2 \,\Delta \cdots \Delta\, A_n$ is unambiguous without parentheses and is equal to the set of all objects x such that x belongs to A_k for an odd number of values of k.

Section 11. Functions

It would be no exaggeration to say that the notion of function is the most important general concept in mathematics.[8] A function f may be thought of as a correspondence which to each suitable object x, associates an object $f(x)$ which is called the value of f at x, or the value[9] that f takes on at x. Given such a function f, the set of all such suitable objects x is called *the domain of* f, denoted $\mathrm{Dom}(f)$. The domain of f is often described as the set of all x such that $f(x)$ is defined. Sometimes the elements of the domain of f are called *arguments of* f.

First Examples of Functions.

11.1 Example. For each student x in your class, let $f(x)$ be the first name of x. Then f is a function. The domain of f is the set of students in your class. Note that different x's may have the same $f(x)$, because different people may have the same first name. But each x in your class has just one $f(x)$.

11.2 Definition. Let A be a set. To say that f *is a function on* A means that f is a function and $\mathrm{Dom}(f) = A$.

11.3 Example. Let A be the set of all web pages on the world wide web. For each $x \in A$, let $\ell(x)$ be the number of web pages which link to the web page x. Then ℓ is a function on A. Search engines such as Google use $\ell(x)$ as a measure of the importance of the web page x. The larger $\ell(x)$, the more important x is likely to be. For each $x \in A$, let $L(x)$ be the set of all web pages which link to x. Then L is also a function on A. Note that for each web page x, the number of elements in $L(x)$ is equal to $\ell(x)$. The values of ℓ are whole numbers but the values of L are sets of web pages. If $L(x)$ contains web pages w for which $\ell(w)$ is large, then that is another indicator that x may be important. By the way, notice that it is nontrivial to find $\ell(x)$ and $L(x)$, since to do so, one must check the entire world wide web to find all the web pages which link to x. This is much more complicated than finding all the web pages to which x links.

11.4 Definition. Let A and B be sets. To say that f *is a function from* A *to* B (denoted $f\colon A \to B$) means that f is a function, $\mathrm{Dom}(f) = A$, and for each x, if $x \in A$, then $f(x) \in B$.

11.5 Example. Let $f(x) = x^2$ for all $x \in \mathbf{R}$. Then f is a function. The domain of f is $\mathbf{R}$, the set of real numbers. To each real number x, f associates the number x^2. For instance, $f(3) = 3^2 = 9$, $f(-3) = (-3)^2 = 9$, and $f(\pi) = \pi^2 \approx 9.87$. Since x^2 is a real number for each real number x, we can say $f\colon \mathbf{R} \to \mathbf{R}$. But in fact, $x^2 \geq 0$ for each real number x. Hence $f\colon \mathbf{R} \to [0, \infty)$. Furthermore, if B is any set such that $[0, \infty) \subseteq B$, then $f\colon \mathbf{R} \to B$.

11.6 Remark. When we define a function, the variable that we use for the argument is a dummy variable. For instance in the preceding example, when we wrote "Let $f(x) = x^2$ for all $x \in \mathbf{R}$," the variable x was a dummy variable. Hence, for example, it would have meant the same thing if we had written "Let $f(a) = a^2$ for all $a \in \mathbf{R}$." As we know, the letter used for a dummy variable can be replaced by any other letter, provided conflicts of notation are avoided.

11.7 Example. For all $y \in [0, \infty)$, let $g(y) = \sqrt{y}$, the positive square root of y. Then $g\colon [0, \infty) \to [0, \infty)$. To each positive real number y, g associates the positive real number whose square is y. For instance, $g(4) = 2$, $g((-3)^2) = g(9) = 3$, and $g(2)$is approximately 1.414.

11.8 Example. Let A be a set. A function f on A is said to be a *constant function* when there exists y_0 such that for each $x \in A$, $f(x) = y_0$. It is easy to see that a function f on A is a constant function iff for all $x_1, x_2 \in A$, $f(x_1) = f(x_2)$.

---

[8] The importance of the concept of a function was expressed with particular eloquence by the mathematician Richard Dedekind in the preface to his famous essay *On the Nature and Meaning of Numbers*, first published, in German, in 1887, when he characterized "the ability of the mind to relate things, to let a thing correspond to a thing, or to represent a thing by a thing" as "an ability without which no thinking is possible."

[9] Notice that $f(x)$ does not denote the function, it denotes the value of the function at x. The function is denoted by f.

11.9 Example. A function need not be defined by a single formula. Sometimes you may have to choose one of several formulas to find $f(x)$, where which formula you are to use depends on what the value of x is. For instance, the absolute value function is defined for all $x \in \mathbf{R}$ by

$$|x| = \begin{cases} x & \text{if } x \geq 0; \\ -x & \text{if } x < 0. \end{cases}$$

This means that for all $x \in \mathbf{R}$, if $x \geq 0$, then $|x| = x$, whereas if $x < 0$, then $|x| = -x$.

11.10 Example. Let A be a set and let S be a subset of A. Then *the indicator function of* S, denoted 1_S, is the function on A defined by

$$1_S(x) = \begin{cases} 1 & \text{if } x \in S, \\ 0 & \text{if } x \notin S, \end{cases}$$

for all $x \in A$. The name is suggestive of the fact that the value of $1_S(x)$ "indicates" whether or not x is in the set S; it is 1 if x is in S and it is 0 if x is in $A \setminus S$. (Some authors call this function *the characteristic function of* S and denote it by χ_S. We prefer to call it the indicator function of S because in probability theory, indicator functions are important and the term "characteristic function" has a different meaning.)

Equality of Functions.

Two functions f and g are considered to be equal when they have the same domain and for each x in their domain, $f(x) = g(x)$.

11.11 Example. Let $f(x) = \sqrt{x^2}$ and let $g(x) = |x|$ for all $x \in \mathbf{R}$. Then the functions f and g have the same domain, namely $\mathbf{R}$, and for each $x \in \mathbf{R}$, we have $f(x) = g(x)$, because if $x \geq 0$, then $\sqrt{x^2} = x = |x|$, whereas if $x < 0$, then $-x > 0$, $|x| = -x$, and $\sqrt{x^2} = \sqrt{(-x)^2} = -x$. Thus $f = g$. This illustrates the point that a function is not the same thing as a formula. Different formulas can define the same function.

11.12 Example. Let $f(x) = x + 1$ for all $x \in \mathbf{R}$ and let $g(x) = (x^2 - 1)/(x - 1)$ for all $x \in \mathbf{R} \setminus \{1\}$. (We exclude the number 1 from the domain of g to avoid dividing by 0.) For each $x \in \mathbf{R} \setminus \{1\}$, $g(x) = (x+1)(x-1)/(x-1) = x + 1 = f(x)$. Nevertheless, $g \neq f$ because the domain of g is not the same as the domain of f.

More Examples of Functions.

11.13 Example. Let A be a set. One of the simplest functions on A is *the identity function on* A. This is the function id_A from A to A that is defined by $\mathrm{id}_A(x) = x$ for all $x \in A$. Now let B be a set such that $A \subseteq B$. Then id_A is also a function from A to B. When viewed as a function from A to B, id_A is sometimes called *the inclusion function from* A *to* B. (It is still the same function. Just the point of view is different.)

11.14 Example. Perhaps the simplest function of all is *the empty function*. This is the function whose domain is the empty set. To see that there is a function whose domain is the empty set, notice that $\mathrm{id}_\emptyset$, the identity function on the empty set, is such a function. Now we claim that there is only one such function. To see this, suppose f and g are functions such that $\mathrm{Dom}(f) = \emptyset$ and $\mathrm{Dom}(g) = \emptyset$. We wish to show that $f = g$. Notice that no matter what x is, the conditional sentence

$$\text{if } x \in \emptyset, \text{ then } f(x) = g(x)$$

is true because the antecedent in it, namely $x \in \emptyset$, is false. Hence for each x, if $x \in \emptyset$, then $f(x) = g(x)$. In other words, for each $x \in \emptyset$, $f(x) = g(x)$. Thus f and g agree at all points in their domain, so $f = g$ as desired. It might seem silly to consider the empty function, but it does sometimes serve a purpose.

11.15 Example. Let $S = \{1, 2, 3, 4, 5\}$ and let $\mathscr{A} = \mathscr{P}(S)$, the power set of S. For all $A \in \mathscr{A}$, let $N(A)$ be the number of elements of A. (For instance, $N(\{2, 4, 5\}) = 3$.) Then N is a function on $\mathscr{A}$. Notice that N is a function on a set of sets, not on a set of numbers.

"Well-Defined" Functions.

11.16 Example. Let $S = \{ a, b \}$. If we try to define a function with domain S by letting $f(a) = 1$ and $f(b) = 2$, then there is a potential problem. It is possible that $a = b$. In this case, $f(a)$ should be equal to $f(b)$, so our attempted definition of f calls for $f(a)$ to be equal to 1 and also equal to 2. Clearly this is not possible. Thus we have not given a valid definition of a function. It is common to describe such a situation in colloquial mathematical language by saying that f is not *well-defined*.

Exercise 1. Let $S = \{ a, b, c \}$.

- **(a)** If we try to define a function f on S by letting $f(a) = 2$, $f(b) = 3$, and $f(c) = 5$, what do we need to know to be sure that f is well-defined?
- **(b)** If we try to define a function g on S by letting $g(a) = 1$, $g(b) = 0$, and $g(c) = 0$, what do we need to know to be sure that g is well-defined?
- **(c)** If we try to define a function h on S by letting $h(a) = 1$, $h(b) = 1$, and $h(c) = 1$, do we need to know anything to be sure that h is well-defined?

11.17 Example. Let A and B be sets, let f be a function on A, and let g be a function on B. Suppose we try to define a function h on $A \cup B$ by letting

$$h(x) = \begin{cases} f(x) & \text{if } x \in A, \\ g(x) & \text{if } x \in B, \end{cases}$$

for all $x \in A \cup B$. If $x \in A \cup B$, then is $h(x) = f(x)$ or is $h(x) = g(x)$? We see that if $f(x) = g(x)$ for all $x \in A \cap B$, then h is well-defined. In particular, if $A \cap B = \emptyset$, then h is well-defined. However, if there exists $x \in A \cap B$ such that $f(x) \neq g(x)$, then h is not well-defined.

11.18 Example. Here is another example of a purported function that turns out not to be well-defined. Let $A = \big\{ \{ x, y \} : x, y \in \mathbf{R} \big\}$. If we try to define a function f with domain A by letting $f(\{ x, y \}) = x - y$ for all $\{ x, y \} \in A$, then we run into trouble. The reason is that $\{ x, y \} = \{ y, x \}$. So for instance, on the one hand, $f(\{ 2, 6 \})$ should be $2 - 6 = -4$, but on the other hand, $f(\{ 2, 6 \})$ should be $6 - 2 = 4$, because $\{ 2, 6 \} = \{ 6, 2 \}$. The problem is that a typical element a in A has more than one description as $\{ x, y \}$ and our attempted definition of $f(a)$ depends on which description of a is used, not just on a itself. Thus we have not given a valid definition of a function. In other words, in colloquial mathematical language, f is not *well-defined*.

In contrast, if we let $g(\{ x, y \}) = x + y$ for all $\{ x, y \} \in A$, then g is well-defined, because the dependence of $g(a)$ on the description of a as $\{ x, y \}$ is only apparent. Since $x + y = y + x$, both such descriptions of an element a in A give the same value for $g(a)$. If you were alert, you will have noticed the following fact: for each $x \in \mathbf{R}$, $g(\{ x \})$ is defined and is equal to $x + x$, because $\{ x \} = \{ x, x \}$.

Functions of Two or More Variables.

The general notion of a function is broad enough to encompass the notion of a function of two variables. A function of two variables is simply a function whose domain is a set of ordered pairs. Similarly, a function of three variables is a function whose domain is a set of ordered triples. Similar remarks hold for functions of four variables, five variables, and so on.

11.19 Example. Let $f(x, y) = \log(x^2 + y^2)$ for all $(x, y) \in \mathbf{R}^2 \setminus \{ (0, 0) \}$. Then f is a function. (Note that f is well-defined because if $(x, y) = (x', y')$, then $x = x'$ and $y = y'$ by the fundamental property of ordered pairs, so $x^2 + y^2 = (x')^2 + (y')^2$, so $\log(x^2 + y^2) = \log\big((x')^2 + (y')^2\big)$. You should contrast this with what we saw in Example 11.18.) The domain of f is the whole xy-plane except for the origin. (The origin $(0, 0)$ is omitted from the domain of f because $\log 0$ is undefined.)

11.20 Remark. In Example 11.19, the argument of the function f is an ordered pair (x, y). Thus it would be more consistent to write $f((x, y))$ instead of $f(x, y)$. However, it is customary not to do so, as such notation would be cumbersome. This remark applies to the next example too.

11.21 Example. Let A and B be sets and let $\pi_A(x, y) = x$ and $\pi_B(x, y) = y$ for all $(x, y) \in A \times B$. Then π_A and π_B are functions on $A \times B$. (They are well-defined because if $(x, y) = (x', y')$, then $x = x'$ and $y = y'$ by the fundamental property of ordered pairs.) We have $\pi_A \colon A \times B \to A$ and $\pi_B \colon A \times B \to B$. The functions π_A and π_B are called the *projections* from $A \times B$ to A and B respectively.

Mappings.

Sometimes a function f is called a *map* or *mapping*, and for each x in the domain of f, the point x is said to be *mapped* to $f(x)$ by f. This terminology was probably inspired by examples such as the next one.

11.22 Example. A map of a city, or of a country, or of any region on the surface of planet Earth, may be thought of as representing a function from the set of points on the paper on which the map is printed, to the set of points of the region in question. (Alternatively, it makes equally good sense to think of the map as representing a function from the set of points of the region to the set of points on the paper.)

Functions of Functions.

It is perfectly possible for the domain of a function to itself be a set of functions. In fact, some of the most interesting functions are of this sort.

11.23 Example. Let $a, b \in \mathbf{R}$ and suppose $a < b$. Let $C[a,b]$ be the set of all continuous functions from the interval $[a,b]$ to $\mathbf{R}$. For each $f \in C[a,b]$, let

$$I(f) = \int_a^b f(x)\,dx.$$

Then I is a function from $C[a,b]$ to $\mathbf{R}$. Notice that I is a function from a set of functions to a set of numbers. Such a function is sometimes called a *functional*.

Exercise 2. Let a, b, and I be as in Example 11.23, let $c \in \mathbf{R}$, and let $g(x) = c$ for all $x \in [a,b]$. Find $I(g)$.

11.24 Example. Let $a, b \in \mathbf{R}$ and suppose $a < b$. Let $C[a,b]$ be the set of continuous functions from $[a,b]$ to $\mathbf{R}$ and let $C^1[a,b]$ be the set of continuously differentiable functions on $[a,b]$. For each $f \in C^1[a,b]$, let $D(f)$ be the function defined by $D(f)(x) = f'(x)$ for all $x \in [a,b]$, where f' denotes the derivative of f. Note that for each $f \in C^1[a,b]$, we have $D(f) \in C[a,b]$ because the derivative of a continuously differentiable function is a continous function. Thus D is a function from $C^1[a,b]$ to $C[a,b]$. Notice in particular that D is a function from a set of functions to another set of functions. Such a function is often called an *operator*.

11.25 Example. Here is another example of a functional. Let $a, b \in \mathbf{R}$ and suppose $a < b$. Let $C^1[a,b]$ be the set of all continuously differentiable functions from $[a,b]$ to $\mathbf{R}$. For each $f \in C^1[a,b]$, let

$$L(f) = \int_a^b \sqrt{1 + [f'(x)]^2}\,dx.$$

where f' denotes the derivative of f. Then L is a function from $C^1[a,b]$ to $\mathbf{R}$. From your study of calculus, you should know that for each $f \in C^1[a,b]$, $L(f)$ is the length of the curve $y = f(x)$ where x varies over $[a,b]$.

Exercise 3. Let a, b, and L be as in Example 11.25.

- **(a)** Show that for each $f \in C^1[a,b]$, we have $L(f) \geq b - a$.
- **(b)** Let $m \in [0,\infty)$ and let $h(x) = m(x-a)$ for all $x \in [a,b]$. Calculate $L(h)$. Then sketch the graph of h and explain the connection between the value you found for $L(h)$ and the Pythagorean theorem. (Recall that the Pythagorean theorem states that the square of the length of the hypotenuse of a right triangle is equal to the sum of the squares of the lengths of the other two sides.)

Functional Equations.

Sometimes instead of being given an explicit formula for a function, we are just given an identity or *functional equation* that it satisfies.[10] Usually such a functional equation is satisfied by many functions. However, from the fact that a function satisfies a given functional equation, it is often possible and useful to deduce other properties that the function must have. Moreover, such deductions are good illustrations of proof techniques. Accordingly, we include an example and a couple of exercises on this topic here.

11.26 Example. Let $h\colon \mathbf{R} \to \mathbf{R}$ such that

(i) for all $x_1, x_2 \in \mathbf{R}$, $h(x_1 + x_2) = h(x_1) + h(x_2)$.

Then the following are true:

(a) $h(0) = 0$.

(b) For each $x \in \mathbf{R}$, $h(-x) = -h(x)$.

(c) For all $x_1, x_2 \in \mathbf{R}$, $h(x_1 - x_2) = h(x_1) - h(x_2)$.

(d) For each $x \in \mathbf{R}$, $h(2x) = 2h(x)$, $h(3x) = 3h(x)$, and $h(4x) = 4h(x)$.

(e) For each $x \in \mathbf{R}$, $h(-2x) = -2h(x)$, $h(-3x) = -3h(x)$, and $h(-4x) = -4h(x)$.

(f) For each $x \in \mathbf{R}$ and each $n \in \mathbf{Z}$, $h(nx) = nh(x)$.

Proof. (a) Since $0 = 0 + 0$, we have $h(0) = h(0 + 0)$. But $h(0 + 0) = h(0) + h(0)$ by (i). Hence $h(0) = h(0) + h(0)$. Subtracting $h(0)$ from both sides of this equation, we get $0 = h(0)$.

(b) Consider any $x \in \mathbf{R}$. Since $-x + x = 0$, we have $h(-x + x) = h(0)$. But $h(0) = 0$ by (a). Hence $h(-x + x) = 0$. But by (i), $h(-x + x) = h(-x) + h(x)$. Hence $h(-x) + h(x) = 0$. Subtracting $h(x)$ from both sides of this equation, we get $h(-x) = -h(x)$.

(c) Consider any $x_1, x_2 \in \mathbf{R}$. Since $x_1 - x_2 = x_1 + (-x_2)$, we have $h(x_1 - x_2) = h(x_1 + (-x_2))$. But by (i), $h(x_1 + (-x_2)) = h(x_1) + h(-x_2)$. Next, by (b), $h(-x_2) = -h(x_2)$. Thus $h(x_1 - x_2) = h(x_1 + (-x_2)) = h(x_1) + h(-x_2) = h(x_1) + [-h(x_2)] = h(x_1) - h(x_2)$, as desired.

(d) Consider any $x \in \mathbf{R}$. Since $2x = x+x$, we have $h(2x) = h(x+x)$. But by (i), $h(x+x) = h(x)+h(x)$. Thus $h(2x) = h(x+x) = h(x)+h(x) = 2h(x)$. Similarly, $h(3x) = h(2x+x) = h(2x)+h(x) = 2h(x)+h(x) = 3h(x)$ and $h(4x) = h(3x + x) = h(3x) + h(x) = 3h(x) + h(x) = 4h(x)$.

(e) Consider any $x \in \mathbf{R}$. By (b), we have $h(-2x) = -h(2x)$. By (d), we have $h(2x) = 2h(x)$. Thus $h(-2x) = -h(2x) = -2h(x)$. Similarly, $h(-3x) = -h(3x) = -3h(x)$ and $h(-4x) = -h(4x) = -4h(x)$.

(f) Consider any $x \in \mathbf{R}$. First, let us prove by induction that for each $n \in \mathbf{N}$, we have $h(nx) = nh(x)$. Let $P(n)$ be the sentence

$$h(nx) = nh(x).$$

BASE CASE: Obviously $P(1)$ is true because $h(1 \cdot x) = h(x) = 1 \cdot h(x)$.

INDUCTIVE STEP: Let $n \in \mathbf{N}$ such that $P(n)$ is true. Then $h(nx) = nh(x)$. Now $h((n+1)x) = h(nx+x)$. But $h(nx + x) = h(nx) + h(x)$ by (i). Hence $h((n + 1)x) = h(nx) + h(x) = nh(x) + h(x) = (n + 1)h(x)$. Thus $P(n + 1)$ is true too.

CONCLUSION: Therefore, by induction, for each $n \in \mathbf{N}$, $P(n)$ is true. In other words, for each $n \in \mathbf{N}$, $h(nx) = nh(x)$.

Now consider any $n \in \mathbf{Z}$. Then either $n \in \mathbf{N}$ or $n = 0$ or $-n \in \mathbf{N}$. We have already shown that $h(nx) = nh(x)$ if $n \in \mathbf{N}$. If $n = 0$, then $h(nx) = h(0 \cdot x) = h(0) = 0$ by (b) and $nh(x) = 0 \cdot h(x) = 0$, so $h(nx) = nh(x)$ in this case too. Finally, if $-n \in \mathbf{N}$, then $h(nx) = h(-(-n)x) = -h((-n)x)$ by (b) and $h((-n)x) = (-n)h(x)$ since $-n \in \mathbf{N}$, so $h(nx) = -[(-n)h(x)] = nh(x)$. ■

11.27 Remark. If $c \in \mathbf{R}$ and $h(x) = cx$ for all $x \in \mathbf{R}$, then h satisfies condition (i) of Example 11.26 because $c(x_1 + x_2) = cx_1 + cx_2$ for all $x_1, x_2 \in \mathbf{R}$. However in Example 11.26, it is not given that $h(x)$ is of the form cx, so we must not assume that $h(x)$ is of this form in the proof. As a matter of fact, there are functions h satisfying condition (i) of Example 11.26 that are not of the form $h(x) = cx$. Such functions turn out to be very bizarre, but they can be shown to exist.

[10] This is a different use of the word "functional" than we saw in Example 11.23 or Example 11.25.

Exercise 4. Let $f\colon (0,\infty) \to \mathbf{R}$ such that

(i) for all $x_1, x_2 \in (0,\infty)$, $f(x_1 x_2) = f(x_1) + f(x_2)$.

Prove the following:

(a) $f(1) = 0$.

(b) For each $x \in (0,\infty)$, $f(1/x) = -f(x)$.

(c) For all $x_1, x_2 \in (0,\infty)$, $f(x_1/x_2) = f(x_1) - f(x_2)$.

(d) For each $x \in (0,\infty)$, $f(x^2) = 2f(x)$, $f(x^3) = 3f(x)$, and $f(x^4) = 4f(x)$.

(e) For each $x \in (0,\infty)$, $f(x^{-2}) = -2f(x)$, $f(x^{-3}) = -3f(x)$, and $f(x^{-4}) = -4f(x)$.

(f) For each $x \in (0,\infty)$ and each $n \in \mathbf{Z}$, $f(x^n) = nf(x)$.

(Note: If $a \in (0,1) \cup (1,\infty)$ and $f(x) = \log_a x$ for all $x \in (0,\infty)$, then f satisfies condition (i) above. However, in your proof, you must not assume that $f(x)$ is of the form $\log_a x$, because this is not given. As a matter of fact, there are functions, albeit very bizarre ones, that satisfy (i) but are not of the form $\log_a x$.)

Exercise 5. Let $g\colon \mathbf{R} \to \mathbf{R}$ such that

(i) for all $y_1, y_2 \in \mathbf{R}$, $g(y_1 + y_2) = g(y_1)g(y_2)$.

Suppose in addition that

(ii) there exists $y \in \mathbf{R}$ such that $g(y) \neq 0$.

Prove the following:

(a) $g(0) = 1$. (Hint: This is analogous to (a) in Exercise 4 and Example 11.26, but it must be proved in a slightly different way. Notice that if we had $g(y) = 0$ for all $y \in \mathbf{R}$, then g would satisfy condition (i) but not condition (ii) and not what you are asked to prove in this part. Therefore your proof will have to make use of the fact that g satisfies condition (ii).)

(b) For each $y \in \mathbf{R}$, $g(y) \neq 0$ and $g(-y) = 1/g(y)$.

(c) For all $y_1, y_2 \in \mathbf{R}$, $g(y_1 - y_2) = g(y_1)/g(y_2)$.

(d) For each $y \in \mathbf{R}$, $g(2y) = g(y)^2$.

(e) For each $y \in \mathbf{R}$, $g(y) > 0$.

(f) For each $y \in \mathbf{R}$, $g(3y) = g(y)^3$ and $g(4y) = g(y)^4$.

(g) For each $y \in \mathbf{R}$, $g(-2y) = g(y)^{-2}$, $g(-3y) = g(y)^{-3}$, and $g(-4y) = g(y)^{-4}$.

(h) For each $y \in \mathbf{R}$ and each $n \in \mathbf{Z}$, $g(ny) = g(y)^n$.

(Note: If $a \in (0,\infty)$ and $g(y) = a^y$ for all $y \in \mathbf{R}$, then g satisfies conditions (i) and (ii). However, in your proof, you must not assume that $g(y)$ is of the form a^y, because this is not given. As a matter of fact, there are functions, albeit very bizarre ones, that satisfy (i) and (ii) but are not of the form a^y.)

The Range of a Function.

11.28 Definition. Let f be a function. The *range of* f (denoted $\mathrm{Rng}(f)$) is the set of all values of f; in other words,

$$\begin{aligned}\mathrm{Rng}(f) &= \{\, f(x) : x \in \mathrm{Dom}(f) \,\} \\ &= \{\, y : y = f(x) \text{ for some } x \in \mathrm{Dom}(f) \,\}.\end{aligned}$$

11.29 Example. Let $f(x) = x^2$ for all $x \in \mathbf{R}$ and let $g(y) = y+4$ for all $y \in [2,5]$. Then $\mathrm{Rng}(f) = [0,\infty)$, $\mathrm{Dom}(g) = [2,5]$, and $\mathrm{Rng}(g) = [6,9]$.

11.30 Example. If f is the empty function, then the domain of f is the empty set, so the range of f is also the empty set. Conversely, if f is a function whose range is the empty set, then the domain of f is the empty set, so f is the empty function.

11.31 Remark. Let f be a function. The range of f is the set of all y such that the equation $f(x) = y$ has at least one solution x in the domain of f.

11.32 Remark. Let A and B be sets. Then $f\colon A \to B$ iff f is a function, $\mathrm{Dom}(f) = A$, and $\mathrm{Rng}(f) \subseteq B$.

Exercise 6. Let $f(x) = x^2 + 1$ for all $x \in \mathbf{R}$, let $g(y) = \sqrt{y-1}$ for all $y \in [1,\infty)$, and let $h(u) = 1 - u$ for all $u \in [2,3)$. Find the range of f, the range of g, and the range of h.

Exercise 7. Let A and B be sets and let π_A and π_B be the projections from $A \times B$ to A and B respectively. (See Example 11.21.) Show that if $B \neq \emptyset$, then $\mathrm{Rng}(\pi_A) = A$, and that if $A \neq \emptyset$, then $\mathrm{Rng}(\pi_B) = B$.

Exercise 8. Let I be as in Example 11.23. What is the range of I? Prove your answer.

Exercise 9. Let L be as in Example 11.25. What is the range of L? Prove your answer.

Composition of Functions.

11.33 Definition. Let f and g be functions. Then *the composition of g with f* is the function, denoted $g \circ f$, that is defined by $(g \circ f)(x) = g(f(x))$ for all $x \in \mathrm{Dom}(f)$ such that $f(x) \in \mathrm{Dom}(g)$. The domain of $g \circ f$ is the set of all $x \in \mathrm{Dom}(f)$ such that $f(x) \in \mathrm{Dom}(g)$.

The short way to read $g \circ f$ is "g composed with f."

11.34 Example. Let A, B, and C be sets, let $f\colon A \to B$, and let $g\colon B \to C$. Then $\mathrm{Dom}(f) = A$ and for each $x \in A$, we have $f(x) \in B = \mathrm{Dom}(g)$. Hence $\mathrm{Dom}(g \circ f) = A$ and $(g \circ f)(x) = g(f(x))$ for all $x \in A$.

11.35 Example. Let $f(x) = x^{1/2}$ for all $x \in [0, \infty)$ and let $g(y) = 1 - y^2$ for all $y \in \mathbf{R}$. Then $f\colon [0,\infty) \to [0,\infty)$ and $g\colon \mathbf{R} \to (-\infty, 1]$. We have $(g \circ f)(x) = g(f(x)) = 1 - f(x)^2 = 1 - x$ for all $x \in [0,\infty)$. Note that $g \circ f$ is not equal to the function h that is defined by $h(x) = 1 - x$ for all $x \in \mathbf{R}$, because $g \circ f$ and h have different domains. The domain of $g \circ f$ is the interval $[0,\infty)$ but the domain of h is the whole real line $\mathbf{R}$.

11.36 Example. Let f and g be as in Example 11.35. Then the domain of $f \circ g$ is the set of all $x \in \mathbf{R}$ such that $g(x) \in \mathrm{Dom}(f)$. This is the set of all $x \in \mathbf{R}$ such that $1 - x^2 \in [0,\infty)$. But for each real number x, we have $1 - x^2 \geq 0$ iff $x^2 \leq 1$ iff $-1 \leq x \leq 1$. Thus the domain of $f \circ g$ is the interval $[-1, 1]$. We have $(f \circ g)(x) = f(g(x)) = g(x)^{1/2} = (1 - x^2)^{1/2}$ for all $x \in [-1, 1]$.

Exercise 10. Let $f(x) = x + 1$ for all $x \in \mathbf{R}$ and let $g(x) = 2x$ for all $x \in \mathbf{R}$. Find $(g \circ f)(x)$ and $(f \circ g)(x)$ for all $x \in \mathbf{R}$. You should find that $g \circ f \neq f \circ g$.

As you can see from preceding exercise and the two preceding examples, in general $g \circ f \neq f \circ g$. In other words, composition of functions is not commutative. Another example of this is furnished by the operations of scraping and painting. You should scrape first and then paint. If you paint first and then scrape, the result will be different!

11.37 Theorem. *Composition of functions is associative. In other words, for all functions f, g, and h, we have*

$$(h \circ g) \circ f = h \circ (g \circ f).$$

This theorem is a consequence of the following more detailed result.

11.38 Theorem. *Let f, g, and h be functions. Let*

$$A = \mathrm{Dom}((h \circ g) \circ f),$$
$$B = \{\, x \in \mathrm{Dom}(f) : f(x) \in \mathrm{Dom}(g) \text{ and } g(f(x)) \in \mathrm{Dom}(h) \,\},$$
$$C = \mathrm{Dom}(h \circ (g \circ f)).$$

Then $A = B = C$ and for each $x \in B$, we have $((h \circ g) \circ f)(x) = h(g(f(x))) = (h \circ (g \circ f))(x)$.

Proof. First let us show that $A = B$ and that for each $x \in B$, we have $((h \circ g) \circ f)(x) = h(g(f(x)))$. To show that $A = B$, we shall show that $A \subseteq B$ and $B \subseteq A$. Consider any $x \in A$. Then $x \in \mathrm{Dom}(f)$ and $f(x) \in \mathrm{Dom}(h \circ g)$. Since $f(x) \in \mathrm{Dom}(h \circ g)$, we have $f(x) \in \mathrm{Dom}(g)$ and $g(f(x)) \in \mathrm{Dom}(h)$. Thus $x \in B$. This shows that $A \subseteq B$. Now consider any $x \in B$. Then $x \in \mathrm{Dom}(f)$, $f(x) \in \mathrm{Dom}(g)$, and $g(f(x)) \in \mathrm{Dom}(h)$. Since $f(x) \in \mathrm{Dom}(g)$ and $g(f(x)) \in \mathrm{Dom}(h)$, we have $f(x) \in \mathrm{Dom}(h \circ g)$ and $(h \circ g)(f(x)) = h(g(f(x)))$. Since $x \in \mathrm{Dom}(f)$ and $f(x) \in \mathrm{Dom}(h \circ g)$, we have $x \in \mathrm{Dom}((h \circ g) \circ f)$ and $((h \circ g) \circ f)(x) = (h \circ g)(f(x))$. Hence $x \in A$ and $((h \circ g) \circ f)(x) = h(g(f(x)))$. This shows that $B \subseteq A$ and that for each $x \in B$, $((h \circ g) \circ f)(x) = h(g(f(x)))$. Since $A \subseteq B$ and $B \subseteq A$, we have $A = B$. By a similar argument, one can show that $C = B$ and that for each $x \in B$, $(h \circ (g \circ f))(x) = h(g(f(x)))$. ■

Exercise 11. Supply the "similar argument" alluded to at the end of the proof of the preceding theorem.

Restriction and Extension of Functions.

11.39 Definition. Let f be a function and let C be a subset of the domain of f. Then *the restriction of f to C* is the function, denoted $f \restriction C$, defined by $(f \restriction C)(x) = f(x)$ for all $x \in C$. The domain of $f \restriction C$ is C.

11.40 Example. Let $\varphi(u) = 1 - u$ for all $u \in \mathbf{R}$ and let $h(u) = 1 - u$ for all $u \in [2, 3)$. Then $h = \varphi \restriction [2, 3)$, the restriction of φ to the interval $[2, 3)$.

11.41 Example. Let f, g, and h be as in Example 11.35. As was pointed out there, $g \circ f \neq h$. Instead, $g \circ f = h \restriction [0, \infty)$, the restriction of h to the interval $[0, \infty)$. Here we have a natural example where we cannot avoid considering the restriction of a function to a proper subset of what might be thought of as its natural domain.

11.42 Example. Let f be a function, let C be a subset of the domain of f, and let id_C be the identity function on C. Then $f \circ \mathrm{id}_C = f \restriction C$.

11.43 Definition. Let f and g be functions. To say that *f is an extension of g* means that the domain of f is a superset of the domain of g and for each x in the domain of g, $f(x) = g(x)$.

Clearly if f and g are functions, then f is an extension of g iff $\mathrm{Dom}(f) \supseteq \mathrm{Dom}(g)$ and $f \restriction \mathrm{Dom}(g) = g$.

Surjections, Injections, and Inverse Functions.

11.44 Definition. Let A and B be sets. To say that *f is a surjection from A to B* means that f is a function from A to B and for each $y \in B$, there exists $x \in A$ such that $f(x) = y$.

11.45 Example. Let $f(x) = x^2$ for all $x \in \mathbf{R}$. Then f is a surjection from $\mathbf{R}$ to $[0, \infty)$ but f is not a surjection from $\mathbf{R}$ to $\mathbf{R}$.

11.46 Example. Let $g(y) = \sqrt{y}$ for all $y \in [0, \infty)$. Then g is a surjection from $[0, \infty)$ to $[0, \infty)$.

11.47 Remark. Another name for a surjection from A to B is a function from A *onto* B.

11.48 Remark. If A and B are sets, then f is a surjection from A to B iff f is a function, $\mathrm{Dom}(f) = A$, and $\mathrm{Rng}(f) = B$.

11.49 Remark. Any function is a surjection from its domain to its range.

11.50 Remark. Let A and B be sets and let $f \colon A \to B$. Then f is a surjection from A to B iff for each $y \in B$, the equation $f(x) = y$ has at least one solution x in A.

11.51 Definition. To say that *f is an injection* means that f is a function and for all $x_1, x_2 \in \mathrm{Dom}(f)$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$.

Equivalently, f is an injection iff f is a function and for all $x_1, x_2 \in \mathrm{Dom}(f)$, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$. Another term for an injection is a *one-to-one* function. Given sets A and B, to say that *f is an injection from A to B* means that f is a function from A to B and f is an injection.

11.52 Example. Let $f(x) = x^2$ for all $x \in \mathbf{R}$ and let $g(y) = \sqrt{y}$ for all $y \in [0, \infty)$. As we have seen, $f \colon \mathbf{R} \to [0, \infty)$ and $g \colon [0, \infty) \to [0, \infty)$. Now f is not an injection from $\mathbf{R}$ to $[0, \infty)$ because for instance, $f(-2) = f(2)$. In contrast, g *is* an injection from $[0, \infty)$ to $[0, \infty)$. To see this, suppose $y_1, y_2 \in [0, \infty)$ and $g(y_1) = g(y_2)$. We wish to show that $y_1 = y_2$. In view of the definition of g, we have $\sqrt{y_1} = \sqrt{y_2}$. Hence $(\sqrt{y_1})^2 = (\sqrt{y_2})^2$. But $(\sqrt{y_1})^2 = y_1$ and $(\sqrt{y_2})^2 = y_2$. Thus $y_1 = y_2$, as desired.

11.53 Remark. Let A and B be sets and let $f \colon A \to B$. Then f is an injection from A to B iff for each $y \in B$, the equation $f(x) = y$ has *at most* one solution x in A.

11.54 Remark. Let A and B be sets and let $f \colon A \to B$. Then f is an injection from A to B iff f sends different elements of A to different elements of B. In other words, f is an injection from A to B iff for all $x_1, x_2 \in A$, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$. To see this, recall that a conditional sentence $P \Rightarrow Q$ is logically equivalent to its contrapositive $\neg Q \Rightarrow \neg P$.

11.55 Example. Let C be the set of people in your class. For each $x \in C$, let $N(x)$ be the name of x. Then N is a function on C. The function N is an injection iff no two people in your class have the same name.

Exercise 12. Let A be the set of countries in the world and let B be the set of cities in the world. Define a function f from A to B by letting $f(x)$ be the capital city of x, for each country x. (A few countries have multiple capital cities.[11] However, for the purposes of this exercise, so that f will be well-defined, pretend that each country has exactly one capital city.)

(a) Is f a surjection from A to B? Explain.

(b) Is f an injection? Explain.

Exercise 13. Let C be the set of people in the world and for each $x \in C$, let $g(x)$ be the number of hairs on the head of x. Then g is a function from C to the set $\boldsymbol{\omega} = \{\, 0, 1, 2, \dots \}$ of whole numbers.

(a) Is g a surjection from C to $\boldsymbol{\omega}$? Explain.

(b) The diameter of a human hair is about 0.001 inches. From this and from an estimate, which I leave to you, of the area of a person's scalp, calculate an upper bound on the number of hairs on a person's head.[12] In other words, find a number M such that for each $x \in C$, we have $g(x) \leq M$.

(c) Is g an injection? Explain your answer in terms of the number M you found in part (b) and the size of the world population (which you can find with google, for instance).

11.56 Example. Let G be a set of girls and let B be a set of boys. Suppose each girl in G likes exactly one boy in B. For each girl x in G, let $f(x)$ be the unique boy in B that x likes. Then f is a function from G to B. f is a surjection from G to B iff each boy in B is liked by at least one girl in G. f is an injection from G to B iff no two girls in G like the same boy in B.

Exercise 14. The preceding example is a little artificial, in that it asks us to assume that each girl in G likes one and only one boy in B. Let us consider a more realistic situation. Once again, let G be a set of girls and let B be a set of boys. For each girl x in G, let $L(x)$ be the set of boys in B that x likes; in other words,

$$L(x) = \{\, y \in B : x \text{ likes } y \,\}.$$

Then L is a function from G to $\mathscr{P}(B)$, the power set of B.

(a) When is L a surjection from G to $\mathscr{P}(B)$?

(b) When is L an injection from G to $\mathscr{P}(B)$?

(c) If L is an injection from G to $\mathscr{P}(B)$, does it necessarily follow that for all $x_1, x_2 \in G$, if $x_1 \neq x_2$, then $L(x_1)$ and $L(x_2)$ are disjoint? Explain.

Exercise 15. Let S and T be sets. Define a function

$$f\colon \mathscr{P}(S) \times \mathscr{P}(T) \to \mathscr{P}(S \cup T)$$

by $f(A, B) = A \cup B$ for all $A \subseteq S$ and all $B \subseteq T$.

(a) Show that f is a surjection.

(b) Show f is an injection iff S and T are disjoint.

11.57 Definition. Let f be an injection. Then for each y in the range of f, we shall write $f^{-1}(y)$ for the unique x in the domain of f such that $f(x) = y$. This defines a function f^{-1} from $\mathrm{Rng}(f)$ to $\mathrm{Dom}(f)$. The function f^{-1} is called the *inverse of the function* f.

---

[11] See `https://en.wikipedia.org/wiki/List_of_countries_with_multiple_capitals`. I am indebted to Ivo Terek Couto for bringing this to my attention.

[12] The upper bound that you find in this way will be good enough to use in part (c) but it will be much larger than the true number. According to the Encyclopædia Britannica, the average total number of hairs on a person's head is between 100,000 and 150,000. By the way, according to Wikipedia, actual diameters of human hairs range from about 0.0007 inches to about 0.007 inches, with Europeans generally having hair between 0.002 and 0.0035 inches in diameter and Asians around 0.005 inches. (I have converted the diameters into inches. Wikipedia gives them in micrometers.) The figure of 0.001 inches is a good enough approximation for the purposes of this problem.

11.58 Remark. If we think of functions as operations, so that f operates on x to produce $f(x)$, then the inverse function of an injection f is the operation that undoes what f does. For instance, if $f(x) = x + 1$ for all $x \in \mathbf{R}$ (so f is the operation of adding 1), then $f^{-1}(y) = y - 1$ for all $y \in \mathbf{R}$ (so f^{-1} is the operation of subtracting 1). As another example, if $g(x) = 2x$ for all $x \in \mathbf{R}$ (so g is the operation of multiplying by 2), then $g^{-1}(y) = y/2$ for all $y \in \mathbf{R}$ (so g is the operation of dividing by 2).

11.59 Remark. Let f be an injection, so that f has an inverse function f^{-1}. Then $\mathrm{Dom}(f^{-1}) = \mathrm{Rng}(f)$ and $\mathrm{Rng}(f^{-1}) = \mathrm{Dom}(f)$. That $\mathrm{Dom}(f^{-1}) = \mathrm{Rng}(f)$ is obvious from the definition of f^{-1}. To see that $\mathrm{Rng}(f^{-1}) = \mathrm{Dom}(f)$, first note that obviously $\mathrm{Rng}(f^{-1}) \subseteq \mathrm{Dom}(f)$ by the definition of f^{-1}. Now consider any $x \in \mathrm{Dom}(f)$. Let $y = f(x)$. Then $x = f^{-1}(y)$ by the definition of f^{-1}. Hence $x \in \mathrm{Rng}(f^{-1})$. Thus $\mathrm{Dom}(f) \subseteq \mathrm{Rng}(f^{-1})$. Since $\mathrm{Rng}(f^{-1}) \subseteq \mathrm{Dom}(f)$ and $\mathrm{Dom}(f) \subseteq \mathrm{Rng}(f^{-1})$, we have $\mathrm{Rng}(f^{-1}) = \mathrm{Dom}(f)$.

11.60 Example. Let $A = \{a, b, c\}$ where a, b, and c are distinct. Define $f\colon A \to \mathbf{R}$ by $f(a) = 2$, $f(b) = 1$, and $f(c) = 3$. Then f is an injection. The inverse of f is the function $f^{-1}\colon \{1, 2, 3\} \to A$ that is defined by $f(1) = b$, $f(2) = a$, and $f(3) = c$. The inverse of f should not be confused with the reciprocal of f. The reciprocal of f in this example is the function g from A to $\mathbf{R}$ that is defined by $g(a) = 1/2$, $g(b) = 1/1 = 1$, and $g(c) = 1/3$. Every injective function has an inverse function. Every function whose range is a subset of $\mathbf{R} \setminus \{0\}$ has a reciprocal function. The two are seldom the same.

11.61 Definition. Let A and B be sets. To say that *f is a bijection from A to B* means that f is both a surjection from A to B and an injection.

11.62 Remark. Let A and B be sets. Another name for a bijection from A to B is *a one-to-one correspondence between A and B*.

11.63 Theorem. *Let A and B be sets, let f be a function whose domain is A, and let g be a function whose domain is B. Then the following are equivalent.*

(a) *f is a bijection from A to B and $g = f^{-1}$.*

(b) *For all x and all y, we have $x \in A$ and $f(x) = y$ iff $y \in B$ and $x = g(y)$.*

(c) *g is a bijection from B to A and $f = g^{-1}$.*

Proof. We shall prove that (a) implies (b) and that (b) implies (a). (In a similar way, you can show that (c) implies (b) and that (b) implies (c). Just interchange the roles of f and g and of A and B.)

(a)⇒(b): Suppose f is a bijection from A to B and $g = f^{-1}$. Then in particular, $f\colon A \to B$ and $g\colon B \to A$. Consider any x and any y. Suppose $x \in A$ and $f(x) = y$. Then $y \in B$ because $f\colon A \to B$. Furthermore, $x = f^{-1}(y)$. But $g = f^{-1}$. Hence $x = g(y)$. This proves the forward implication in (b). Conversely, suppose $y \in B$ and $x = g(y)$. Then $x \in A$ because $g\colon B \to A$. Furthermore $x = f^{-1}(y)$ because $g = f^{-1}$. Hence $f(x) = y$. This proves the reverse implication in (b).

(b)⇒(a): Suppose that for all x and all y we have $x \in A$ and $f(x) = y$ iff $y \in B$ and $x = g(y)$. We wish to show that f is a bijection from A to B and that $g = f^{-1}$. If $x \in A$, then letting $y = f(x)$, we get $y \in B$ and $x = g(y)$. Hence $f\colon A \to B$ and for each $x \in A$, we have $x = g(f(x))$. If $y \in B$, then letting $x = g(y)$, we get $x \in A$ and $f(x) = y$. Hence f is a surjection from A to B. If $x_1, x_2 \in A$ and $f(x_1) = f(x_2)$, then $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$. Hence f is an injection. Since f is both an injection and a surjection from A to B, f is a bijection from A to B. Hence f^{-1} is defined and is a function from B to A. For each $y \in B$, letting $x = g(y)$, we have $f(x) = y$, so $x = f^{-1}(y)$, so $g(y) = f^{-1}(y)$. Hence $g = f^{-1}$. ■

11.64 Corollary. *Let A and B be sets and let f be a bijection from A to B. Then f^{-1} is a bijection from B to A.*

Proof. Let $g = f^{-1}$. Then by Theorem 11.63, g is a bijection from B to A. ■

The next result tells us that if f is an injection, then the function that undoes what f^{-1} does is f itself.

11.65 Corollary. *Let f be an injection. Then f^{-1} is an injection too and $(f^{-1})^{-1} = f$.*

Proof. Let $A = \mathrm{Dom}(f)$, $B = \mathrm{Rng}(f)$, and $g = f^{-1}$. Then f is a bijection from A to B. Hence by Theorem 11.63, g is a bijection from B to A and $f = g^{-1}$. In particular, f^{-1} is an injection and $f = (f^{-1})^{-1}$. ■

11.66 Example. Let $f(x) = 1 - x$ for all $x \in [0,1)$. We shall show that $f\colon [0,1) \to (0,1]$, that f is an injection, that $f^{-1}(y) = 1 - y$ for all $y \in \mathrm{Rng}(f)$, and finally that $\mathrm{Rng}(f) = (0,1]$. (Consequently, f is a bijection from $[0,1)$ to $(0,1]$.) Let $x \in [0,1)$ and let $y = f(x)$. Since $0 \le x < 1$, $-0 \ge -x > -1$, so $-1 < -x \le 0$, so $-1+1 < -x+1 \le 0+1$, so $0 < 1-x \le 1$, so $f(x) \in (0,1]$. Also, since $y = f(x) = 1-x$, we have $y + x = 1$, so $x = 1 - y$. Thus $f\colon [0,1) \to (0,1]$, f is an injection, and for each $y \in \mathrm{Rng}(f)$, we have $f^{-1}(y) = 1 - y$. To show that $\mathrm{Rng}(f) = (0,1]$, it remains only to show that each y in $(0,1]$ belongs to $\mathrm{Rng}(f)$. Let $y \in (0,1]$. We wish to show that there exists $x \in [0,1)$ such that $f(x) = y$. Let $x = 1 - y$. Then $x + y = 1$, so $y = 1 - x$. Hence, once we have shown that $x \in [0,1)$, we will have that $f(x) = 1 - x = y$. Now $0 < y \le 1$, so $-0 > -y \ge -1$, so $-1 \le -y < -0$, so $-1+1 \le -y+1 < -0+1$, so $0 \le 1 - y < 1$, so $0 \le x < 1$, so $x \in [0,1)$ as desired.

Exercise 16. Sketch the graph of the function f in Example 11.66.

Exercise 17. Let $f(x) = x - 1$ for all $x \in [1,\infty)$.

(a) Show that $f\colon [1,\infty) \to [0,\infty)$ and that f is an injection, and find $f^{-1}(y)$ for each $y \in \mathrm{Rng}(f)$. Then show that $\mathrm{Rng}(f) = [0,\infty)$. Conclude that f is a bijection from $[1,\infty)$ to $[0,\infty)$.

(b) Sketch the graph of f.

Exercise 18. For all $x \in (4,7]$, let $f(x) = 2x + 3$ and $g(x) = 3 - 2x$.

(a) Show that $f\colon (4,7] \to (11,17]$ and that f is an injection, and find $f^{-1}(y)$ for each $y \in \mathrm{Rng}(f)$. Then show that $\mathrm{Rng}(f) = (11,17]$. Conclude that f is a bijection from $(4,7]$ to $(11,17]$.

(b) Show that $g\colon (4,7] \to [-11,-5)$ and that g is an injection, and find $g^{-1}(y)$ for each $y \in \mathrm{Rng}(g)$. Then show that $\mathrm{Rng}(g) = [-11,-5)$. Conclude that g is a bijection from $(4,7]$ to $[-11,-5)$.

(c) Sketch the graphs of f and g.

Exercise 19. Let $f(x) = 1/x$ for all $x \in (0,1]$.

(a) Show that $f\colon (0,1] \to [1,\infty)$ and that f is an injection, and find $f^{-1}(y)$ for each $y \in \mathrm{Rng}(f)$. Then show that $\mathrm{Rng}(f) = [1,\infty)$. Conclude that f is a bijection from $(0,1]$ to $[1,\infty)$.

(b) Sketch the graph of f.

Exercise 20.

(a) Let $g(x) = x/(1-x)$ for all $x \in [0,1)$. Show that $g\colon [0,1) \to [0,\infty)$ and that g is an injection, and find $g^{-1}(y)$ for each $y \in \mathrm{Rng}(g)$. Then show that $\mathrm{Rng}(g) = [0,\infty)$. Conclude that g is a bijection from $[0,1)$ to $[0,\infty)$.

(b) Let $h(x) = x/(1+x)$ for all $x \in (-1,0)$. Show that $h\colon (-1,0) \to (-\infty,0)$ and that h is an injection, and find $h^{-1}(y)$ for each $y \in \mathrm{Rng}(h)$. Then show that $\mathrm{Rng}(h) = (-\infty,0)$. Conclude that h is a bijection from $(-1,0)$ to $(-\infty,0)$.

Exercise 21. Sketch the graph of each of the functions in Exercise 20.

Exercise 22. Let A, C, B, and D be sets. Let $g\colon A \to C$ and let $h\colon B \to D$. Also, let $X = A \cup B$ and $Y = C \cup D$. Suppose that $A \cap B = \emptyset$. Then we can define a function $\varphi\colon X \to Y$ by letting

$$\varphi(x) = \begin{cases} g(x) & \text{if } x \in A, \\ h(x) & \text{if } x \in B, \end{cases}$$

for all $x \in X$. Prove the following statements.

(a) If g is a surjection from A to C and h is a surjection from B to D, then φ is a surjection from X to Y.

(b) If g and h are injections and $C \cap D = \emptyset$, then φ is an injection.

(c) If g is a bijection from A to C and h is a bijection from B to D and $C \cap D = \emptyset$, then φ is a bijection from X to Y and for all $y \in Y$, we have

$$\varphi^{-1}(y) = \begin{cases} g^{-1}(y) & \text{if } y \in C, \\ h^{-1}(y) & \text{if } y \in D. \end{cases}$$

Exercise 23. Let $\varphi(x) = x/(1-|x|)$ for all $x \in (-1,1)$.

(a) Show that φ is a bijection from $(-1,1)$ to $\mathbf{R}$.

(b) Find φ^{-1}. By a suitable use of $|y|$, write your answer in the form of a single formula.

(Hint for both parts: Combine the results of Exercise 20 and Exercise 22.)

11.67 Example. Let $f(x) = (x+2)/(x-3)$ for all $x \in \mathbf{R} \setminus \{3\}$. Then f is a function from $\mathbf{R} \setminus \{3\}$ to $\mathbf{R}$. We shall find the range of f, we shall show that f is a bijection from its domain to its range, and we shall find f^{-1}. Consider any x and any y. Suppose $x \in \mathbf{R} \setminus \{3\}$ and $f(x) = y$. Then $(x+2)/(x-3) = y$, so $x+2 = (x-3)y$, so $x+2 = xy-3y$, so $x-xy = -3y-2$, so $xy-x = 3y+2$, so $x(y-1) = 3y+2$. But then $y \neq 1$, because if y were equal to 1, then from the equation $x(y-1) = 3y+2$ we would get we would get the false statement $0 = 5$. Since $y \neq 1$, we can divide by $y-1$ in the equation $x(y-1) = 3y+2$, to get $x = (3y+2)/(y-1)$. We have shown that if $x \in \mathbf{R} \setminus \{3\}$ and $f(x) = y$, then $y \in \mathbf{R} \setminus \{1\}$ and $x = (3y+2)/(y-1)$. Now let us show the converse. Suppose $y \in \mathbf{R} \setminus \{1\}$ and $x = (3y+2)/(y-1)$. Then $x(y-1) = 3y+2$, so $xy-x = 3y+2$, so $xy-3y = x+2$, so $(x-3)y = x+2$. But then $x \neq 3$, because if x were equal to 3, then from the equation $(x-3)y = x+2$ we would get the false statement $0 = 5$. Since $x \neq 3$, we can divide by $x-3$ in the equation $(x-3)y = x+2$, to get $y = (x+2)/(x-3)$, so $y = f(x)$. Thus $x \in \mathbf{R} \setminus \{3\}$ and $f(x) = y$. This completes the proof of the converse. Now x and y are arbitrary. Therefore for all x and all y, we have $x \in \mathbf{R} \setminus 3$ and $f(x) = y$ iff $y \in \mathbf{R} \setminus \{1\}$ and $x = (3y+2)/(y-1)$. Hence by Theorem 11.63, f is a bijection from $\mathbf{R} \setminus \{3\}$ to $\mathbf{R} \setminus \{1\}$ and f^{-1} is the function g from $\mathbf{R} \setminus \{1\}$ to $\mathbf{R} \setminus \{3\}$ defined by $g(y) = (3y+2)/(y-1)$ for all $\mathbf{R} \setminus \{1\}$. The range of f is $\mathbf{R} \setminus \{1\}$.

Exercise 24. Sketch the graph of the function f in Example 11.67.

11.68 Example. It is not always a simple matter to find the inverse of a given injective function f. Sometimes it may be so difficult that even the most powerful computers cannot do it within a reasonable amount of time. While you might think at first that this is unfortunate, it can actually be quite useful. It is the basis for what are called *public-key encryption schemes*. These are coding schemes in which you can tell everybody how to encode messages to send to you, but in which your having publicized the encoding method does not help people to decode messages intended for you. The encoding method may be thought of as a one-to-one function f whose inverse f^{-1} is the method of decoding. If f is easy to compute but only you know how to compute f^{-1}, then no one else will be able to decode messages intended for you even though you have told everybody how to encode messages to you. To find such an encoding function f is a nice application of some advanced mathematics, but we shall not go into details about it here.[13]

11.69 Example. Let $f(x) = x^2$ for all $x \in \mathbf{R}$ and let $g(y) = \sqrt{y}$ for all $y \in [0,\infty)$. Since $f(-x) = f(x)$ for all $x \in \mathbf{R}$, the function f is not an injection, so it does not have an inverse function. However $f \restriction [0,\infty)$, the restriction of f to the interval $[0,\infty)$, is an injection and hence does have an inverse function. In fact, the inverse function for $f \restriction [0,\infty)$ is g; in other words, $(f \restriction [0,\infty))^{-1} = g$.

11.70 Example. Let $f(x) = x^3$ for all $x \in \mathbf{R}$ and let $g(y) = \sqrt[3]{y}$ for all $y \in \mathbf{R}$. Then f is an injection, so f has an inverse function. In fact, the inverse function for f is g; in other words, $f^{-1} = g$.

11.71 Example. Let $f(\theta) = \sin\theta$ for all $\theta \in \mathbf{R}$ and let $g(y) = \arcsin y$ for all $y \in [-1,1]$. Then f is not an injection because $f(\theta + 2\pi) = f(\theta)$ for all $\theta \in \mathbf{R}$. However $f \restriction [-\pi/2, \pi/2]$, the restriction of f to the interval $[-\pi/2, \pi/2]$, is an injection and hence does have an inverse function. In fact, the inverse function for $f \restriction [-\pi/2, \pi/2]$ is g. In other words, $(\sin \restriction [-\pi/2, \pi/2])^{-1} = \arcsin$.

Exercise 25. For each of the following functions, state whether it is an injection. If it is an injection, determine its inverse function. If it is not an injection, find an interval such that the restriction of the function to that interval is an injection whose inverse function has a standard name, and determine that inverse function.

(a) $f(x) = 10^x$ for all $x \in \mathbf{R}$.

(b) $f(x) = e^x$ for all $x \in \mathbf{R}$.

(c) $f(\theta) = \cos\theta$ for all $\theta \in \mathbf{R}$.

[13] If you are curious about public-key encryption, you might enjoy reading the article about it by Martin E. Helman in *Scientific American*, August, 1979, pages 146–157.

(d) $f(\theta) = \sin\theta/\cos\theta$ for all $\theta \in \mathbf{R}$ such that $\cos\theta \neq 0$. (In this part, you should also find a more explicit description of the domain of f).

The next result tells us that if f and g are injections, then to undo what $g \circ f$ does, one should first undo what g does and then undo what f does. This makes sense, because $g \circ f$ applies the operation g to the result of the operation f, and to undo this one must undo the last operation first.

11.72 Theorem. *Let f and g be injections. Then $g \circ f$ is an injection and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Proof. Let $h = g \circ f$ and let $A = \mathrm{Dom}(h)$. Then $A = \{\, x \in \mathrm{Dom}(f) : f(x) \in \mathrm{Dom}(g) \,\}$. Also let $k = f^{-1} \circ g^{-1}$ and let $B = \mathrm{Dom}(k)$. Then $B = \{\, y \in \mathrm{Dom}(g^{-1}) : g^{-1}(y) \in \mathrm{Dom}(f^{-1}) \,\}$. To prove what we want, it suffices to show that h is a bijection from A to B and $k = h^{-1}$. To show this, by Theorem 11.63 it suffices to show that for all x and y, we have $x \in A$ and $h(x) = y$ iff $y \in B$ and $x = k(y)$. Consider any x and y. Suppose $x \in A$ and $h(x) = y$. Then $x \in \mathrm{Dom}(f)$, $f(x) \in \mathrm{Dom}(g)$, and $g(f(x)) = y$. Since $f(x) \in \mathrm{Dom}(g)$ and $g(f(x)) = y$, we have $y \in \mathrm{Dom}(g^{-1})$ and $f(x) = g^{-1}(y)$. Since $x \in \mathrm{Dom}(f)$ and $f(x) = g^{-1}(y)$, we have $g^{-1}(y) \in \mathrm{Dom}(f^{-1})$ and $x = f^{-1}(g^{-1}(y))$. Since $y \in \mathrm{Dom}(g^{-1})$, $g^{-1}(y) \in \mathrm{Dom}(f^{-1})$, and $x = f^{-1}(g^{-1}(y))$, we have $y \in \mathrm{Dom}(f^{-1} \circ g^{-1})$ and $x = (f^{-1} \circ g^{-1})(y)$. In other words, $y \in B$ and $x = k(y)$. Conversely, suppose $y \in B$ and $x = k(y)$. Then $y \in \mathrm{Dom}(g^{-1})$, $g^{-1}(y) \in \mathrm{Dom}(f^{-1})$, and $x = f^{-1}(g^{-1}(y))$. Since $g^{-1}(y) \in \mathrm{Dom}(f^{-1})$ and $x = f^{-1}(g^{-1}(y))$, we have $x \in \mathrm{Dom}(f)$ and $f(x) = g^{-1}(y)$. Since $y \in \mathrm{Dom}(g^{-1})$ and $f(x) = g^{-1}(y)$, we have $f(x) \in \mathrm{Dom}(g)$ and $g(f(x)) = y$. Since $x \in \mathrm{Dom}(f)$, $f(x) \in \mathrm{Dom}(g)$, and $g(f(x)) = y$, we have $x \in \mathrm{Dom}(g \circ f)$ and $(g \circ f)(x) = y$. In other words, $x \in A$ and $h(x) = y$. Thus for all x and y, we have $x \in A$ and $h(x) = y$ iff $y \in B$ and $x = k(y)$, as desired. ■

Exercise 26. Let A, B, and C be sets, let f be a bijection from A to B, and let g be a bijection from B to C. Prove that $g \circ f$ is a bijection from A to C.

Exercise 27. In this exercise, you are asked to work through an alternative approach to part (a) of Exercise 20. (In fact, the approach outlined here is the way I made up Exercise 20(a).) Let $g_1(x) = 1 - x$ for all $x \in [0, 1)$, let $g_2(s) = 1/s$ for all $s \in (0, 1]$, let $g_3(t) = t - 1$ for all $t \in [1, \infty)$, and let $g(x) = x/(1 - x)$ for all $x \in [0, 1)$.

(a) Verify that $g_3 \circ g_2 \circ g_1 = g$.

(b) Use the result of Exercise 26, together with earlier examples and exercises (but not Exercise 20), to show that g is a bijection from $[0, 1)$ to $[0, \infty)$.

(c) Use Theorem 11.72, together with earlier examples and exercises, to find g^{-1}.

Exercise 28. Work out an alternative approach to part (b) of Exercise 20 along the lines of Exercise 27.

In terms of identity functions and composition of functions, Theorem 11.63 can be reformulated as follows.

11.73 Theorem. *Let A and B be sets, let f be a function whose domain is A, and let g be a function whose domain is B. Let id_A and id_B be the identity functions on A and B respectively. Then the following are equivalent.*

(a) *f is a bijection from A to B and $g = f^{-1}$.*

(b) *$g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$.*

(c) *g is a bijection from B to A and $f = g^{-1}$.*

Proof. We already know that (a) and (c) are equivalent, by Theorem 11.63. Hence we have only to show that (a) and (b) are equivalent.

(a)⇒(b): Suppose f is a bijection from A to B and $g = f^{-1}$. Then by Theorem 11.63, for all x and all y, we have $x \in A$ and $f(x) = y$ iff $y \in B$ and $x = g(y)$. Consider any $x \in A$. Let $y = f(x)$. Then $y \in B$. Also $x = g(y)$. That is, $x = g(f(x))$. In other words, $\mathrm{id}_A(x) = (g \circ f)(x)$. This holds for each $x \in A$. Hence $\mathrm{id}_A = g \circ f$. Similarly, for each $y \in B$, $\mathrm{id}_B(y) = (f \circ g)(y)$. Hence $\mathrm{id}_B = f \circ g$.

(b)⇒(a): Suppose $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$. By Theorem 11.63, to prove (a), it suffices to show that for all x and all y, we have $x \in A$ and $f(x) = y$ iff $y \in B$ and $x = g(y)$. Consider any x and any y. Suppose $x \in A$ and $f(x) = y$. Since $g \circ f = \mathrm{id}_A$, we have $x \in \mathrm{Dom}(g \circ f)$ and $(g \circ f)(x) = x$. Hence $f(x) \in \mathrm{Dom}(g)$ and $g(f(x)) = x$. But $f(x) = y$ and $\mathrm{Dom}(g) = B$. Hence $y \in B$ and $x = g(y)$. Conversely,

suppose $y \in B$ and $x = g(y)$. Then by a similar argument, using $f \circ g = \mathrm{id}_B$ and $\mathrm{Dom}(f) = A$, one can show that $x \in A$ and $f(x) = y$. ■

Still More Examples of Functions: Sequences and Indexed Families.

11.74 Finite Sequences. Let $n \in \mathbf{N}$. Then given objects $a_1, \ldots, a_n$, the notation $\langle a_1, \ldots, a_n \rangle$ stands for the function f such that the domain of f is $\{1, \ldots, n\}$ and such that $f(1) = a_1, \ldots, f(n) = a_n$. Such a function is called *a sequence of length n* or more briefly *an n-sequence*. The objects $a_1, \ldots, a_n$ are called the *terms* of the sequence. The set $\{a_1, \ldots, a_n\}$ is not the sequence $f = \langle a_1, \ldots, a_n \rangle$, it is the range of f. In such a sequence, the order of the terms matters, the terms need not all be distinct,[14] and repetitions count.[15] In contrast, all that matters about a set, such as $\{a_1, \ldots, a_n\}$, is which objects belong to it, not the order in which these objects happen to be listed in a particular description of the set, nor whether some of these objects are listed more than once. Thus $\{3, 5\}$, $\{5, 3\}$ and $\{5, 3, 5\}$ all stand for the same set but $\langle 3, 5 \rangle$, $\langle 5, 3 \rangle$ and $\langle 5, 3, 5 \rangle$ all stand for different sequences.

Note that we write $\langle a_1, \ldots, a_n \rangle$ for the n-sequence whose terms are $a_1, \ldots, a_n$, whereas we write $(a_1, \ldots, a_n)$ for the ordered n-tuple whose entries are $a_1, \ldots, a_n$. In other words, we use angle brackets "⟨" and "⟩" for n-sequences but we use parentheses "(" and ")" for ordered n-tuples. Ordered n-tuples and n-sequences are similar in some ways. For instance, if $\langle a_1, \ldots, a_n \rangle = \langle a'_1, \ldots, a'_n \rangle$, then $a_1 = a'_1$, ..., $a_n = a'_n$, and likewise for ordered n-tuples. However notice that if an n-sequence is equal to an n'-sequence, then $n = n'$, whereas an ordered n-tuple can be equal to an ordered n'-tuple without n being equal to n'. For instance, the ordered triple (a, b, c) is equal to the ordered pair $((a, b), c)$ by the definition of ordered triples. In this respect n-sequences are better than ordered n-tuples as a mathematical representation of ordered lists.

The empty function is a sequence of length 0. A *finite sequence* is a sequence of length n for some $n \in \boldsymbol{\omega}$.

11.75 Infinite Sequences. A function f whose domain is the set $\mathbf{N}$ of natural numbers is called *an infinite sequence*, or just *a sequence* if no confusion with finite sequences is likely. The values $a_1 = f(1)$, $a_2 = f(2)$, $a_3 = f(3)$, and so on, of such a function f are called the terms of the sequence. The notation $\langle a_1, a_2, a_3, \ldots \rangle$ is an alternative notation for the sequence f. This is often abbreviated as $\langle a_n \rangle_{n \in \mathbf{N}}$ or even simply $\langle a_n \rangle$. Thus for instance, $\langle 1, 1/2, 1/3, 1/4, \ldots \rangle$, $\langle 1/n \rangle_{n \in \mathbf{N}}$, and $\langle 1/n \rangle$ all denote the sequence that is the function f defined by $f(n) = 1/n$ for all $n \in \mathbf{N}$. The set $\{a_1, a_2, a_3, \ldots\}$ is not the sequence $f = \langle a_1, a_2, a_3, \ldots \rangle$, it is the range of f.

Just as for finite sequences, it follows from the meaning of equality for functions that the order of the terms in a sequence matters and that repetitions count. Thus the sequence $\langle (-1)^{n+1} \rangle = \langle 1, -1, 1, -1, \ldots \rangle$ is not equal to the sequence $\langle (-1)^n \rangle = \langle -1, 1, -1, 1, \ldots \rangle$. Contrast this with what we know for sets, where order and repetitions are immaterial: the set $\{(-1)^{n+1} : n \in \mathbf{N}\} = \{1, -1, 1, -1, \ldots\}$ is just $\{1, -1\} = \{-1, 1\}$ and this is the same as $\{(-1)^n : n \in \mathbf{N}\} = \{-1, 1, -1, 1, \ldots\}$.

11.76 Sequences in a Given Set. If A is a set, then a sequence whose terms are elements of A is called *a sequence consisting of elements of A*, or more briefly *a sequence of elements of A*, or still more briefly *a sequence in A*. This terminology applies to finite sequences as well as to infinite sequences.

11.77 Indexed Families. An *indexed family* $\langle y_\alpha \rangle_{\alpha \in A}$ is just a function whose domain is the set A and whose value at each α in A is y_α. The set A is called the *index set* of the indexed family $\langle y_\alpha \rangle_{\alpha \in A}$. In the notation $\langle y_\alpha \rangle_{\alpha \in A}$ for an indexed family, the variable α is a dummy variable, so for instance $\langle y_i \rangle_{i \in A}$ stands for the same indexed family as $\langle y_\alpha \rangle_{\alpha \in A}$. Sometimes an indexed family $\langle y_\alpha \rangle_{\alpha \in A}$ is called *a family indexed by A* or even just *a family*.

Notice that an infinite sequence is an indexed family whose index set is $\mathbf{N}$, the set of natural numbers. Similarly, if $n \in \mathbf{N}$, then a sequence of length n is an indexed family whose index set is the set $\{1, \ldots, n\}$. Thus an n-sequence $\langle a_1, \ldots, a_n \rangle$ may also be written $\langle a_k \rangle_{k \in \{1, \ldots, n\}}$. However, this is not common.

---

[14] Given an n-sequence $f = \langle a_1, \ldots, a_n \rangle$, its terms $a_1, \ldots, a_n$ are distinct exactly when f is one-to-one. Indeed, this essentially defines what we mean when we say that $a_1, \ldots, a_n$ are distinct.

[15] Recall that two functions f and f' are equal iff f and f' have the same domain, say D, and for each $x \in D$, $f(x) = f'(x)$. Hence an n-sequence $\langle a_1, \ldots, a_n \rangle$ is equal to an n'-sequence $\langle a'_1, \ldots, a'_{n'} \rangle$ iff $n = n'$ and $a_1 = a'_1, \ldots, a_n = a'_n$.

An indexed family $\langle y_\alpha \rangle_{\alpha \in A}$ is not the same as the set $\{ y_\alpha : \alpha \in A \}$. The indexed family is a function and the set $\{ y_\alpha : \alpha \in A \}$ is the range of this function.

Given any set A, there is an indexed family whose range is A. For instance, if $y_\alpha = \alpha$ for all $\alpha \in A$, then the indexed family $\langle y_\alpha \rangle_{\alpha \in A}$ is such an indexed family. Note that this indexed family is none other than the identity function on A.

Section 12. More About Functions

Functions as Sets of Ordered Pairs.

12.1 Definition. Let f be a function. The *graph of* f (denoted $\text{Graph}(f)$) is the set of all ordered pairs (x, y) such that x is in the domain of f and $y = f(x)$; in other words,

$$\begin{aligned} \text{Graph}(f) &= \{ (x, y) : x \in \text{Dom}(f) \text{ and } y = f(x) \} \\ &= \{ (x, f(x)) : x \in \text{Dom}(f) \}. \end{aligned}$$

12.2 Example. For each x in the interval $[-1, 1]$, let $f(x) = (1 - x^2)^{1/2}$. If we think of the x-axis as horizontal and the y-axis as vertical, then $\text{Graph}(f)$ is the upper half of the circle with center $(0, 0)$ and radius 1.

12.3 Example. Let A be the set of all ordered pairs (x, y) in $\mathbf{R}^2$ such that $x^2 + y^2 \leq 9$ and let $f(x, y) = [9 - (x^2 + y^2)]^{1/2}$ for all $(x, y) \in A$. Notice that A consists of the boundary and interior of the circle in the xy-plane with center $(0, 0)$ and radius 3. If we think of the xy-plane as horizontal and the z-axis as vertical, then $\text{Graph}(f) = \{ (x, y, z) : (x, y) \in A \text{ and } z = f(x, y) \}$ is the upper half of the sphere with center $(0, 0, 0)$ and radius 3.

12.4 Example. Suppose $S = \{ a, b, c \}$ where a, b, and c are distinct. Suppose $T = \{ u, v, w \}$. Let f be the function from S to T defined by $f(a) = u$, $f(b) = v$, and $f(c) = w$. Then the graph of f does not have an obvious geometrical description. Nevertheless, the definition of $\text{Graph}(f)$ still applies. We have

$$\text{Graph}(f) = \{ (a, u), (b, v), (c, w) \}.$$

12.5 Example. If f is the empty function, then the domain of f is the empty set, so the graph of f is also the empty set. Conversely, if f is a function whose graph is the empty set, then the domain of f is the empty set, so f is the empty function.

Exercise 1. Let A and B be sets and let $f \colon A \to B$. Show that $\text{Graph}(f) \subseteq A \times B$.

12.6 Proposition. *Let f be a function. Then*

(a) *For each x, there exists at most one y such that $(x, y) \in \text{Graph}(f)$.*
(b) $\text{Dom}(f) = \{ x : \text{there exists } y \text{ such that } (x, y) \in \text{Graph}(f) \}$.
(c) *For each $x \in \text{Dom}(f)$, $f(x)$ is the unique y such that $(x, y) \in \text{Graph}(f)$.*
(d) $\text{Rng}(f) = \{ y : \text{there exists } x \text{ such that } (x, y) \in \text{Graph}(f) \}$.

Proof. (a) Consider any x. We wish to show that there exists at most one y such that $(x, y) \in \text{Graph}(f)$. To show this, we consider any y_1 and any y_2 such that $(x, y_1) \in \text{Graph}(f)$ and $(x, y_2) \in \text{Graph}(f)$, and we show that $y_1 = y_2$. Since $(x, y_1) \in \text{Graph}(f)$, we have $x \in \text{Dom}(f)$ and $y_1 = f(x)$. Since $(x, y_2) \in \text{Graph}(f)$, we have $y_2 = f(x)$. Thus y_1 and y_2 are both equal to $f(x)$. Hence $y_1 = y_2$, as desired.

(b) To save writing, let $R = \{ x : \text{there exists } y \text{ such that } (x, y) \in \text{Graph}(f) \}$. We wish to show that $\text{Dom}(f) = R$. Suppose $x \in \text{Dom}(f)$. Let $y = f(x)$. Then $(x, y) \in \text{Graph}(f)$. Hence $x \in R$. This shows that $\text{Dom}(f) \subseteq (R)$. Now suppose $x \in R$. Then there exists y such that $(x, y) \in \text{Graph}(f)$. Since $(x, y) \in \text{Graph}(f)$, we have $x \in \text{Dom}(f)$ and $y = f(x)$. In particular, $x \in \text{Dom}(f)$. This shows that $R \subseteq \text{Dom}(f)$. Since $\text{Dom}(f) \subseteq R$ and $R \subseteq \text{Dom}(f)$, we have $\text{Dom}(f) = R$, as desired.

(c) Consider any $x \in \text{Dom}(f)$. Then for each y, we have $(x, y) \in \text{Graph}(f)$ iff $y = f(x)$. Thus $f(x)$ is the unique y such that $(x, y) \in \text{Graph}(f)$.

(d) To save writing, let $R = \{\, y : \text{there exists } x \text{ such that } (x,y) \in \text{Graph}(f) \,\}$. We wish to show that $\text{Rng}(f) = R$. Suppose $y \in \text{Rng}(f)$. Then $y = f(x)$ for some $x \in \text{Dom}(f)$. But then $(x,y) \in \text{Graph}(f)$. Hence $y \in R$. This shows that $\text{Rng}(f) \subseteq R$. Now suppose $y \in R$. Then there exists x such that $(x,y) \in \text{Graph}(f)$. Since $(x,y) \in \text{Graph}(f)$, we have $x \in \text{Dom}(f)$ and $y = f(x)$. Thus $y \in \text{Rng}(f)$. This shows that $R \subseteq \text{Rng}(f)$. Since $\text{Rng}(f) \subseteq R$ and $R \subseteq \text{Rng}(f)$, we have $R = \text{Rng}(f)$, as desired. ■

12.7 Theorem. *Let f and g be functions. Then $f = g$ iff $\text{Graph}(f) = \text{Graph}(g)$.*

Proof. If $f = g$, then $\text{Graph}(f) = \text{Graph}(g)$, because equals may be substituted for equals. Conversely, suppose $\text{Graph}(f) = \text{Graph}(g)$. Consider any $x \in \text{Dom}(f)$. Let $y = f(x)$. Then $(x,y) \in \text{Graph}(f)$, so $(x,y) \in \text{Graph}(g)$, so $x \in \text{Dom}(g)$ and $y = g(x)$. Since $f(x)$ and $g(x)$ are both equal to y, $f(x) = g(x)$. Thus $\text{Dom}(f) \subseteq \text{Dom}(g)$ and for each $x \in \text{Dom}(f)$, $f(x) = g(x)$. Similarly, $\text{Dom}(g) \subseteq \text{Dom}(f)$ and for each $x \in \text{Dom}(g)$, $g(x) = f(x)$. Hence f and g have the same domain and they agree at all points in their domain, so $f = g$. ■

From the preceding result, we see that the graph of a function tells us everything about the function. The next result tells us when a given set is the graph of a function.

12.8 Theorem. *Let S be a set. Then S is the graph of a function iff S is a set of ordered pairs and for each x, there exists at most one y such that $(x,y) \in S$.*

Proof. Suppose S is the graph of a function. Then there exists a function f such that $S = \text{Graph}(f)$. Then obviously S is a set of ordered pairs and by Proposition 12.6, for each x, there exists at most one y such that $(x,y) \in S$. This proves the forward implication.

Conversely, suppose S is a set of ordered pairs and for each x, there exists at most one y such that $(x,y) \in S$. Let $A = \{\, x : \text{there exists } y \text{ such that } (x,y) \in S \,\}$. Then for each $x \in A$, there exists a unique y such that $(x,y) \in S$. Hence we can define a function f, with domain A, by letting $f(x)$ be the unique y such that $(x,y) \in S$, for all $x \in A$. Then S is the graph of the function f, because for all x and y, we have $(x,y) \in \text{Graph}(f)$ iff $x \in A$ and $y = f(x)$ iff $x \in A$ and $(x,y) \in S$ iff $(x,y) \in S$. This proves the reverse implication. ■

12.9 Remark. Recall that the Cartesian plane is $\mathbf{R}^2 = \{\, (x,y) : x \in \mathbf{R} \text{ and } y \in \mathbf{R} \,\}$. In the special case where S is a subset of $\mathbf{R}^2$, then the preceding result tells us that S is the graph of a function iff for each $x \in \mathbf{R}$, the intersection of S with the "vertical line" $\{\, (x,y) : y \in \mathbf{R} \,\}$ consists of at most one point. This is the so-called *vertical line test* for a subset of $\mathbf{R}^2$ to be the graph of a function. Note that by Proposition 12.6, the domain of such a function is a subset of $\mathbf{R}$.

12.10 Remark. Since the graph of a function tells us everything about the function, and since we know when a set is the graph of a function, it is possible to regard a function as being its graph. If one adopts this point of view, then one may define a function to be a set f of ordered pairs such that for each x, there exists at most one y such that $(x,y) \in f$. (Note that if one adopts this definition, then for each function f, we have $\text{Graph}(f) = f$, so for instance the empty function is the same thing as the empty set.) In this way, the concept of function may be reduced to a special case of the concept of set. (Remember that we have already seen that ordered pairs can be defined as sets.) We do not wish to insist on this point of view here. We only wish to point out that it is possible.

12.11 Remark. An indexed family $\langle\, y_\alpha \,\rangle_{\alpha \in A}$ is the function whose graph is $\{\, (\alpha, y_\alpha) : \alpha \in A \,\}$. If we adopt the point of view that a function is the same thing as its graph, as outlined in Remark 12.10, then the distinction between such an indexed family $\langle\, y_\alpha \,\rangle_{\alpha \in A}$ and the set $\{\, y_\alpha : \alpha \in A \,\}$, which is the range of this function, can be expressed quite vividly, for then $\langle\, y_\alpha \,\rangle_{\alpha \in A} = \{\, (\alpha, y_\alpha) : \alpha \in A \,\}$, not $\{\, y_\alpha : \alpha \in A \,\}$.

The next result describes how to tell from its graph whether a function is an injection and if it is, how to find the graph of the inverse function from the graph of the original function.

12.12 Theorem. *Let f be a function, let $S = \text{Graph}(f)$, and let $S^{-1} = \{\, (y,x) : (x,y) \in S \,\}$. Then f is an injection iff S^{-1} is the graph of a function. In this case, S^{-1} is the graph of f^{-1}, the inverse function for f.*

Proof. Suppose f is an injection. Then f has an inverse function f^{-1}. We shall show that $S^{-1} = \text{Graph}(f^{-1})$. Consider any x and any y. Then $x \in \text{Dom}(f)$ and $y = f(x)$ iff $y \in \text{Dom}(f^{-1})$ and

$x = f^{-1}(y)$, by Theorem 11.63 (with $A = \mathrm{Dom}(f)$, $g = f^{-1}$, and $B = \mathrm{Dom}(g)$). But $(x, y) \in \mathrm{Graph}(f)$ iff $x \in \mathrm{Dom}(f)$ and $y = f(x)$. Likewise, $(y, x) \in \mathrm{Graph}(f^{-1})$ iff $y \in \mathrm{Dom}(f^{-1})$ and $x = f^{-1}(y)$. Combining these three equivalences, we see that $(y, x) \in \mathrm{Graph}(f^{-1})$ iff $(x, y) \in \mathrm{Graph}(f)$. In other words, $(y, x) \in \mathrm{Graph}(f^{-1})$ iff $(x, y) \in S$. But by the definition of S^{-1}, we have $(x, y) \in S$ iff $(y, x) \in S^{-1}$. Hence $(y, x) \in \mathrm{Graph}(f^{-1})$ iff $(y, x) \in S^{-1}$. Since this holds for all x and all y, and since $\mathrm{Graph}(f^{-1})$ and S^{-1} are sets of ordered pairs, we see that $\mathrm{Graph}(f^{-1})$ and S^{-1} have the same elements, so they are one and the same set, as was to be shown.

Conversely, suppose S^{-1} is the graph of a function. We wish to show that f is an injection. Since S^{-1} is the graph of a function, for each y, there exists at most one x such that $(y, x) \in S^{-1}$, by Proposition 12.6. Hence, by the definition of S^{-1}, for each y, there exists at most one x such that $(x, y) \in S$. Since S is the graph of f, this means that for each y, there exists at most one x such that $x \in \mathrm{Dom}(f)$ and $y = f(x)$. Hence f is an injection, as was to be shown. ■

Exercise 2. Let $f(x) = x/(x-1)$ for all $x \in \mathbf{R} \setminus \{1\}$. Find $\mathrm{Rng}(f)$ and f^{-1}. Explain why your answer implies that the graph of f is symmetric about the line $y = x$.

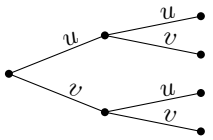
The Set of all Functions from a Set to another Set.

12.13 Definition. Let A and B be sets. Then B^A denotes the set of all functions from A to B; in other words,

$$B^A = \{ f : f \text{ is a function from } A \text{ to } B \}.$$

12.14 Remark. As you know, the notation B^A is also used to denote a number B raised to the power of a number A. You should be able to infer from the context which meaning B^A has.

12.15 Example. Let $A = \{1, 2\}$ and let $B = \{u, v\}$ where u and v are distinct. We can represent the set B^A of all functions from A to B by drawing a *tree diagram*, as follows:



Each path from the leftmost node to one of the rightmost nodes in this tree diagram represents one of the functions from A to B, and since u and v are distinct, each function from A to B is represented by exactly one such path. Since there are $2 \cdot 2 = 4$ such paths, there are 4 such functions. These 4 functions are the following 4 sequences of length 2:

$$\langle u, u \rangle,\ \langle u, v \rangle,\ \langle v, u \rangle,\ \langle v, v \rangle.$$

The reason why the elements of B^A turn out to be sequences of length 2 in this example is that the set A is the set $\{1, 2\}$. As we know, a sequence of length 2 is a function whose domain is the set $\{1, 2\}$.

Exercise 3. In Example 12.15, which of the elements of B^A are injections? Draw a tree diagram to represent just these elements of B^A.

Exercise 4. Robert, Susan, and Thomas are the sole contestants in a lottery in which two prizes will be awarded. Three tickets with their names on them are placed in a hat. The person whose name is on the first ticket drawn wins first prize. That ticket is then replaced in the hat. Then a second ticket is drawn from the hat and the person whose name is on it wins second prize. (Thus it is possible that the same person will win both prizes.) Let $A = \{1, 2\}$ and let $B = \{r, s, t\}$, where $r = \text{Robert}$, $s = \text{Susan}$, and $t = \text{Thomas}$.

- **(a)** Explain how each possible assignment of prizes to contestants may be thought of as a function from A to B and why B^A may be thought of as representing the set of all such possible assignments.
- **(b)** Draw a tree diagram to represent the set B^A. Then list all the elements of B^A, using the notation for sequences of length 2. How many such elements are there?
- **(c)** Which elements of B^A are injections? Draw a tree diagram to represent just these elements. Then list them all.
- **(d)** In terms of assignments of prizes in the lottery, what does it mean to say that an element of B^A is an injection?

Exercise 5. Let $A = \{ 1, 2, 3 \}$ and let $B = \{ x, y \}$ where x and y are distinct. Draw a tree diagram to represent the set B^A. Then list all the elements of B^A using the notation for sequences of length 3. How many such elements are there? Are any of them are injections?

12.16 Remark. Let $n \in \mathbf{N}$ and let B be a set. Then $B^{\{1,2,\ldots,n\}}$ is the set of all n-sequences of elements of B. In other words,

$$B^{\{1,2,\ldots,n\}} = \big\{ \langle y_1, y_2, \ldots, y_n \rangle : y_1 \in B,\, y_2 \in B, \ldots,\, y_n \in B \big\}.$$

Let us compare this with B^n. Recall that B^n denotes the Cartesian product of B with itself n times, which is the set of all ordered n-tuples of elements of B. In other words,

$$\begin{aligned} B^n &= \overbrace{B \times B \times \cdots \times B}^{n \text{ times}} \\ &= \big\{ (y_1, y_2, \ldots, y_n) : y_1 \in B,\, y_2 \in B, \ldots,\, y_n \in B \big\}. \end{aligned}$$

Now $B^{\{1,2,\ldots,n\}}$ is not literally the same thing as B^n. (The former is a set of n-sequences and the latter is a set of ordered n-tuples.) However there is a natural one-to-one correspondence between $B^{\{1,2,\ldots,n\}}$ and B^n. Specifically, if we let

$$\Phi(\langle y_1, y_2, \ldots, y_n \rangle) = (y_1, y_2, \ldots, y_n)$$

for all $y_1, y_2, \ldots, y_n \in B$, then Φ is a bijection from $B^{\{1,2,\ldots,n\}}$ to B^n.

12.17 Example. Let B be a set. Then $B^{\varnothing}$, the set of all functions from the empty set to B, is not empty. Rather, $B^{\varnothing}$ has one element, namely the empty function. If we think of a function as being the same thing as its graph, so that the empty function is the same thing as the empty set, then $B^{\varnothing} = \{ \varnothing \}$.

Exercise 6. What is $\varnothing^{\varnothing}$? If A is a nonempty set, what is $\varnothing^A$?

12.18 Remark. Let B be a set. Then $B^{\mathbf{N}}$, the set of all functions from $\mathbf{N}$ to B, is the set of all (infinite) sequences of elements of B; in other words,

$$\begin{aligned} B^{\mathbf{N}} &= \{ f : f \text{ is a function from } \mathbf{N} \text{ to } B \} \\ &= \big\{ \langle y_1, y_2, y_3, \ldots \rangle : y_n \in B \text{ for all } n \in \mathbf{N} \big\}. \end{aligned}$$

12.19 Example. Each real number x in the interval $[0, 1)$ has a unique decimal expansion not ending in repeating 9's. This is called the standard decimal expansion[16] of x. For instance, $1/2 = 0.5000\ldots$, $1/6 = 0.1666\ldots$, and $\sqrt{2} - 1 = 0.414213562\ldots$. For each $k \in \mathbf{N}$, for each $x \in [0, 1)$, let $a_k(x)$ be the k-th digit after the decimal point in the standard decimal expansion of x. Then for each $k \in \mathbf{N}$, a_k is a function from $[0, 1)$ to $D = \{ 0, 1, \ldots, 9 \}$, the set of decimal digits. For instance, from the decimal expansion of $\sqrt{2} - 1$ that is shown above, we see that $a_6(\sqrt{2} - 1) = 3$. Next, for each $x \in [0, 1)$, let

$$f(x) = \langle a_1(x), a_2(x), a_3(x), \ldots \rangle.$$

In other words, for each $x \in [0, 1)$, let $f(x)$ be the sequence of the digits after the decimal place in the standard decimal expansion of x. Then f is a function from $[0, 1)$ to $D^{\mathbf{N}}$, the set of infinite sequences of decimal digits. For instance,

$$f(\sqrt{2} - 1) = \langle 4, 1, 4, 2, 1, 3, 6, \ldots \rangle.$$

Since different numbers have different decimal expansions, f is an injection from $[0, 1)$ to $D^{\mathbf{N}}$. However, f is not a surjection from $[0, 1)$ to $D^{\mathbf{N}}$. Instead, the range of f is the set of infinite sequences in D that do not end in repeating 9's. For now we content ourselves with just stating these facts about decimal expansions. We shall review the reasons for them later.

Exercise 7. Let A and B be sets. Show that if we regard each function as being the same thing as its graph, then $B^A \subseteq \mathscr{P}(A \times B)$.

[16] Some numbers have two decimal expansions, a standard one ending in repeating 0's and an alternative one ending in repeating 9's. For instance, $1/2$ has the alternative decimal expansion $1/2 = 0.4999\ldots$. The numbers in $[0, 1)$ that have two decimal expansions are the ones of the form $m/10^n$ where $n \in \mathbf{N}$ and $m \in \{ 1, 2, \ldots, 10^n - 1 \}$. All other numbers in $[0, 1)$ have just one decimal expansion.

Indexed Families of Sets.

An *indexed family of sets* $\langle B_\alpha \rangle_{\alpha\in A}$ is an indexed family such that B_α is a set for each $\alpha \in A$. The *union* of an indexed family of sets $\langle B_\alpha \rangle_{\alpha\in A}$ is

$$\bigcup_{\alpha\in A} B_\alpha = \{\, x : x \in B_\alpha \text{ for some } \alpha \in A \,\}$$

and if $A \neq \emptyset$, the *intersection* of such an indexed family of sets is

$$\bigcap_{\alpha\in A} B_\alpha = \{\, x : x \in B_\alpha \text{ for each } \alpha \in A \,\}.$$

Although the indexed family of sets $\langle B_\alpha \rangle_{\alpha\in A}$ is not the same thing[17] as the set of sets $\{\, B_\alpha : \alpha \in A \,\}$, it has the same union and intersection as this set of sets:

$$\bigcup_{\alpha\in A} B_\alpha = \bigcup \{\, B_\alpha : \alpha \in A \,\}$$

and if $A \neq \emptyset$,

$$\bigcap_{\alpha\in A} B_\alpha = \bigcap \{\, B_\alpha : \alpha \in A \,\}.$$

Note that if $\alpha_0 \in A$, then

$$\bigcap_{\alpha\in A} B_\alpha \subseteq B_{\alpha_0} \subseteq \bigcup_{\alpha\in A} B_\alpha.$$

Given a set S and an indexed family of sets $\langle B_\alpha \rangle_{\alpha\in A}$, where A is nonempty, it is not difficult to verify the generalized De Morgan's laws

$$S \setminus \bigcup_{\alpha\in A} B_\alpha = \bigcap_{\alpha\in A} (S \setminus B_\alpha),$$

$$S \setminus \bigcap_{\alpha\in A} B_\alpha = \bigcup_{\alpha\in A} (S \setminus B_\alpha),$$

the generalized distributive laws

$$S \cap \bigcup_{\alpha\in A} B_\alpha = \bigcup_{\alpha\in A} (S \cap B_\alpha),$$

$$S \cup \bigcap_{\alpha\in A} B_\alpha = \bigcap_{\alpha\in A} (S \cup B_\alpha),$$

and also the relations

$$S \cup \bigcup_{\alpha\in A} B_\alpha = \bigcup_{\alpha\in A} (S \cup B_\alpha),$$

$$S \cap \bigcap_{\alpha\in A} B_\alpha = \bigcap_{\alpha\in A} (S \cap B_\alpha).$$

These are the analogs, for indexed families of sets, of results we considered earlier for sets of sets, and they may be deduced from these results.

12.20 Remark. One often writes $\bigcup_{n=1}^{\infty} B_n$ in place of $\bigcup_{n\in\mathbf{N}} B_n$. (Note that since ∞ is not an element of $\mathbf{N}$, there is no B_∞ term in $\bigcup_{n=1}^{\infty} B_n$, contrary to what the notation might appear to suggest.) Likewise, one usually writes $\bigcup_{k=1}^{n} B_k$ in place of $\bigcup_{k\in\{1,\ldots,n\}} B_k$ and one often writes $\bigcup_{n=-\infty}^{\infty} B_n$ in place of $\bigcup_{n\in\mathbf{Z}} B_n$. Similar remarks apply to intersections.

12.21 Definition. Let $\langle B_\alpha \rangle_{\alpha\in A}$ be an indexed family of sets. To say that $\langle B_\alpha \rangle_{\alpha\in A}$ *is pairwise disjoint* means that for all $\alpha_1, \alpha_2 \in A$, if $\alpha_1 \neq \alpha_2$, then $B_{\alpha_1} \cap B_{\alpha_2} = \emptyset$.

[17] Remember that an indexed family $\langle B_\alpha \rangle_{\alpha\in A}$ is a function whose domain is the set A and whose value at α is B_α for each $\alpha \in A$. Remember also that if $\langle B_\alpha \rangle_{\alpha\in A}$ is an indexed family, then the set $\{\, B_\alpha : \alpha \in A \,\}$ is not the same thing as the indexed family $\langle B_\alpha \rangle_{\alpha\in A}$, it is the range of the function that this indexed family is.

Exercise 8. For each $n \in \mathbf{N}$, let $B_n = \{ n \}$.
- **(a)** Find $\bigcup_{n=1}^{\infty} B_n$ and $\bigcap_{n=1}^{\infty} B_n$.
- **(b)** Is the family $\langle B_n \rangle_{n \in \mathbf{N}}$ pairwise disjoint?
- **(c)** For each $n \in \mathbf{N}$, find $\bigcup_{k=1}^{n} B_k$ and $\bigcap_{k=1}^{n} B_k$. (For the intersection, you will need to consider two cases depending on the value of n.)

Exercise 9. Let $B_n = [n-1, n+1]$ for all $n \in \mathbf{N}$.
- **(a)** Find $\bigcup_{n=1}^{\infty} B_n$ and $\bigcap_{n=1}^{\infty} B_n$.
- **(b)** Is the family $\langle B_n \rangle_{n \in \mathbf{N}}$ pairwise disjoint?
- **(c)** For each $n \in \mathbf{N}$, find $\bigcup_{k=1}^{n} B_k$ and $\bigcap_{k=1}^{n} B_k$.

Exercise 10. Let $B_n = (n, n+1]$ for all $n \in \mathbf{Z}$.
- **(a)** Find $\bigcup_{n=-\infty}^{\infty} B_n$ and $\bigcap_{n=-\infty}^{\infty} B_n$.
- **(b)** Is the family $\langle B_n \rangle_{n \in \mathbf{Z}}$ pairwise disjoint?

Exercise 11. Let $B_n = (0, 1/n]$ for all $n \in \mathbf{N}$.
- **(a)** For each $n \in \mathbf{N}$, find $\bigcap_{k=1}^{n} B_k$ and $\bigcup_{k=1}^{n} B_k$.
- **(b)** Find $\bigcap_{n=1}^{\infty} B_n$ and $\bigcup_{n=1}^{\infty} B_n$

Exercise 12. Let $B_\alpha = (-\infty, \alpha] \times [\alpha, \infty)$ for all $\alpha \in \mathbf{R}$.
- **(a)** Sketch B_α as a subset of the xy-plane for $\alpha = 1, \sqrt{2}, \pi$. (You should make three separate sketches.)
- **(b)** Find $\bigcup_{\alpha \in \mathbf{R}} B_\alpha$ and $\bigcap_{\alpha \in \mathbf{R}} B_\alpha$.
- **(c)** Sketch $\bigcup_{\alpha \in \mathbf{R}} B_\alpha$ as a subset of the xy-plane.

Images of Sets.

12.22 Definition. Let f be a function and let A be a subset of the domain of f. Then *the image of A under f* (denoted $f[A]$) is the set of all values that f takes on at points of A; in other words,

$$f[A] = \{ f(x) : x \in A \}.$$

12.23 Remark. Let f be any function. Then for certain sets A, it may happen that A is both a subset of the domain of f and an element of the domain of f. In such a case, there is no reason to expect the image of A under f to be equal to the value of f at A. This is why we use brackets, as in $f[A]$, when we write the image and parentheses, as in $f(A)$, when we write the value.

Here is an example to show that this distinction really does matter. Let $X = \{ \emptyset \}$. Define a function f on X by $f(\emptyset) = \{ \emptyset \}$. Recall that $\emptyset$ is a subset of any set. In particular, $\emptyset$ is a subset of X, the domain of f. We have $f[\emptyset] = \{ f(x) : x \in \emptyset \} = \emptyset$ but $f(\emptyset) = \{ \emptyset \} \neq \emptyset$.

It must be admitted that many books are not careful to distinguish between the image $f[A]$ and the value $f(A)$, using the notation $f(A)$ to mean sometimes the latter and sometimes the former. When you read such books, you will have to determine what $f(A)$ means from the context.

12.24 Remark. Let S and T be sets and let $f\colon S \to T$. Then $\mathrm{Rng}(f) = f[S]$. In other words, the range of f is the image, under f, of the domain of f.

Exercise 13. Let $f(x) = x^2$ for all $x \in \mathbf{R}$. Let $A = [1, 3)$, $B = (-4, -2] \cup [2, 4)$, and $C = (-2, 1]$. Find $f[A]$, $f[B]$, and $f[C]$.

Exercise 14. Let $f(x, y) = (2x, 3y)$ for all $(x, y) \in \mathbf{R}^2$. Let $A = \{ (x, y) : x^2 + y^2 \leq 1 \}$. Note that A can be described geometrically as the set of all points in the plane that lie on or inside the circle $C = \{ (x, y) : x^2 + y^2 = 1 \}$. Find a geometrical description for $f[A]$, the image of A under f.

Exercise 15. Let $f(x) = x^2$ for all $x \in \mathbf{R}$. Recall that $\mathbf{Q}$ denotes the set of rational numbers.
- **(a)** Show that $f[\mathbf{Q}] \subseteq \mathbf{Q}$.
- **(b)** Is $f[\mathbf{Q}] = \mathbf{Q}$? Justify your answer.

The next result tells us that unions are preserved in passing to images.

12.25 Theorem. *Let S and T be sets and let $f\colon S \to T$. Then for each indexed family $\langle B_\alpha \rangle_{\alpha\in A}$ of subsets of S, we have*

$$f\left[\bigcup_{\alpha\in A} B_\alpha\right] = \bigcup_{\alpha\in A} f[B_\alpha].$$

In particular, for all subsets $B, C \subseteq S$, we have $f[B \cup C] = f[B] \cup f[C]$.

Proof. Consider any indexed family $\langle B_\alpha \rangle_{\alpha\in A}$ of subsets of S. To save writing, let

$$L = \bigcup_{\alpha\in A} B_\alpha \quad \text{and} \quad R = \bigcup_{\alpha\in A} f[B_\alpha].$$

We wish to show that $f[L] = R$. As usual, we shall show this by showing that $f[L] \subseteq R$ and $R \subseteq f[L]$. Consider any $y \in f[L]$. Then $y = f(x)$ for some $x \in L$. But then $x \in B_{\alpha_0}$ for some $\alpha_0 \in A$, so $y = f(x) \in f[B_{\alpha_0}]$, so $y \in R$. Thus $f[L] \subseteq R$. Now consider any $y \in R$. Then $y \in f[B_{\alpha_0}]$ for some $\alpha_0 \in A$. But then $y = f(x)$ for some $x \in B_{\alpha_0}$. Now since $x \in B_{\alpha_0}$, we have $x \in L$. Hence $f(x) \in f[L]$. In other words, $y \in f[L]$. Thus $R \subseteq f[L]$. ■

Exercise 16. Let $S = \{1, 2\} = T$ and define $f\colon S \to T$ by $f(1) = 1 = f(2)$. Let $B = \{1\}$ and let $C = \{2\}$. Find $f[B \cap C]$ and $f[B] \cap f[C]$ and observe that they are not equal. (Thus intersections are not always preserved in passing to images.)

Exercise 17. Find sets S and T, a function $f\colon S \to T$, and subsets $B, C \subseteq S$ such that $f[B \setminus C] \neq f[B] \setminus f[C]$. (Thus relative complements are not always preserved in passing to images.)

As we saw in the two preceding exercises, intersections and relative complements are not always preserved in passing to images. However, they are if the function is an injection, as is shown in the next result.

12.26 Theorem. *Let S and T be sets and let f be an injection from S to T. Then:*

(a) *For each indexed family $\langle B_\alpha \rangle_{\alpha\in A}$ of subsets of S such that $A \neq \emptyset$, we have*

$$f\left[\bigcap_{\alpha\in A} B_\alpha\right] = \bigcap_{\alpha\in A} f[B_\alpha].$$

In particular, for all subsets $B, C \subseteq S$, we have $f[B \cap C] = f[B] \cap f[C]$.

(b) *For all subsets $B, C \subseteq S$, we have $f[B \setminus C] = f[B] \setminus f[C]$.*

Proof. (a) Consider any indexed family $\langle B_\alpha \rangle_{\alpha\in A}$ of subsets of S such that $A \neq \emptyset$. To save writing, let

$$L = \bigcap_{\alpha\in A} B_\alpha \quad \text{and} \quad R = \bigcap_{\alpha\in A} f[B_\alpha].$$

We wish to show that $f[L] = R$. Consider any $y \in f[L]$. Then $y = f(x)$ for some $x \in L$. Since $x \in L$, we have $x \in B_\alpha$ for all $\alpha \in A$, so $y = f(x) \in f[B_\alpha]$ for all $\alpha \in A$, so $y \in R$. Thus $f[L] \subseteq R$. (Notice that for this inclusion, we did not use the assumption that f is an injection.) Now consider any $y \in R$. Then $y \in f[B_\alpha]$ for all $\alpha \in A$. Since $A \neq \emptyset$, we can pick an $\alpha_0 \in A$. Then $y \in f[B_{\alpha_0}]$, so $y = f(x_0)$ for some $x_0 \in B_{\alpha_0}$. We claim that $x_0 \in L$. To show this, we must show that $x_0 \in B_\alpha$ for each $\alpha \in A$. Consider any $\alpha_1 \in A$. Then $y \in f[B_{\alpha_1}]$ because $y \in R$. Hence $y = f(x_1)$ for some $x_1 \in B_{\alpha_1}$. But then $f(x_1) = f(x_0)$, so since f is an injection, $x_1 = x_0$. Hence $x_0 \in B_{\alpha_1}$. Since α_1 is an arbitrary element of A, this shows that for each $\alpha \in A$, $x_0 \in B_\alpha$. Hence $x_0 \in L$, as claimed. Since $x_0 \in L$ and $y = f(x_0)$, we have $y \in f[L]$. Thus $R \subseteq f[L]$. Since $f[L] \subseteq R$ and $R \subseteq f[L]$, we have $f[L] = R$ as desired.

(b) Consider any subsets $B, C \subseteq S$. To save writing, let $L = B \setminus C$ and let $R = f[B] \setminus f[C]$. Let $y \in f[L]$. Then $y = f(x)$ for some $x \in L$. Since $x \in L$, we have $x \in B$ and $x \notin C$. Since $x \in B$ and $y = f(x)$, we have $y \in f[B]$. Now we claim that $y \notin f[C]$. To show this, we suppose that $y \in f[C]$ and we show that this assumption leads to a contradiction. Since $y \in f[C]$, we have $y = f(x')$ for some $x' \in C$. Then $f(x) = f(x')$, so since f is an injection, $x = x'$. Hence $x \in C$. But $x \notin C$. Thus we have reached a contradiction. Hence it must be that $y \notin f[C]$. Since $y \in f[B]$ and $y \notin f[C]$, we have $y \in R$. Thus $f[L] \subseteq R$. Now let us show that $R \subseteq f[L]$. Consider any $y \in R$. Then $y \in f[B]$ and $y \notin f[C]$. Since $y \in f[B]$, we have $y = f(x)$ for some $x \in B$. Now $x \notin C$, for if it were we would have $y \in f[C]$, which is not the case. Since $x \in B$ and $x \notin C$, we have $x \in B \setminus C$. In other words, $x \in L$. Hence $f(x) \in f[L]$. In other words, $y \in f[L]$. Thus $R \subseteq f[L]$. ■

12.27 Remark. If you examine the proof of the previous theorem, you will see that even if f is not an injection, we always have $f\left[\bigcap_{\alpha\in A} B_\alpha\right] \subseteq \bigcap_{\alpha\in A} f[B_\alpha]$ and $f[B \setminus C] \supseteq f[B] \setminus f[C]$.

Exercise 18. Let S and T be sets and let $f\colon S \to T$.

(a) Show that if $f[B \cap C] = f[B] \cap f[C]$ for all subsets $B, C \subseteq S$, then f is an injection.

(b) Show that if $f[S \setminus C] = f[S] \setminus f[C]$ for each subset $C \subseteq S$, then f is an injection.

Pre-Images of Sets.

12.28 Definition. Let B be a set and let f be a function. Then *the pre-image of B under f* (denoted $f^{-1}[B]$) is the set of all elements of the domain of f that are mapped into B by f; in other words,

$$f^{-1}[B] = \{\, x \in \mathrm{Dom}(f) : f(x) \in B \,\}.$$

12.29 Remark. As was the case for images, we have been careful to distinguish between the pre-image $f^{-1}[B]$ of a set B and the value $f^{-1}(B)$ of the inverse function f^{-1} at an element B in the range of f. Note that the pre-image makes sense whether or not f has an inverse function. And when f has an inverse function, if B is a set which also happens to be an element of the range of f, then there is no reason to expect $f^{-1}[B]$ and $f^{-1}(B)$ to be the same, so it is important to use notation which distinguishes between them.

To see that this distinction really does matter, first note that for any function f, $f^{-1}[\emptyset] = \emptyset$. Now let f be the function on $\big\{\, \{\, \emptyset \,\} \,\big\}$ defined by $f(\{\, \emptyset \,\}) = \emptyset$. Since the domain of f has only one element, f cannot help but be one-to-one, so f has an inverse function f^{-1}. We have $f^{-1}(\emptyset) = \{\, \emptyset \,\} \neq \emptyset = f^{-1}[\emptyset]$.

It must be admitted that many books are not careful to distinguish between the pre-image $f^{-1}[B]$ and the value $f^{-1}(B)$, using the notation $f^{-1}(B)$ to mean sometimes the latter and sometimes the former. When you read such books, you will have to determine what $f^{-1}(B)$ means from the context.

Exercise 19. Let $f(x) = x^2$ for all $x \in \mathbf{R}$. Let $B = [1, 4)$. Find $f^{-1}[B]$. Make a sketch of the graph of f showing B on the vertical axis and $f^{-1}[B]$ on the horizontal axis.

Exercise 20. Let $f(x, y) = (2x, 3y)$ for all $(x, y) \in \mathbf{R}^2$. Let $A = \big\{\, (x, y) : x^2 + y^2 \leq 1 \,\big\}$. Note that A can be described geometrically as the set of all points in the plane that lie on or inside the circle $C = \big\{\, (x, y) : x^2 + y^2 = 1 \,\big\}$. Find a geometrical description for $f^{-1}[A]$, the pre-image of A under f. Contrast your answer with the answer to Exercise 14.

Perhaps the simplest kind of pre-image of a set is a pre-image of a one-element set. In particular, when f is a function whose range is a subset of $\mathbf{R}$, then for each $y \in \mathbf{R}$, the pre-image $f^{-1}[\{\, y \,\}]$ of the one-element set $\{\, y \,\}$ is called the *level set* for f corresponding to the level y. (To understand the motivation for this terminology, think of the special case where the domain of f is a subset of the surface of the earth and for each point x in the domain of f, $f(x)$ is the elevation of x above sea level. Then for each $y \in \mathbf{R}$, $f^{-1}[\{\, y \,\}]$ is the set of all points in the domain of f whose elevation above sea level is y.)

Exercise 21. Let $f(x, y) = x^2 + y^2$ for all $(x, y) \in \mathbf{R}^2$. Find the level sets for f corresponding to the levels 1, 4, and 9. Sketch these three level sets as subsets of the xy-plane and label them.

In contrast to what we saw for images, not only unions but also intersections and relative complements are all preserved under passing to pre-images, as the following result shows.

12.30 Theorem. *Let S and T be sets and let $f\colon S \to T$. Then:*

(a) *For each indexed family $\langle\, B_\alpha \,\rangle_{\alpha \in A}$ of subsets of T, we have*

$$f^{-1}\left[\, \bigcup_{\alpha \in A} B_\alpha \,\right] = \bigcup_{\alpha \in A} f^{-1}[B_\alpha].$$

In particular, for all subsets $B, C \subseteq T$, we have $f^{-1}[B \cup C] = f^{-1}[B] \cup f^{-1}[C]$.

(b) *For each indexed family $\langle\, B_\alpha \,\rangle_{\alpha \in A}$ of subsets of T such that $A \neq \emptyset$, we have*

$$f^{-1}\left[\, \bigcap_{\alpha \in A} B_\alpha \,\right] = \bigcap_{\alpha \in A} f^{-1}[B_\alpha].$$

In particular, for all subsets $B, C \subseteq T$, we have $f^{-1}[B \cap C] = f^{-1}[B] \cap f^{-1}[C]$.

(c) *For all subsets* $B, C \subseteq T$*, we have* $f^{-1}[B \setminus C] = f^{-1}[B] \setminus f^{-1}[C]$.

Proof. Consider any indexed family $\langle B_\alpha \rangle_{\alpha \in A}$ of subsets of T. For each x, we have

$$\begin{array}{ll} & x \in f^{-1}\left[\bigcup_{\alpha\in A} B_\alpha\right] \\ \text{iff} & x \in \mathrm{Dom}(f) \text{ and } f(x) \in \bigcup_{\alpha\in A} B_\alpha \\ \text{iff} & x \in \mathrm{Dom}(f) \text{ and } f(x) \in B_\alpha \text{ for some } \alpha \in A \\ \text{iff} & x \in f^{-1}[B_\alpha] \text{ for some } \alpha \in A \\ \text{iff} & x \in \bigcup_{\alpha\in A} f^{-1}[B_\alpha]. \end{array}$$

Hence $f^{-1}\left[\bigcup_{\alpha\in A} B_\alpha\right] = \bigcup_{\alpha\in A} f^{-1}[B_\alpha]$. This proves (a). Now suppose $A \neq \emptyset$. Then for each x, we have

$$\begin{array}{ll} & x \in f^{-1}\left[\bigcap_{\alpha\in A} B_\alpha\right] \\ \text{iff} & x \in \mathrm{Dom}(f) \text{ and } f(x) \in \bigcap_{\alpha\in A} B_\alpha \\ \text{iff} & x \in \mathrm{Dom}(f) \text{ and } f(x) \in B_\alpha \text{ for each } \alpha \in A \\ \text{iff} & x \in f^{-1}[B_\alpha] \text{ for each } \alpha \in A \\ \text{iff} & x \in \bigcap_{\alpha\in A} f^{-1}[B_\alpha]. \end{array}$$

Hence $f^{-1}\left[\bigcap_{\alpha\in A} B_\alpha\right] = \bigcap_{\alpha\in A} f^{-1}[B_\alpha]$. This proves (b). Finally, consider any subsets $B, C \subseteq T$. Then for each x, we have

$$\begin{array}{ll} & x \in f^{-1}[B \setminus C] \\ \text{iff} & x \in \mathrm{Dom}(f) \text{ and } f(x) \in B \setminus C \\ \text{iff} & x \in \mathrm{Dom}(f) \text{ and } f(x) \in B \text{ and } f(x) \notin C \\ \text{iff} & x \in f^{-1}[B] \text{ and } x \notin f^{-1}[C] \\ \text{iff} & x \in f^{-1}[B] \setminus f^{-1}[C]. \end{array}$$

Hence $f^{-1}[B \setminus C] = f^{-1}[B] \setminus f^{-1}[C]$. This proves (c). ■

Exercise 22. Where was nonemptiness of A used in the proof of (b) of the preceding theorem?

Now we shall consider pre-images of images and vice versa.

12.31 Theorem. *Let* S *and* T *be sets and let* $f\colon S \to T$*. Then:*

(a) *For each subset* $A \subseteq S$*, we have* $A \subseteq f^{-1}\big[f[A]\big]$*, with equality iff* $A = f^{-1}[B]$ *for some* $B \subseteq T$.

(b) *For each subset* $B \subseteq T$*, we have* $f\big[f^{-1}[B]\big] = B \cap \mathrm{Rng}(f)$.

Proof. (a) Consider any subset $A \subseteq S$. For each $x \in A$, we have $f(x) \in f[A]$, so $x \in f^{-1}\big[f[A]\big]$. This shows that $A \subseteq f^{-1}\big[f[A]\big]$. Next, we wish to show that $A = f^{-1}\big[f[A]\big]$ iff $A = f^{-1}[B]$ for some $B \subseteq T$. If $A = f^{-1}\big[f[A]\big]$, then obviously $A = f^{-1}[B]$, where $B = f[A] \subseteq T$. Conversely, suppose $A = f^{-1}[B]$ for some $B \subseteq T$. Then for each $x \in A$, we have $f(x) \in B$ by the definition of $f^{-1}[B]$. Hence $f[A] \subseteq B$, so $f^{-1}\big[f[A]\big] \subseteq f^{-1}[B] = A$. Since $f^{-1}\big[f[A]\big]$ is a subset of A and A is always a subset of $f^{-1}\big[f[A]\big]$, we have $A = f^{-1}\big[f[A]\big]$. Thus $A = f^{-1}\big[f[A]\big]$ iff $A = f^{-1}[B]$ for some $B \subseteq T$, as desired.

(b) Consider any subset $B \subseteq T$. To save writing, let $L = f^{-1}[B]$ and let $R = B \cap \mathrm{Rng}(f)$. Since $S = \mathrm{Dom}(f)$, we have $L \subseteq S$ and $\mathrm{Rng}(f) = \{\, f(x) : x \in S \,\}$. We wish to show that $f[L] = R$. Consider any $y \in f[L]$. Then $y = f(x)$ for some $x \in L$. Since $L \subseteq S$, we have $x \in S$, so $y = f(x) \in \mathrm{Rng}(f)$. Since $x \in L = f^{-1}[B]$, we have $f(x) \in B$. In other words, $y \in B$. Since $y \in B$ and $y \in \mathrm{Rng}(f)$, we have $y \in B \cap \mathrm{Rng}(f)$. In other words, $y \in R$. This shows that $f[L] \subseteq R$. Now consider any $y \in R$. Then $y \in B$ and $y \in \mathrm{Rng}(f)$. Since $y \in \mathrm{Rng}(f)$, we have $y = f(x)$ for some $x \in S$. Since $f(x) = y$ and $y \in B$, we have $f(x) \in B$, so $x \in f^{-1}[B] = L$. Hence $f(x) \in f[L]$. In other words, $y \in f[L]$. This shows that $R \subseteq f[L]$. Since $f[L] \subseteq R$ and $R \subseteq f[L]$, we have $f[L] = R$, as desired. ■

Exercise 23. Let S and T be sets and let $f\colon S \to T$.

(a) Show that for each subset $A \subseteq S$, we have $A = f^{-1}\big[f[A]\big]$ iff $f[A]$ and $f[S \setminus A]$ are disjoint.

(b) Show that f is an injection from S to T iff for each subset $A \subseteq S$, $A = f^{-1}\big[f[A]\big]$.

(c) Show that for each subset $B \subseteq T$, we have $f\big[f^{-1}[B]\big] = B$ iff $B \subseteq \mathrm{Rng}(f)$.

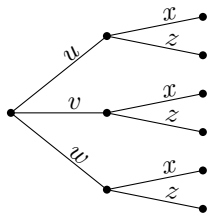
(d) Show that f is a surjection from S to T iff for each subset $B \subseteq T$, $f\big[f^{-1}[B]\big] = B$.

Choice Functions and Cartesian Products.

12.32 Definition. Let $\langle B_\alpha \rangle_{\alpha\in A}$ be an indexed family of sets. To say that f is *a choice function for* $\langle B_\alpha \rangle_{\alpha\in A}$ means that f is a function, $\mathrm{Dom}(f) = A$, and for each $\alpha \in A$, we have $f(\alpha) \in B_\alpha$.

12.33 Remark. Informally, we may say that a choice function f for an indexed family of nonempty sets $\langle B_\alpha \rangle_{\alpha\in A}$ is a function that chooses an element $f(\alpha)$ in B_α for each α in A.

12.34 Example. Let $B_1 = \{ u, v, w \}$ where u, v, and w are distinct. Let $B_2 = \{ x, z \}$ where x and z are distinct. Let $f(1) = u$ and $f(2) = x$. Then f is a choice function for the indexed family of sets $\langle B_n \rangle_{n\in\{1,2\}}$. But f is not the only such choice function. We can represent all of the possible choice functions for this indexed family of sets by drawing a tree diagram, as follows:



Each path from the leftmost node to one of the rightmost nodes in this tree diagram represents one of the choice functions for the indexed family of sets $\langle B_n \rangle_{n\in\{1,2\}}$, and each such choice function is represented by exactly one such path. Since there are $3 \cdot 2 = 6$ such paths, there are 6 such choice functions. These 6 choice functions are the following 6 sequences of length 2:

$$\langle u, x \rangle,\ \langle u, z \rangle,\ \langle v, x \rangle,\ \langle v, z \rangle,\ \langle w, x \rangle,\ \langle w, z \rangle.$$

(The first of these is the function f defined above.) The reason why a choice function turns out to be a sequence of length 2 in this example is that the index set is the set $\{ 1, 2 \}$. As we know, a sequence of length 2 is a function whose domain is the set $\{ 1, 2 \}$.

Exercise 24. Suppose a restaurant offers a fixed-price menu on which you may choose one item from each of the following three sets:

$$B_1 = \{ \text{soup, coleslaw} \},$$
$$B_2 = \{ \text{meatloaf, turkey, halibut} \},$$
$$B_3 = \{ \text{potatoes, rice} \}.$$

Draw a tree diagram to represent all the possible choice functions for the indexed family of sets $\langle B_n \rangle_{n\in\{1,2,3\}}$. Then list all of these choice functions, using the notation for sequences of length 3. (To save writing, you may wish to abbreviate each food item by the first letter of its name.) How many such choice functions are there? In how many different ways can you select a meal from this menu if you take one item from each set?

12.35 Definition. Let $\langle B_\alpha \rangle_{\alpha\in A}$ be an indexed family of sets. The *Cartesian product of the indexed family* $\langle B_\alpha \rangle_{\alpha\in A}$ is

$$\prod_{\alpha\in A} B_\alpha = \big\{ f : f \text{ is a choice function for } \langle B_\alpha \rangle_{\alpha\in A} \big\}.$$

12.36 Remark. The $\prod$ notation is also used to denote the ordinary product of numbers, as in $\prod_{k=1}^{n} c_k = c_1 c_2 \cdots c_n$. You should be able to infer from the context which meaning $\prod$ has.

12.37 Remark. The Cartesian product of an indexed family of sets $\langle B_\alpha \rangle_{\alpha\in A}$ makes sense no matter what the index set A is. However, it is easiest to understand when the index set A is of the form $\{ 1, \ldots, n \}$ where $n \in \mathbf{N}$. In this case, the Cartesian product of the indexed family is often denoted $\prod_{k=1}^{n} B_k$ and is the set of all n-sequences whose first, second, ..., n-th terms are in B_1, B_2, ..., B_n respectively; in other words,

$$\prod_{k=1}^{n} B_k = \big\{ \langle y_1, y_2, \ldots, y_n \rangle : y_1 \in B_1,\ y_2 \in B_2, \ldots,\ y_n \in B_n \big\}.$$

Let us compare this with the Cartesian product $B_1 \times B_2 \times \cdots \times B_n$, which was defined earlier to be the set of all ordered n-tuples whose first, second, …, n-th entries are in B_1, B_2, …, B_n respectively; in other words,

$$B_1 \times B_2 \times \cdots \times B_n = \big\{\, (y_1, y_2, \ldots, y_n) : y_1 \in B_1,\, y_2 \in B_2, \ldots,\, y_n \in B_n \,\big\}.$$

Now $\prod_{k=1}^{n} B_k$ is not literally the same thing as $B_1 \times B_2 \times \cdots \times B_n$. (The former is a set of n-sequences and the latter is a set of ordered n-tuples.) However there is a natural one-to-one correspondence between $\prod_{k=1}^{n} B_k$ and $B_1 \times B_2 \times \cdots \times B_n$. Specifically, if we let

$$\Phi(\langle\, y_1, y_2, \ldots, y_n \,\rangle) = (y_1, y_2, \ldots, y_n)$$

for all $y_1 \in B_1$, $y_2 \in B_2, \ldots, y_n \in B_n$, then Φ is a bijection from $\prod_{k=1}^{n} B_k$ to $B_1 \times B_2 \times \cdots \times B_n$.

12.38 Remark. It is only a little harder to understand the Cartesian product of an infinite sequence of sets $\langle\, B_n \,\rangle_{n\in\mathbf{N}}$. In this case, the Cartesian product is often denoted $\prod_{n=1}^{\infty} B_n$ and is the set of all infinite sequences with first term in B_1, second term in B_2, third term in B_3, and so on. In other words,

$$\prod_{n=1}^{\infty} B_n = \big\{\, \langle\, y_1, y_2, y_3, \ldots \,\rangle : y_n \in B_n \text{ for all } n \in \mathbf{N} \,\big\}.$$

Exercise 25. Let $\langle\, B_\alpha \,\rangle_{\alpha\in A}$ be an indexed family of sets and let $B = \bigcup_{\alpha\in A} B_\alpha$. Show that $\prod_{\alpha\in A} B_\alpha \subseteq B^A$.

Exercise 26. Let A and B be sets and let $B_\alpha = B$ for all $\alpha \in A$. Show that $\prod_{\alpha\in A} B_\alpha = B^A$.

The Axiom of Choice. It is not difficult to prove by induction that for each $n \in \mathbf{N}$, for each family of nonempty sets $\langle\, B_k \,\rangle_{k\in\{1,\ldots,n\}}$ indexed by the set $\{\,1, \ldots, n\,\}$, there exists a choice function for the family $\langle\, B_k \,\rangle_{k\in\{1,\ldots,n\}}$. *The axiom of choice* asserts that each indexed family of nonempty sets $\langle\, B_\alpha \,\rangle_{\alpha\in A}$ has a choice function, no matter what the index set A is. This natural-sounding principal was once considered rather controversial by mathematicians, because when the index set A is infinite, it asserts the existence of a function that may not be definable by any formula. Nevertheless, it is now generally accepted as a valid principle because of its naturalness and because without it many other things that intuitively should be true just cannot be proved. It is not our purpose here to go into details about the philosophical standing of the axiom of choice. We wish only to introduce it and to illustrate its use in some simple situations.

Exercise 27. Let

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

Find $\bigcap_{i=1}^{2} \bigcup_{j=1}^{2} C(i,j)$ and $\bigcup_{j=1}^{2} \bigcap_{i=1}^{2} C(i,j)$, and observe that they are not equal.

Exercise 28. Let A and B be sets and let $\langle\, C(i,j) \,\rangle_{i\in A, j\in B}$ be a family of sets indexed by $A \times B$, the Cartesian product of A and B. Show that

$$\bigcap_{i\in A} \bigcup_{j\in B} C(i,j) \supseteq \bigcup_{j\in B} \bigcap_{i\in A} C(i,j).$$

(As Exercise 27 shows, "$\supseteq$" cannot be strengthened to "$=$" here in general.)

12.39 Example. Let $C(1,1)$, $C(1,2)$, $C(2,1)$, and $C(2,2)$ be sets. Then, since intersection is distributive over union, we have

$$\begin{aligned}
&\bigcap_{i=1}^{2} \bigcup_{j=1}^{2} C(i,j) = \bigcap_{i=1}^{2} \big(C(i,1) \cup C(i,2)\big) \\
&\big(C(1,1) \cup C(1,2)\big) \cap \big(C(2,1) \cup C(2,2)\big) \\
&= \Big(\big(C(1,1) \cup C(1,2)\big) \cap C(2,1)\Big) \cup \Big(\big(C(1,1) \cup C(1,2)\big) \cap C(2,2)\Big) \\
&= \big(C(1,1) \cap C(2,1)\big) \cup \big(C(1,2) \cap C(2,1)\big) \cup \big(C(1,1) \cap C(2,2)\big) \cup \big(C(1,2) \cap C(2,2)\big)
\end{aligned}$$

The next result is a generalization of this. It tells us what $\bigcap_{i\in A} \bigcup_{j\in B} C(i,j)$ is equal to when A and B are arbitrary sets. It provides our first illustration of the use of the axiom of choice.

12.40 Proposition. *Let A and B be sets and let $\langle C(i,j)\rangle_{i\in A, j\in B}$ be a family of sets indexed by $A\times B$, the Cartesian product of A and B. Then*

$$\bigcap_{i\in A}\bigcup_{j\in B} C(i,j) = \bigcup_{f\in B^A}\bigcap_{i\in A} C(i,f(i)).$$

Proof. To save writing, let

$$L = \bigcap_{i\in A}\bigcup_{j\in B} C(i,j) \quad\text{and}\quad R = \bigcup_{f\in B^A}\bigcap_{i\in A} C(i,f(i)).$$

Consider any $x\in L$. Then for each $i\in A$, we have $x\in\bigcup_{j\in B} C(i,j)$, so there exists $j\in B$ such that $x\in C(i,j)$. For each $i\in A$, let $B_i = \{\, j\in B : x\in C(i,j)\,\}$. Then for each $i\in A$, $B_i\neq\emptyset$. Hence by the axiom of choice, we can pick a choice function f_0 for the indexed family of sets $\langle B_i\rangle_{i\in A}$. Then for each $i\in I$, $f_0(i)\in B_i$, so by the definition of B_i, $x\in C(i,f_0(i))$. Hence $x\in\bigcap_{i\in I} C(i,f_0(i))$. Since $f_0(i)\in B_i\subseteq B$ for all $i\in I$, f_0 is a function from A to B; in other words, f_0 is an element of B^A. Thus $f_0\in B^A$ and $x\in\bigcap_{i\in I} C(i,f_0(i))$. Hence $x\in\bigcup_{f\in B^A}\bigcap_{i\in A} C(i,f(i))$. In other words, $x\in R$. Thus $L\subseteq R$. Conversely, suppose $x\in R$. Then $x\in\bigcap_{i\in A} C(i,f_0(i))$ for some $f_0\in B^A$. Hence for each $i\in A$, $x\in C(i,f_0(i))$, so since $f_0(i)\in B$, $x\in\bigcup_{j\in B} C(i,j)$. Thus $x\in\bigcap_{i\in A}\bigcup_{j\in B} C(i,j)$. In other words $x\in L$. Thus $R\subseteq L$. Since $L\subseteq R$ and $R\subseteq L$, we have $L=R$, as desired. ■

Exercise 29. Let A and B be sets.

- **(a)** Suppose $f\colon A\to B$ and $g\colon B\to A$ such that $f\circ g = \mathrm{id}_B$. (By the way, in this situation, g is said to be *a right inverse for* f and f is said to be *a left inverse for* g.) Show that f is a surjection from A to B and g is an injection from B to A.
- **(b)** Suppose f is a surjection from A to B. Show that there exists a function $g\colon B\to A$ such that $f\circ g = \mathrm{id}_B$. (For this part, let $A_y = f^{-1}[\{\, y\,\}]$ for all $y\in B$. Show that $A_y\neq\emptyset$ for all $y\in B$, so that you can apply the axiom of choice to the indexed family of sets $\langle A_y\rangle_{y\in B}$.)

12.41 Proposition. *For each set $\mathscr{M}$ of nonempty sets, there exists a function g on $\mathscr{M}$ such that for each $A\in\mathscr{M}$, we have $g(A)\in A$.*

Proof. Consider any set $\mathscr{M}$ all of whose elements are nonempty sets. For each $A\in\mathscr{M}$, let $B_A = A$. Then $\langle B_A\rangle_{A\in\mathscr{M}}$ is a family of nonempty sets indexed by $\mathscr{M}$. By the axiom of choice, we can pick a choice function g for this family. Then g is a function on $\mathscr{M}$ and for each $A\in\mathscr{M}$, we have $g(A)\in B_A$. But for each $A\in\mathscr{M}$, $B_A = A$. Thus for each $A\in\mathscr{M}$, we have $g(A)\in A$, as desired. ■

12.42 Remark. Given a set $\mathscr{M}$ of nonempty sets, a function g on $\mathscr{M}$ of the sort described in Proposition 12.41 is often called *a choice function for* $\mathscr{M}$. As a matter of fact, Proposition 12.41 is an alternative form of the axiom of choice. In other words, not only does Proposition 12.41 follow from the axiom of choice (as we have just seen) but conversely, the axiom of choice follows from Proposition 12.41. To see that the axiom of choice follows from Proposition 12.41, consider any indexed family of nonempty sets $\langle B_\alpha\rangle_{\alpha\in A}$. We wish to show that there is a choice function f for the family $\langle B_\alpha\rangle_{\alpha\in A}$. Let $\mathscr{M} = \{\, B_\alpha : \alpha\in A\,\}$. Then $\mathscr{M}$ is a set of nonempty sets. By Proposition 12.41, there exists a choice function g for $\mathscr{M}$. In other words, there is a function g on $\mathscr{M}$ such that for each $B\in\mathscr{M}$, we have $g(B)\in B$. Let $f(\alpha) = g(B_\alpha)$ for all $\alpha\in A$. Then f is a function on A and for each $\alpha\in A$, we have $f(\alpha)\in B_\alpha$. In other words, f is a choice function for the family $\langle B_\alpha\rangle_{\alpha\in A}$.

12.43 Example. By Proposition 12.41, there is a choice function for the set of all nonempty subsets of $\mathbf{R}$. However, it seems not to be possible to write down a formula for such a choice function. Perhaps if you think about this, you may begin to see why the axiom of choice could be controversial.

Section 13. The Fundamental Principles of Counting

This section and the next are devoted to the fundamentals of combinatorics. Combinatorics is the branch of mathematics that is concerned with questions about counting, such as in how many different ways can a committee of three people can be formed from a collection of twelve people, or in how many different ways can four people be seated if there are seven chairs. Our approach to combinatorics will be based explicitly on sets and functions. This approach presents some notational and linguistic hurdles, but it has the compensating advantage that it provides a precise conceptual framework for thinking about combinatorial questions and a flexible, concise language and notation for discussing such questions. This conceptual framework is important in many other areas of mathematics, such as group theory, probability theory, the Lebesgue theory of integration, and general topology.

In this section, we shall begin by discussing what we mean when we say that two sets have the same number of elements. In terms of this, we shall make precise what we mean when we say that a set has n elements. Then we shall discuss the distinction between finite and infinite sets. (In this section and the next, we shall be concerned mostly with finite sets, although we shall have some things to say about infinite sets.) Then we shall discuss basic rules for counting, such as the addition rule and the multiplication rule. Most of the results in this section will probably seem so obvious as not to require proof. Nevertheless, it is worth knowing that these very fundamental facts can be proved (by induction, in most cases) and you will probably develop an improved grasp of set theory by working through these proofs and doing the exercises.

13.1 Definition. Let A and B be sets. To say that A *is equinumerous to* B means that there exists a bijection from A to B.

13.2 Remark. You may find it convenient to write "$A \approx B$" as an abbreviation for "A is equinumerous to B."

13.3 Remark. Informally, we say A *and* B *have the same number of elements* when A is equinumerous to B. Notice that this applies even if A and B have infinitely many elements, although in this section we shall concentrate on the case where A and B have only finitely many elements.

13.4 Example. Let $A = \{1, 2\}$ and $B = \{7, 11\}$. Then A is equinumerous to B. To see this, observe that the 2-sequence $\langle 7, 11 \rangle$ is a bijection from A to B. Of course, this is not the only bijection from A to B. There is one other one, namely the 2-sequence $\langle 11, 7 \rangle$.

Exercise 1. A bijection from the set $\{1, 2, 3\}$ to the set $\{\pi, e, 5\}$ is the same thing as a 3-sequence of distinct elements of the set $\{\pi, e, 5\}$. There are six such bijections. List them.

13.5 Proposition. *Equinumerousness is reflexive, symmetric, and transitive. In other words*:

- **(a)** *For each set A, we have A is equinumerous to A.* (Reflexivity.)
- **(b)** *For all sets A and B, if A is equinumerous to B, then B is equinumerous to A.* (Symmetry.)
- **(c)** *For all sets A, B, C, if A is equinumerous to B and B is equinumerous to C, then A is equinumerous to C.* (Transitivity.)

Proof. (a) Consider any set A. Let f be the identity function on A. In other words, let f be the function from A to A defined by $f(x) = x$ for all $x \in A$. Then f is a bijection from A to A. Hence A is equinumerous to A.

(b) Consider any sets A and B. Suppose A is equinumerous to B. Then we can pick a bijection f from A to B. Let $g = f^{-1}$, the inverse of the function f. In other words, let g be the function from B to A with the property that for each $y \in B$, $g(y)$ is the unique x in A such that $f(x) = y$. Then g is a bijection from B to A. Hence B is equinumerous to A.

(c) Consider any sets A, B, C. Suppose A is equinumerous to B and B is equinumerous to C. Then we can pick a bijection f from A to B and we can also pick a bijection g from B to C. Let $h = g \circ f$, the composition of g with f. In other words, let h be the function from A to C defined by $h(x) = g(f(x))$ for all $x \in A$. Then h is a bijection from A to C. Hence A is equinumerous to C. ■

Exercise 2. Let A, B, C, f, g, h be as in part (c) of the proof of Proposition 13.5. Verify that h is indeed a bijection from A to C.

13.6 Remark. Consider a collection A of finitely many objects. For definiteness, suppose there are five objects in the collection A. When we count the objects in A, we point at them one after another and as we do this, we say "one, two, three, four, five." By this act, we specify a bijection from the set A to the set $\{1,2,3,4,5\}$. Thus A is equinumerous to $\{1,2,3,4,5\}$. This discussion is intended to motivate the next definition.

13.7 Reminder. Recall that $\boldsymbol{\omega} = \{0,1,2,\dots\}$ and $\mathbf{N} = \{1,2,3,\dots\}$.

13.8 Remark. For each $n \in \boldsymbol{\omega}$, $\{1,\dots,n\}$ denotes the set $\{k \in \mathbf{N} : k \le n\}$. In particular, if $n = 0$, then the set $\{1,\dots,n\}$ is empty. More generally, if $n = 0$, then we take $\{a_1,\dots,a_n\}$ to denote the empty set. These conventions are consistent with other peculiarities of "dot dot dot" notation. For instance, if $n = 2$, then $1 + 2 + 3 + \cdots + n = 1 + 2$.

13.9 Remark. Let $n \in \boldsymbol{\omega}$. Another notation that one sometimes sees for $\{1,\dots,n\}$ is $\mathbf{N}_{\le n}$. And sometimes, you might find it convenient to write $\underline{n}$ for $\{1,\dots,n\}$, in order to save space or to save time writing. However, before you do this, you should be sure to explain what you mean by $\underline{n}$.

13.10 Definition. Let A be a set and let $n \in \boldsymbol{\omega}$. To say that A *has n elements* means that A is equinumerous to $\{1,\dots,n\}$.

13.11 Example. The set $\{1,\dots,n\}$ has n elements, because $\{1,\dots,n\}$ is equinumerous to $\{1,\dots,n\}$.

13.12 Remark. A set has 0 elements iff it is empty.

13.13 Warning. Let A be a set and let $m,n \in \boldsymbol{\omega}$. If A has m elements and A also has n elements, then naturally we expect that $m = n$. This does turn out to be true but it requires proof. Until we have proved it, we should be on guard against assuming it.

13.14 Remark. Sometimes, instead of saying A has n elements, we may say A *is an n-element set.*

13.15 Remark. If A is a set and $n \in \boldsymbol{\omega}$, then A is equinumerous to $\{1,\dots,n\}$ iff $\{1,\dots,n\}$ is equinumerous to A, by Proposition 13.5(b), the symmetry of equinumerousness.

13.16 Proposition. *Let A be a set and let $n \in \boldsymbol{\omega}$. Then the following are equivalent.*

(a) *A has n elements.*

(b) *There exist distinct objects $a_1,\dots,a_n$ such that $A = \{a_1,\dots,a_n\}$.*

Proof. Suppose A has n elements. Then there is a bijection f from $\{1,\dots,n\}$ to A. Let $a_k = f(k)$ for $k = 1,\dots,n$. Since f maps $\{1,\dots,n\}$ onto A, we have $A = \{a_1,\dots,a_n\}$. Since f is one-to-one, the objects $a_1,\dots,a_n$ are distinct.

Conversely, suppose there exist distinct objects $a_1,\dots,a_n$ such that $A = \{a_1,\dots,a_n\}$. Then A is the range of the function f defined on $\{1,\dots,n\}$ by $f(k) = a_k$. Since $a_1,\dots,a_n$ are distinct, f is one-to-one, so f is a bijection from $\{1,\dots,n\}$ to A, so A has n elements. ■

13.17 Definition. Let A be a set. To say that A *is finite* means that there exists $n \in \boldsymbol{\omega}$ such that A has n elements.

13.18 Definition. Let A be a set. To say that A *is infinite* means that A is not finite.

13.19 Lemma. *Suppose A and B are sets, A is equinumerous to B, $s \notin A$, and $t \notin B$. Then $A \cup \{s\}$ is equinumerous to $B \cup \{t\}$.*

Proof. Since A is equinumerous to B, we can pick a bijection f from A to B. Define a function g from $A \cup \{s\}$ to $B \cup \{t\}$ by

$$g(x) = \begin{cases} t & \text{if } x = s; \\ f(x) & \text{if } x \in A. \end{cases}$$

Then g is a bijection from $A \cup \{s\}$ to $B \cup \{t\}$. Hence $A \cup \{s\}$ is equinumerous to $B \cup \{t\}$. ■

13.20 Lemma. *Let A be a set and let s be any object. Then*:

(a) *For each $n \in \boldsymbol{\omega}$, if A has n elements and $s \notin A$, then $A \cup \{s\}$ has $n + 1$ elements.*

(b) *If A is finite, then $A \cup \{s\}$ is finite.*

Exercise 3. Prove Lemma 13.20. (Hint: Apply Lemma 13.19 with $B = \{1,\dots,n\}$.)

13.21 Lemma. *Let B be a set and let $u, v \in B$. Then $B \setminus \{u\}$ is equinumerous to $B \setminus \{v\}$.*

Proof. Either $u = v$ or $u \neq v$.

Case 1. Suppose $u = v$. Then $B \setminus \{u\} = B \setminus \{v\}$. Hence $B \setminus \{u\}$ is equinumerous to $B \setminus \{v\}$, by the reflexivity of equinumerousness.

Case 2. Suppose $u \neq v$. Then $v \in B \setminus \{u\}$ and $u \in B \setminus \{v\}$. Define h on $B \setminus \{u\}$ by

$$h(x) = \begin{cases} u & \text{if } x = v; \\ x & \text{if } x \in B \setminus \{u, v\}. \end{cases}$$

Then h is a bijection from $B \setminus \{u\}$ to $B \setminus \{v\}$. Hence $B \setminus \{u\}$ is equinumerous to $B \setminus \{v\}$.

Thus in either case, $B \setminus \{u\}$ is equinumerous to $B \setminus \{v\}$. ■

Exercise 4. Let B, u, v, and h be as in Case 2 of the proof of Lemma 13.21. Verify that h is indeed a bijection from $B \setminus \{u\}$ to $B \setminus \{v\}$.

13.22 Lemma. *Suppose A and B are sets, A is equinumerous to B, $s \in A$, and $t \in B$. Then $A \setminus \{s\}$ is equinumerous to $B \setminus \{t\}$.*

Proof. Since A is equinumerous to B, we can pick a bijection f from A to B. Let $u = f(s)$ and let g be the restriction of f to $A \setminus \{s\}$. Then g is a bijection from $A \setminus \{s\}$ to $B \setminus \{u\}$. Hence $A \setminus \{s\}$ is equinumerous to $B \setminus \{u\}$. Now by Lemma 13.21, $B \setminus \{u\}$ is equinumerous to $B \setminus \{t\}$. It follows that $A \setminus \{s\}$ is equinumerous to $B \setminus \{t\}$, by the transitivity of equinumerousness. ■

Exercise 5. Let A, B, s, f, u, and g be as in the proof of Lemma 13.22. Verify that g is indeed a bijection from $A \setminus \{u\}$ to $B \setminus \{u\}$.

13.23 Lemma. *For all $m, n \in \boldsymbol{\omega}$, if $\{1, \ldots, m\}$ is equinumerous to $\{1, \ldots, n\}$, then $m = n$.*

Proof. Let $P(m)$ be the sentence

$$\text{For each } n \in \boldsymbol{\omega}, \text{ if } \{1, \ldots, m\} \text{ is equinumerous to } \{1, \ldots, n\}, \text{ then } m = n.$$

Clearly it suffices to prove that for each $m \in \boldsymbol{\omega}$, $P(m)$ is true. We shall do this by induction.

BASE CASE: If $m = 0$, then $\{1, \ldots, m\}$ is empty, so for each $n \in \boldsymbol{\omega}$, if $\{1, \ldots, m\}$ is equinumerous to $\{1, \ldots, n\}$, then $\{1, \ldots, n\}$ is empty, so $n = 0$. Thus $P(0)$ is true.

INDUCTIVE STEP: Let $m \in \boldsymbol{\omega}$ such that $P(m)$ is true. We wish to show that $P(m+1)$ is true too. Let $n \in \boldsymbol{\omega}$ such that $\{1, \ldots, m+1\}$ is equinumerous to $\{1, \ldots, n\}$. Now $m + 1 \geq 1$, so $\{1, \ldots, m+1\}$ is not empty, so $\{1, \ldots, n\}$ is not empty, so $n \geq 1$. Thus $m+1 \in \{1, \ldots, m+1\}$ and $n \in \{1, \ldots, n\}$. Hence, by Lemma 13.22, $\{1, \ldots, m+1\} \setminus \{m+1\}$ is equinumerous to $\{1, \ldots, n\} \setminus \{n\}$. In other words, $\{1, \ldots, m\}$ is equinumerous to $\{1, \ldots, n-1\}$. Thus, by the inductive hypothesis, $m = n - 1$. Hence $m + 1 = n$. Therefore $P(m+1)$ is true too, as desired.

CONCLUSION: Therefore, by induction, for each $m \in \boldsymbol{\omega}$, $P(m)$ is true.

This completes the proof of the lemma. ■

13.24 Remark. The next result confirms the fact, familiar from experience, that regardless of the order in which one counts the elements in a given finite set, one always gets the same number.

13.25 Theorem. *The number of elements in a finite set is uniquely determined.*

Proof. Consider any finite set A. Suppose A has m elements and A has n elements, where $m, n \in \boldsymbol{\omega}$. We wish to show that $m = n$. Since A has m elements, A is equinumerous to $\{1, \ldots, m\}$. Hence, by the symmetry of equinumerousness, $\{1, \ldots, m\}$ is equinumerous to A. Since A has n elements, A is equinumerous to $\{1, \ldots, n\}$. Then, by the transitivity of equinumerousness, $\{1, \ldots, m\}$ is equinumerous to $\{1, \ldots, n\}$. Therefore, by Lemma 13.23, $m = n$, as desired. ■

13.26 Remark. Theorem 13.25 gives us the right to introduce the following notation. For each finite set A, we write $\overline{\overline{A}}$ for the unique $n \in \boldsymbol{\omega}$ such that A has n elements. (n is unique by the theorem.) The

notation $\overline{\overline{A}}$ is read *the number of elements in* A or *the cardinality of* A. Later, we shall explore what $\overline{\overline{A}}$ might mean when A is infinite.[18] For the time being though, we shall only use the notation $\overline{\overline{A}}$ when A is finite.

13.27 Remark. The notation $\overline{\overline{A}}$ is not a standard way to denote the number of elements in A. I have chosen to use it simply because it is not commonly used for any other purpose. A common notation for the number of elements in A is $|A|$. Sometime this notation is more convenient than $\overline{\overline{A}}$ but obviously it can be confused with the notation for absolute value. Usually, though, it would be clear from the context how $|A|$ is to be interpreted.

13.28 Remark. If A and B are finite sets, then $\overline{\overline{A}} = \overline{\overline{B}}$ if and only if A is equinumerous to B. This follows easily from the symmetry and transitivity of equinumerousness.

13.29 Lemma. *Let A be a set with $n+1$ elements, where $n \in \boldsymbol{\omega}$. Then A is not empty and for each $s \in A$, the set $A \setminus \{ s \}$ has n elements.*

Exercise 6. Prove Lemma 13.29. (Hint: Apply Lemma 13.22 with $B = \{ 1, \ldots, n+1 \}$.)

13.30 Theorem. *A subset of a finite set is finite and has at most as many elements as the whole set.*

Proof. To be precise, we wish to prove that for each $n \in \boldsymbol{\omega}$, $P(n)$ is true, where $P(n)$ is the sentence

$$\text{For each set } B, \text{ if } B \text{ has } n \text{ elements, then for each } A \subseteq B,\ A \text{ is finite and } \overline{\overline{A}} \leq n.$$

We shall show this by induction.

BASE CASE: $P(0)$ is true, because for each set B, if B has 0 elements, then $B = \emptyset$, so for each $A \subseteq B$, we have $A = \emptyset$, so A is finite and $\overline{\overline{A}} = 0 = \overline{\overline{B}}$.

INDUCTIVE STEP: Let $n \in \boldsymbol{\omega}$ such that $P(n)$ is true. Consider any set B. Suppose B has $n+1$ elements. Let $A \subseteq B$. We wish to show that A is finite and $\overline{\overline{A}} \leq n+1$. Either $A = \emptyset$ or $A \neq \emptyset$.

Case 1. Suppose $A = \emptyset$. Then A is finite and $\overline{\overline{A}} = 0 \leq n+1$.

Case 2. Suppose $A \neq \emptyset$. Let $s \in A$, let $A' = A \setminus \{ s \}$, and let $B' = B \setminus \{ s \}$. Then B' has n elements, by Lemma 13.29, and $A' \subseteq B'$. Hence, by the inductive hypothesis, A' is finite and $\overline{\overline{A'}} \leq n$. Now $A = A' \cup \{ s \}$ and $s \notin A'$, so by Lemma 13.20, A is finite and $\overline{\overline{A}} = \overline{\overline{A'}} + 1$. Since $\overline{\overline{A'}} \leq n$, it follows that $\overline{\overline{A}} \leq n+1$.

Thus in either case, A is finite and $\overline{\overline{A}} \leq n+1$. It follows that $P(n+1)$ is true too.

CONCLUSION: Therefore, by induction, for each $n \in \boldsymbol{\omega}$, $P(n)$ is true. ■

13.31 Corollary. *Let B be a finite set and let A be a set. Then* (a) *and* (b) *below are equivalent.*

(a) *A is equinumerous to a subset of B.*

(b) *A is finite and $\overline{\overline{A}} \leq \overline{\overline{B}}$.*

Proof. (a)⇒(b): Suppose A is equinumerous to a subset of B. Since B is finite, B has n elements, for some $n \in \boldsymbol{\omega}$. Then $\overline{\overline{B}} = n$. By assumption, we can pick a subset $C \subseteq B$ such that A is equinumerous to C. By Theorem 13.30, C is finite. Hence for some $m \in \boldsymbol{\omega}$, C has m elements. Then A has m elements too, so $\overline{\overline{A}} = m$. In particular, A is finite. Now by Theorem 13.30 (applied to C and B), $m \leq n$. In other words, $\overline{\overline{A}} \leq \overline{\overline{B}}$.

[18] Here is a preview of what $\overline{\overline{A}}$ means when A is infinite. It turns out that each order in which we can count the elements of a set gives a certain "ordinal number." When the set A is finite, Theorem 13.25 tells us that all orders in which we can count its elements give the same ordinal number, which is the cardinality of A. It turns out that when a set is infinite, counting its elements in different orders may give different ordinal numbers. For instance, the usual order in which to count the elements of the set $\boldsymbol{\omega}$ of whole numbers is $0, 1, 2, \ldots$ and the corresponding ordinal number is $\boldsymbol{\omega}$ itself. But we could also count the elements of $\boldsymbol{\omega}$ as $0, 2, 4, \ldots, 1, 3, 5, \ldots$, first counting the even ones and then counting the odd ones, and this gives the ordinal number $\boldsymbol{\omega} + \boldsymbol{\omega}$, which is bigger than $\boldsymbol{\omega}$. The cardinality of an infinite set is defined to be the smallest ordinal number that can be obtained by counting the elements of the set in any order.

(b)⇒(a): Conversely, suppose A is finite and $\overline{\overline{A}} \leq \overline{\overline{B}}$. Let $m = \overline{\overline{A}}$ and let $n = \overline{\overline{B}}$. Then A is equinumerous to A', where $A' = \{1, \ldots, m\}$, and B is equinumerous to B', where $B' = \{1, \ldots, n\}$. Now $A' \subseteq B'$ because $m \leq n$. Since B is equinumerous to B', we can pick a bijection f from B' to B. Let $C = \{f(x) : x \in A'\}$. Then $C \subseteq B$. Also, A' is equinumerous to C because the restriction of f to A' is a bijection from A' to C. Hence A is equinumerous to C, by the transitivity of equinumerousness. Thus A is equinumerous to a subset of B. ■

Exercise 7. Let A be an infinite set and let B be a set such that A is equinumerous to a subset of B. Show that B is infinite.

13.32 Remark. It is possible for an infinite set to be equinumerous to a proper subset of itself. For instance, the set $\boldsymbol{\omega} = \{0, 1, 2, \ldots\}$ is equinumerous to the proper subset $\mathbf{N} = \{1, 2, 3, \ldots\}$, because if we let $f(n) = n + 1$ for all $n \in \boldsymbol{\omega}$, then f is a bijection from $\boldsymbol{\omega}$ to $\mathbf{N}$. As the next result shows, this phenomenon does not occur for finite sets. (By the way, it is this that proves that $\boldsymbol{\omega}$ really is infinite.)

13.33 Theorem. (The rigidity property of finite sets.) *A finite set cannot be equinumerous to a proper subset of itself.*

Proof. Let B be a finite set and let A be a proper subset of B. We wish to show that B is not equinumerous to A. Suppose B is equinumerous to A. Since B is finite, B has n elements for some $n \in \boldsymbol{\omega}$. Since B is equiunumerous to A, A also has n elements. Since A is a proper subset of B, $B \setminus A$ is not empty. Let $b \in B \setminus A$ and let $C = A \cup \{b\}$. Then $C \subseteq B$ and C has $n + 1$ elements. Hence by Theorem 13.30, $n + 1 \leq n$. But $n + 1 > n$. Thus we have reached a contradiction. Therefore B must not be equinumerous to A. ■

13.34 Corollary. *An injection from a finite set to itself is a surjection.*

Proof. Let A be a finite set and let f be an injection from A to A. Let B be the range of f. Then f is a bijection from A to B. Hence A is equinumerous to B. Now B is a subset of A, because f is a function from A to A. But by Theorem 13.33, B cannot be a proper subset of A. Hence $B = A$. Thus f is a surjection from A to A. ■

13.35 Remark. We have just deduced Corollary 13.34 from Theorem 13.33. It is equally easy to deduce Theorem 13.33 from Corollary 13.34. So actually, Corollary 13.34 can be taken as an alternative formulation of the rigidity property of finite sets.

13.36 Remark. We can finally prove that the set $\boldsymbol{\omega} = \{0, 1, 2, \ldots\}$ is indeed infinite, as one would expect and as was already suggested in Remark 13.32. If $\boldsymbol{\omega}$ were finite, then it could not be equinumerous to a proper subset of itself, by Theorem 13.33. But as we have seen, $\boldsymbol{\omega}$ is equinumerous to $\mathbf{N} = \{1, 2, 3, \ldots\}$ and $\mathbf{N}$ is a proper subset of $\boldsymbol{\omega}$. Hence $\boldsymbol{\omega}$ must be infinite.

Exercise 8. Let A and B be finite sets with the same number of elements. Let f be an injection from A to B. Show that f is a bijection from A to B. (This generalizes Corollary 13.34.)

13.37 Remark. The result of the next exercise derives its name from the fact that if we think of A as a set of letters, B as a set of pigeonholes, and f as an assignment of letters to pigeonholes, then it says that if there are strictly more letters than pigeonholes, then some pigeonhole must have at least two letters in it.[19]

Exercise 9. (*The pigeonhole principle.*) Let A be a set with m elements and let B be a set with n elements, where $m, n \in \boldsymbol{\omega}$ and $m > n$. Suppose f is a function from A to B. Show that f is not an injection.

Exercise 10. Answer the following questions. Your answers to parts (c) and (d) should include careful explanations.

(a) How many days are there in 52 weeks?
(b) Is it completely accurate to say that there are 52 weeks in a year?
(c) How many Saturdays are there in a year? (Warning: There are two possible answers. One of these answers is less likely than the other, though it is less unlikely in a leap year.)

[19] Here *pigeonholes* means *letterboxes*.

(d) Each month has at least four Saturdays and at most five. How many months have five Saturdays? (Note: As in part (c), there are two possible answers.)

13.38 Theorem. *Let B be a finite set and let f be a function on B. Then f has a right inverse. In other words, there is a function $g\colon A \to B$, where $A = f[B]$, such that for each $x \in A$, we have $f(g(x)) = x$.*

Proof. Since B is finite, B is equinumerous to $\{1, \ldots, n\}$ for some $n \in \boldsymbol{\omega}$.

First consider the special case where $B = \{1, \ldots, n\}$. For each $x \in A$, the set $f^{-1}[\{x\}]$ is a nonempty subset of $\mathbf{N}$, so it has a least element, by Exercise 4(b) in Section 7. Thus we may define $g\colon A \to B$ by letting $g(x)$ be the least element of $f^{-1}[\{x\}]$. Now for each $x \in A$, since $g(x) \in f^{-1}[\{x\}]$, we have $f(g(x)) = x$. Thus g is a right inverse for f.

Now consider the general case. Let $B' = \{1, \ldots, n\}$. Then B is equinumerous to B', so by the symmetry of equinumerousness, B' is equinumerous to B, so there is a bijection h from B' to B. In particular, h is a surjection from B' to B. Let $f' = f \circ h$. Then f' is a surjection from B' to A and by the first part of the proof, there is a function $g'\colon A \to B'$ such that for each $x \in A$, we have $f'(g'(x)) = x$. Let $g = h \circ g'$. Then $g\colon A \to B$ and for each $x \in A$, we have $f(g(x)) = f(h(g'(x))) = f'(g'(x)) = x$. Thus g is a right inverse for f. ■

13.39 Remark. In Theorem 13.38, we can drop the assumption that B is finite, provided we use the axiom of choice to select an element $g(x)$ in $f^{-1}[\{x\}]$ for each $x \in A$. Actually, the statement that every function has a right inverse is easily seen to be equivalent to the axiom of choice.

13.40 Theorem. *A right inverse for a function is an injection.*

Proof. Let B be a set, let f be a function on B, let $A = f[B]$, and suppose g is a right inverse for f. Then $g\colon A \to B$ and for each $x \in A$, we have $f(g(x)) = x$. Hence for all $x_1, x_2 \in A$, if $g(x_1) = g(x_2)$, then $x_1 = f(g(x_1)) = f(g(x_2)) = x_2$. Thus g is an injection, as we wished to show. ■

Exercise 11. Let B be a finite set, let f be a function on B, and let $A = f[B]$. Prove that A is finite and $\overline{\overline{A}} \leq \overline{\overline{B}}$. (Hint: Use Theorem 13.38, Theorem 13.40, and Corollary 13.31.)

Exercise 12. Prove the converse of Corollary 13.34. In other words, let A be a finite set and let f be a surjection from A to itself. Show that f is an injection. (Hint: Use Theorem 13.38, Theorem 13.40, and Corollary 13.34.)

Exercise 13. Let A and B be finite sets with the same number of elements. Let f be a surjection from B to A. Show that f is an injection. (This generalizes Exercise 12.)

13.41 Proposition. *Let $n \in \boldsymbol{\omega}$ and suppose $A = \{a_1, \ldots, a_n\}$. Then:*

(a) *A is finite and $\overline{\overline{A}} \leq n$.*

(b) *$\overline{\overline{A}} = n$ iff $a_1, \ldots, a_n$ are distinct.*

Proof. (a) Let $B = \{1, \ldots, n\}$. Define f on B by $f(k) = a_k$. Then $A = f[B]$. By Exercise 11, A is finite and $\overline{\overline{A}} \leq \overline{\overline{B}}$. But $\overline{\overline{B}} = n$. Hence $\overline{\overline{A}} \leq n$.

(b) The function f just defined is a surjection from B to A. Suppose $\overline{\overline{A}} = n$. Then A and B have the same number of elements, namely n. Hence, by Exercise 13, f is an injection, so $a_1, \ldots, a_n$ are distinct. Conversely, if $a_1, \ldots, a_n$ are distinct, then as we already saw in Proposition 13.16, A has n elements, so $\overline{\overline{A}} = n$. ■

13.42 Proposition. (The addition rule.) *Let A and B be finite sets. If $A \cap B$ is empty, then $A \cup B$ is finite and*

$$\overline{\overline{A \cup B}} = \overline{\overline{A}} + \overline{\overline{B}}.$$

Proof. Let us hold A fixed and think of B as varying. Let $m = \overline{\overline{A}}$. Then it suffices to prove that for each $n \in \boldsymbol{\omega}$, $P(n)$ is true, where $P(n)$ is the sentence

> for each set B, if $A \cap B$ is empty and B has n elements, then $A \cup B$ has $m + n$ elements.

We shall show this by induction.

BASE CASE: First note that $P(0)$ is true because if B is a set with 0 elements, then B is empty, so $A \cup B = A$, so since A has m elements, $A \cup B$ has $m + 0$ elements.

INDUCTIVE STEP: Now let $n \in \boldsymbol{\omega}$ such that $P(n)$ is true. Under this inductive hypothesis, we wish to show that $P(n+1)$ is true. Consider any set B. Suppose $A \cap B$ is empty and B has $n+1$ elements. We wish to show that $A \cup B$ has $m + n + 1$ elements. Now B is not empty, because B has $n+1$ elements and $n + 1 \geq 1$. Hence we may pick $t \in B$. Let $B_0 = B \setminus \{ t \}$. Then $A \cap B_0$ is empty too and B_0 has n elements. Hence by the inductive hypothesis, $A \cup B_0$ has $m + n$ elements. Hence $(A \cup B_0) \cup \{ t \}$ has $m + n + 1$ elements, since $t \notin A \cup B_0$. But $(A \cup B_0) \cup \{ t \} = A \cup B$. Thus $A \cup B$ has $m + n + 1$ elements, as desired. Thus $P(n+1)$ is true.

CONCLUSION: Therefore, by induction, for each $n \in \boldsymbol{\omega}$, $P(n)$ is true. ■

13.43 Corollary. *Let A and B be finite sets. Then $A \cup B$ is finite.*

Proof. Let $D = B \setminus A$. Then D is a subset of the finite set B, so D is finite. Now A is finite too and $A \cap D$ is empty. Hence by Proposition 13.42, $A \cup D$ is finite. But $A \cup D = A \cup B$. Hence $A \cup B$ is finite. ■

13.44 Corollary. *A union of finitely many finite sets is finite.*

Proof. To be precise, what we want to prove is that for each $n \in \boldsymbol{\omega}$, $P(n)$ is true, where $P(n)$ is the sentence

> for each set A, if A has n elements, then for each family of finite sets $(C_\alpha)_{\alpha \in A}$ indexed by A, the set $\bigcup_{\alpha \in A} C_\alpha$ is finite.

We shall show this by induction.

BASE CASE: First, $P(0)$ is true because if A is a set with 0 elements and $(C_\alpha)_{\alpha \in A}$ is a family of sets indexed by A, then $A = \emptyset$, so $\bigcup_{\alpha \in A} C_\alpha = \emptyset$, which is a finite set.

INDUCTIVE STEP: Now let $n \in \boldsymbol{\omega}$ such that $P(n)$ is true. Under this inductive hypothesis, we wish to show that $P(n+1)$ is true. Consider any set A with $n+1$ elements and any family of finite sets $(C_\alpha)_{\alpha \in A}$ indexed by A. Then $A \neq \emptyset$ because $n + 1 \geq 1$. Hence we may pick $\alpha_0 \in A$. Let $A' = A \setminus \{ \alpha_0 \}$. Then A' has n elements. Let $S = \bigcup_{\alpha \in A'} C_\alpha$ and let $T = C_{\alpha_0}$. By the inductive hypothesis, S is finite. By assumption, T is finite. Hence by Corollary 13.44, $S \cup T$ is finite. But $S \cup T = \bigcup_{\alpha \in A} C_\alpha$. Hence $\bigcup_{\alpha \in A} C_\alpha$ is finite. Thus $P(n+1)$ is true.

CONCLUSION: Therefore, by induction, for each $n \in \mathbf{N}$, $P(n)$ is true. This completes the proof. ■

Exercise 14. (*The generalized addition rule.*) Prove that for each $n \in \boldsymbol{\omega}$, for each set A, if A has n elements, then for each family $(C_\alpha)_{\alpha \in A}$ of pairwise disjoint finite sets indexed by A, we have

$$\overline{\overline{\bigcup_{\alpha \in A} C_\alpha}} = \sum_{\alpha \in A} \overline{\overline{C_\alpha}}.$$

(Hint: Show that this follows from Proposition 13.42 by induction on n. If you get stuck, work through the proof of Corollary 13.44 and then try again.)

Exercise 15. (*The multiplication rule.*) Let $n \in \boldsymbol{\omega}$, let A be a set with n elements, and let $(C_\alpha)_{\alpha \in A}$ be a family of pairwise disjoint finite sets indexed by A, all of which have the same number of elements: say $\overline{\overline{C_\alpha}} = \gamma$ for all $\alpha \in A$, where $\gamma \in \boldsymbol{\omega}$. Use Exercise 14, the generalized addition rule, to show that $\bigcup_{\alpha \in A} C_\alpha$ has $n\gamma$ elements.

Section 14. Applications of the Principles of Counting

In this section, our main goal is to apply the fundamental principles from the previous section (especially the addition rule and the multiplication rule) to establish the basic formulas for numbers of combinations and numbers of permutations. (We recall the definitions of these notions below.)

Recall that for any set A, the power set of A (denoted $\mathscr{P}(A)$) is the set of all subsets of A. In combinatorics, a subset of A is also called *a combination of elements of* A, so the power set of A is also called *the set of combinations of elements of* A. (Do not forget that the empty combination is one of the combinations of elements of A.) Remember that all that matters about a set is which objects belong to it, not the order in which these objects may be listed in a particular description of the set. Thus a combination of elements of A is an unordered selection of elements of A.

14.1 Example. A subset of the set $\{1,2,3\}$ either contains the element 3 or it does not, and these two possibilities are mutually exclusive. Hence $\mathscr{P}(\{1,2,3\})$, the power set of $\{1,2,3\}$, is equal to $\mathscr{B}\cup\mathscr{C}$ where

$$\mathscr{B} = \big\{\, \varnothing,\, \{1\},\, \{2\},\, \{1,2\} \,\big\},$$
$$\mathscr{C} = \big\{\, \{3\},\, \{1,3\},\, \{2,3\},\, \{1,2,3\} \,\big\},$$

and the two sets $\mathscr{B}$ and $\mathscr{C}$ are disjoint. Notice that $\mathscr{B} = \mathscr{P}(\{1,2\})$. Also notice that there is an obvious bijection from $\mathscr{C}$ to $\mathscr{B}$, which is given by removing the element 3 from each of the elements of $\mathscr{C}$. Hence $\mathscr{C}$ is equinumerous to $\mathscr{B} = \mathscr{P}(\{1,2\})$. Thus by the addition rule, $\mathscr{P}(\{1,2,3\})$ has twice as many elements as $\mathscr{P}(\{1,2\})$. More generally, by similar reasoning, if A is any finite set and $r \in A$, and if $A_0 = A \setminus \{r\}$, then $\mathscr{P}(A)$ has twice as many elements as $\mathscr{P}(A_0)$. This observation is the key to the proof of the next result.

14.2 Proposition. (The number of combinations of n objects.) *If A is a set with n elements, where $n \in \boldsymbol{\omega}$, then $\mathscr{P}(A)$ has 2^n elements.*

Proof. To be precise, what we want to show is that for each $n \in \boldsymbol{\omega}$, $P(n)$ is true, where $P(n)$ is the sentence

$$\text{for each set } A, \text{ if } A \text{ has } n \text{ elements, then } \mathscr{P}(A) \text{ has } 2^n \text{ elements.}$$

We shall show this by induction.

BASE CASE: First note that $P(0)$ is true, because if A is a set with 0 elements, then $A = \varnothing$, so $\mathscr{P}(A) = \{\varnothing\}$, so $\mathscr{P}(A)$ has 1 element, and $1 = 2^0$.

INDUCTIVE STEP: Now let $n \in \boldsymbol{\omega}$ such that $P(n)$ is true. Under this inductive hypothesis, we wish to prove that $P(n+1)$ is true. Consider any set A. Suppose A has $n+1$ elements. Then A is not empty, so we may pick $r \in A$. Let $A_0 = A \setminus \{r\}$. Then A_0 has n elements, so by the inductive hypothesis, $\mathscr{P}(A_0)$ has 2^n elements. Let

$$\mathscr{B} = \{\, S \subseteq A : r \notin S \,\},$$
$$\mathscr{C} = \{\, S \subseteq A : r \in S \,\}.$$

Notice that $\mathscr{B} = \mathscr{P}(A_0)$, so $\mathscr{B}$ has 2^n elements. Notice also that $\mathscr{C}$ is equinumerous to $\mathscr{P}(A_0)$, because if we let $f(S) = S \setminus \{r\}$ for all $S \in \mathscr{C}$, then f is a bijection from $\mathscr{C}$ to $\mathscr{P}(A_0)$. Hence $\mathscr{C}$ has 2^n elements too. Finally, notice that $\mathscr{B}\cup\mathscr{C} = \mathscr{P}(A)$ and $\mathscr{B}\cap\mathscr{C}$ is empty. Hence, since $\mathscr{B}$ has 2^n elements and $\mathscr{C}$ has 2^n elements, it follows that $\mathscr{P}(A)$ has $2^n + 2^n$ elements, by the addition rule. But $2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$. Hence $\mathscr{P}(A)$ has 2^{n+1} elements. Thus $P(n+1)$ is true.

CONCLUSION: Therefore, by induction, for each $n \in \boldsymbol{\omega}$, $P(n)$ is true. This completes the proof. ■

Exercise 1. Let $A, r, A_0, \mathscr{B}, \mathscr{C}, f$ be as in the preceding proof.

- **(a)** Verify that $\mathscr{B} = \mathscr{P}(A_0)$.
- **(b)** Verify that f is a bijection from $\mathscr{C}$ to $\mathscr{P}(A_0)$.
- **(c)** Verify that $\mathscr{B}\cup\mathscr{C} = \mathscr{P}(A)$.
- **(d)** Verify that $\mathscr{B}\cap\mathscr{C}$ is empty.

(If you get stuck, work through Example 14.1 and then try again.)

For each set A and each $k \in \boldsymbol{\omega}$, let us write $\mathscr{P}_k(A)$ for the set of all k-element subsets of A. In other words,

$$\mathscr{P}_k(A) = \{\, S \subseteq A : S \text{ has } k \text{ elements} \,\}.$$

(This notation is not standard but it will be convenient in the next few exercises.) In combinatorics, a k-element subset of A is also called *a combination of elements of A taken k at a time* or more briefly *a k-combination of elements of A*, so $\mathscr{P}_k(A)$ is called *the set of k-combinations of elements of A* or *the set of combinations of elements of A taken k at a time*.

14.3 Example. A 2-element subset of the set $\{\,1,2,3,4,5\,\}$ either contains the element 5 or it does not, and these two possibilities are mutually exclusive. Hence $\mathscr{P}_2(\{\,1,2,3,4,5\,\})$, the set of 2-element subsets of $\{\,1,2,3,4,5\,\}$, is equal to $\mathscr{B} \cup \mathscr{C}$ where

$$\mathscr{B} = \big\{\, \{\,1,2\,\}, \{\,1,3\,\}, \{\,1,4\,\}, \{\,2,3\,\}, \{\,2,4\,\}, \{\,3,4\,\} \,\big\},$$
$$\mathscr{C} = \big\{\, \{\,1,5\,\}, \{\,2,5\,\}, \{\,3,5\,\}, \{\,4,5\,\} \,\big\},$$

and the two sets $\mathscr{B}$ and $\mathscr{C}$ are disjoint. Notice that $\mathscr{B} = \mathscr{P}_2(\{\,1,2,3,4\,\})$, the set of 2-element subsets of $\{\,1,2,3,4\,\}$. Also notice that there is an obvious bijection from $\mathscr{C}$ to $\mathscr{P}_1(\{\,1,2,3,4\,\})$, the set of 1-element subsets of $\{\,1,2,3,4\,\}$, which is given by removing the element 5 from each of the elements of $\mathscr{C}$. Hence $\mathscr{C}$ is equinumerous to $\mathscr{P}_1(\{\,1,2,3,4\,\})$. Thus by the addition rule, the number of elements in $\mathscr{P}_2(\{\,1,2,3,4,5\,\})$ is the sum of the number of elements in $\mathscr{P}_2(\{\,1,2,3,4\,\})$ and the number of elements in $\mathscr{P}_1(\{\,1,2,3,4\,\})$.

Exercise 2. Let A be a set. Suppose $r \in A$. Let $A_0 = A \setminus \{\,r\,\}$. Let $k \in \mathbf{N}$ and let

$$\mathscr{B} = \{\, S \in \mathscr{P}_k(A) : r \notin S \,\},$$
$$\mathscr{C} = \{\, S \in \mathscr{P}_k(A) : r \in S \,\}.$$

Verify the following assertions.

(a) $\mathscr{B} = \mathscr{P}_k(A_0)$.

(b) $\mathscr{C}$ is equinumerous to $\mathscr{P}_{k-1}(A_0)$.

(c) $\mathscr{B} \cup \mathscr{C} = \mathscr{P}_k(A)$.

(d) $\mathscr{B} \cap \mathscr{C}$ is empty.

(If you get stuck, work through Example 14.3 and then try again.)

Exercise 3. (*The number of combinations of n objects taken k at a time.*) Prove that for each $n \in \boldsymbol{\omega}$, for each $k \in \{\,0,\ldots,n\,\}$, for each set A, if A has n elements, then $\mathscr{P}_k(A)$ has $\binom{n}{k}$ elements. (Hint: This can be proved by induction on n. Review the properties of Pascal's triangle. In the inductive step, when $k \in \{\,1,\ldots,n\,\}$, Exercise 2 should help. The cases $k = 0$ and $k = n+1$ require a separate argument but are easy.)

Exercise 4. Let $n \in \mathbf{N}$. Give two proofs that $\sum_{k=0}^{n} \binom{n}{k} = 2^n$. For the first proof, apply the binomial theorem to expand $(a+b)^n$ and specialize to the case where $a = 1 = b$. (This first proof is a repetition of an earlier exercise.) For the second proof, combine the result of Exercise 3 with what you know about the total number of subsets of $\{\,1,\ldots,n\,\}$.

Exercise 5. Use the result of Exercise 3 to give alternative proofs of the following results about binomial coefficients that were previously proved by induction.

(a) For each $n \in \mathbf{N}$,

$$\binom{n}{1} = n \quad \text{and} \quad \binom{n}{n-1} = n.$$

(b) For each $n \in \boldsymbol{\omega}$, for each $k \in \{\,0,\ldots,n\,\}$,

$$\binom{n}{k} = \binom{n}{n-k}.$$

Recall that if A and B are sets, then their cartesian product (denoted $A \times B$) is the set of all ordered pairs (x, y) such that $x \in A$ and $y \in B$; in other words,

$$A \times B = \{\, (x, y) : x \in A \text{ and } y \in B \,\}.$$

14.4 Example. Suppose $A = \{\, 4, 5, 6 \,\}$ and $B = \{\, 1, 2, 3, 4 \,\}$. Then the possible values for the first entry x of an ordered pair (x, y) belonging to $A \times B$ are 4, 5 and 6, and these three possibilities are mutually exclusive. Thus $A \times B = C_4 \cup C_5 \cup C_6$ where

$$\begin{aligned} C_4 &= \{\, (4,1),\ (4,2),\ (4,3),\ (4,4) \,\}, \\ C_5 &= \{\, (5,1),\ (5,2),\ (5,3),\ (5,4) \,\}, \\ C_6 &= \{\, (6,1),\ (6,2),\ (6,3),\ (6,4) \,\}, \end{aligned}$$

and the sets C_4, C_5, C_6 are pairwise disjoint. Notice that if we map each of the ordered pairs $(4, y)$ in C_4 to its second entry y, this defines a bijection from C_4 to $B = \{\, 1, 2, 3, 4 \,\}$. Hence C_4 is equinumerous to B. Similary, C_5 is equinumerous to B and C_6 is equinumerous to B. Thus each of the sets C_5, C_6, and C_7 has 4 elements. Hence by the multiplication rule, the union of these 3 disjoint sets has $3 \cdot 4 = 12$ elements. In other words, $A \times B$ has 12 elements. Of course in this concrete example, this is obvious just by counting the elements of $A \times B$. However the purpose of this example is to illustrate the key ideas that are needed for the solution of the next exercise.

Exercise 6. Let A and B be finite sets. Use the multiplication rule (Exercise 15 in Section 13) to show that $A \times B$ is finite and

$$\overline{\overline{A \times B}} = \overline{\overline{A}} \cdot \overline{\overline{B}}.$$

(Hint: Let $m = \overline{\overline{A}}$ and $n = \overline{\overline{B}}$. For all $\alpha \in A$, let $C_\alpha = \{\, \alpha \,\} \times B$. Show that the family $(C_\alpha)_{\alpha \in A}$ is pairwise disjoint and that $\bigcup_{\alpha \in A} C_\alpha = A \times B$. For each $\alpha \in A$, show that C_α is equinumerous to B, by defining a suitable bijection Ψ_α from C_α to B. Deduce that for each $\alpha \in A$, $\overline{\overline{C_\alpha}} = n$.)

Recall that if A and B are sets, then B^A denotes the set of all functions from A to B. In particular, if $k \in \mathbf{N}$, then $B^{\{1,\ldots,k\}}$ is the set of all sequences of length k consisting of elements of B or more briefly, the set of all k-sequences of elements of B; in other words,

$$B^{\{1,\ldots,k\}} = \{\, \langle\, y_1, \ldots, y_k \,\rangle : y_1 \in B, \ldots, y_k \in B \,\}.$$

We emphasize once again that in a k-sequence $\langle\, y_1, \ldots, y_k \,\rangle$, the order of the terms $y_1, \ldots, y_k$ matters, the terms need not all be distinct, and repetitions count.

Note that $B^\varnothing$ is not empty. Rather, $B^\varnothing = \{\, \varnothing \,\}$. The empty set is also the empty function and is a function from the empty set to any set B. Thus $B^\varnothing$ has one element. This is analogous to the convention that for any number c, $c^0 = 1$. (Even $0^0 = 1$.)

It will be convenient to extend the sequence notation, which we have used to denote functions defined on the set $\{\, 1, \ldots, n \,\}$ where $n \in \mathbf{N}$, to denote functions whose domains are subsets of $\{\, 1, \ldots, n \,\}$. To this end, we shall use the symbol $\_$ to denote places where a function defined on a subset of $\{\, 1, \ldots, n \,\}$ is undefined. For instance, if $f = \langle\, \_, 8, 7 \,\rangle$, then f is undefined at 1, $f(2) = 8$, $f(3) = 7$, and the domain of f is $\{\, 2, 3 \,\}$.

14.5 Example. Suppose $A = \{\, 1, 2, 3 \,\}$ and $B = \{\, 5, 7 \,\}$. Then the elements of B^A are the sequences of length 3 consisting of elements of the set $B = \{\, 5, 7 \,\}$. The possible values for the first entry in such a sequence are 5 and 7, and these two possibilities are mutually exclusive. Hence $B^A = C_5 \cup C_7$ where

$$\begin{aligned} C_5 &= \{\, \langle 5,5,5 \rangle,\ \langle 5,5,7 \rangle,\ \langle 5,7,5 \rangle,\ \langle 5,7,7 \rangle \,\}, \\ C_7 &= \{\, \langle 7,5,5 \rangle,\ \langle 7,5,7 \rangle,\ \langle 7,7,5 \rangle,\ \langle 7,7,7 \rangle \,\}, \end{aligned}$$

and C_5 and C_7 are disjoint. Let $A_0 = A \setminus \{\, 1 \,\}$. Then $A_0 = \{\, 2, 3 \,\}$ and B^{A_0} is

$$\{\, 5, 7 \,\}^{\{2,3\}} = \{\, \langle \_, 5, 5 \rangle,\ \langle \_, 5, 7 \rangle,\ \langle \_, 7, 5 \rangle,\ \langle \_, 7, 7 \rangle \,\}.$$

Notice that there is an obvious bijection Ψ_5 from C_5 to B^{A_0}, which is given by restricting each of the sequences in C_5 to the subset $\{2,3\} \subseteq \{1,2,3\}$; in other words, $\Psi_5(f) = f \restriction A_0$ for all $f \in C_5$. (Recall that $f \restriction A_0$ denotes the restriction of the function f to the subset A_0 of its domain.) There is also a similarly defined obvious bijection Ψ_7 from C_7 to B^{A_0}. Thus each of the two disjoint sets C_5 and C_7 is equinumerous to B^{A_0}. Hence by the multiplication rule, $C_5 \cup C_7$ has twice as many elements as B^{A_0}. In other words, B^A has twice as many elements as B^{A_0}. Of course in this concrete example, this is obvious just by counting the elements of B^A and B^{A_0}. However the purpose of this example is to illustrate some of the key ideas that are needed in the inductive step of the solution of the next exercise.

Exercise 7. (*The exponentiation rule.*) Show that if A and B are finite sets, then B^A is finite and

$$\overline{\overline{B^A}} = \overline{\overline{B}}^{\overline{A}}.$$

(Hint: Hold B fixed and think of A as varying. Let $n = \overline{\overline{B}}$. Prove by induction that for each $m \in \boldsymbol{\omega}$, for each set A, if A has m elements, then B^A has n^m elements. In the inductive step, the multiplication rule may be applied by virtue of the following reasoning. Suppose A has $m+1$ elements, $r \in A$, and $A_0 = A \setminus \{r\}$. Then B^A may be expressed as the union of the n disjoint sets

$$C_\beta = \big\{ f \in B^A : f(r) = \beta \big\}, \qquad \beta \in B.$$

Moreover each C_β has n^m elements by the inductive hypothesis because C_β is equinumerous to B^{A_0}, since if we let $\Psi_\beta(f) = f \restriction A_0$ for all $f \in C_\beta$, then Ψ_β is a bijection from C_β to B^{A_0}. If you have trouble filling in the details, work through Example 14.5 and then try again.)

If A is a set and $S \subseteq A$, then *the indicator function for* S is the function from A to $\{0,1\}$ that takes the value 1 at each point in S and that takes the value 0 at each point in $A \setminus S$; in other words, for all $x \in A$,

$$1_S(x) = \begin{cases} 1 & \text{if } x \in S; \\ 0 & \text{if } x \notin S. \end{cases}$$

14.6 Proposition. *For each set A, $\mathscr{P}(A)$ is equinumerous to $\{0,1\}^A$.*

Proof. Note that for each $S \in \mathscr{P}(A)$, 1_S belongs to $\{0,1\}^A$. Hence we may define a function f from $\mathscr{P}(A)$ to $\{0,1\}^A$ by $f(S) = 1_S$ for all $S \in \mathscr{P}(A)$. Then f is a bijection from $\mathscr{P}(A)$ to $\{0,1\}^A$. Hence $\mathscr{P}(A)$ is equinumerous to $\{0,1\}^A$. ■

Exercise 8. Let A and f be as in the preceding proof. Verify that f is indeed a bijection from $\mathscr{P}(A)$ to $\{0,1\}^A$.

14.7 Remark. The importance of Proposition 14.6 is twofold. First, it applies even if the set A is infinite, and we shall have occasion later to use it in this case. Second, when A is a finite set, say with n elements, then by the exponentiation rule, the set $\{0,1\}^A$ has 2^n elements, and by combining this with Proposition 14.6, we get an alternative proof that $\mathscr{P}(A)$ has 2^n elements.

Recall that if $(B_\alpha)_{\alpha \in A}$ is an indexed family of sets, then a choice function for $(B_\alpha)_{\alpha \in A}$ is a function f such that the domain of f is A and for each $\alpha \in A$, we have $f(\alpha) \in B_\alpha$. Informally, we may say that a choice function for $(B_\alpha)_{\alpha \in A}$ is a function that "chooses" an element of B_α for each $\alpha \in A$. Recall also that the cartesian product of the indexed family $(B_\alpha)_{\alpha \in A}$ is

$$\prod_{\alpha \in A} B_\alpha = \{ f : f \text{ is a choice function for } (B_\alpha)_{\alpha \in A} \}.$$

This makes sense even if the index set A is infinite. However in this section, we shall mainly be concerned with finite index sets. In the special case where $A = \{1, \ldots, n\}$, with $n \in \mathbf{N}$, such an indexed family of sets $(B_\alpha)_{\alpha \in A}$ is an n-sequence of sets $\langle B_1, \ldots, B_n \rangle$ and a choice function for such an n-sequence of sets is an n-sequence of objects $\langle y_1, \ldots, y_n \rangle$ such that $y_1 \in B_1, \ldots, y_n \in B_n$.

The $\prod$ notation is also used to denote the ordinary product of numbers, as in $\prod_{k=1}^n c_k = c_1 c_2 \cdots c_n$. You should be able to infer from the context which meaning $\prod$ has.

14.8 Example. Let $A = \{1,2,3\}$ and let $B_1 = \{4,5,6\}$, $B_2 = \{5,6\}$, and $B_3 = \{4,5\}$. Then the cartesian product $\prod_{\alpha\in A} B_\alpha$ is the set of sequences of length 3 consisting of an element of B_1, an element of B_2 and an element of B_3, in that order. The possible values for the first entry of such a sequence are 4, 5 and 6, and these three possibilities are mutually exclusive. Hence $\prod_{\alpha\in A} B_\alpha = C_4 \cup C_5 \cup C_6$ where

$$\begin{aligned} C_4 &= \{\langle 4,5,4\rangle, \langle 4,5,5\rangle, \langle 4,6,4\rangle, \langle 4,6,5\rangle\}, \\ C_5 &= \{\langle 5,5,4\rangle, \langle 5,5,5\rangle, \langle 5,6,4\rangle, \langle 5,6,5\rangle\}, \\ C_6 &= \{\langle 6,5,4\rangle, \langle 6,5,5\rangle, \langle 6,6,4\rangle, \langle 6,6,5\rangle\}, \end{aligned}$$

and the sets C_4, C_5, C_6 are pairwise disjoint. Let $A_0 = A \setminus \{1\}$. Then $A_0 = \{2,3\}$ and

$$\prod_{\alpha\in A_0} B_\alpha = \{\langle \_,5,4\rangle, \langle \_,5,5\rangle, \langle \_,6,4\rangle, \langle \_,6,5\rangle\}.$$

Notice that there is an obvious bijection Ψ_4 from C_4 to $\prod_{\alpha\in A_0} B_\alpha$, which is given by restricting each of the sequences in C_4 to the subset $\{2,3\} \subseteq \{1,2,3\}$; in other words, $\Psi_4(f) = f \restriction A_0$ for all $f \in C_4$. (An equivalent but less succinct way to define Ψ_4 is to say that $\Psi_4(\langle 4,x,y\rangle) = \langle \_,x,y\rangle$ for all $x \in B_2$ and all $y \in B_3$.) There are also similarly defined obvious bijections Ψ_5 and Ψ_6 from C_5 and C_6 respectively to $\prod_{\alpha\in A_0} B_\alpha$. Thus each of the three disjoint sets C_4, C_5, and C_6 is equinumerous to $\prod_{\alpha\in A_0} B_\alpha$. Hence by the multiplication rule, the set $C_4 \cup C_5 \cup C_6$ has three times as many elements as $\prod_{\alpha\in A_0} B_\alpha$. In other words, $\prod_{\alpha\in A} B_\alpha$ has three times as many elements as $\prod_{\alpha\in A_0} B_\alpha$.

Exercise 9. (*The generalized multiplication rule.*) Prove that for each $n \in \mathbf{N}$, for each set A, if A has n elements, then for each family of finite sets $(B_\alpha)_{\alpha\in A}$ indexed by A, the cartesian product $\prod_{\alpha\in A} B_\alpha$ is finite and

$$\overline{\overline{\prod_{\alpha\in A} B_\alpha}} = \prod_{\alpha\in A} \overline{\overline{B_\alpha}}.$$

(Hint: This can be proved by induction on n, by a generalization of the method that was suggested to prove the exponentiation rule. If you get stuck, work through Example 14.8 and then try again.)

For any sets A and B, let $\mathrm{inj}(A,B)$ denote the set of injections from A to B and let $\mathrm{bij}(A,B)$ denote the set of bijections from A to B. This is not standard notation but it will be convenient in the next few exercises. Note that if $k \in \mathbf{N}$, then an injection f from $\{1,\ldots,k\}$ to B may be thought of as an ordered list $f(1),\ldots,f(k)$ of k distinct elements of B. In combinatorics, an injection from $\{1,\ldots,k\}$ to B is called *a permutation of elements of B taken k at a time* or more briefly *a k-permutation of elements of B*, so $\mathrm{inj}(\{1,\ldots,k\},B)$ is called *the set of k-permutations of elements of B* or *the set of permutations of elements of B taken k at a time*. By the way, $\mathrm{inj}(\emptyset,B)$ is not empty. Rather, $\mathrm{inj}(\emptyset,B) = \{\emptyset\}$, so $\mathrm{inj}(\emptyset,B)$ has one element. The empty set is also the empty function and is an injection from the empty set to any set B.

14.9 Example. Suppose $A = \{1,2,3\}$ and $B = \{4,5,6,7\}$. Then $\mathrm{inj}(A,B)$, the set of injections from A to B, is the set of sequences of length 3 consisting of distinct elements of the set $\{4,5,6,7\}$. The possible values for the first entry of such a sequence are 4, 5, 6 and 7, and these four possibilities are mutually exclusive. Hence $\mathrm{inj}(A,B) = C_4 \cup C_5 \cup C_6 \cup C_7$ where

$$\begin{aligned} C_4 &= \{\langle 4,5,6\rangle, \langle 4,5,7\rangle, \langle 4,6,5\rangle, \langle 4,6,7\rangle, \langle 4,7,5\rangle, \langle 4,7,6\rangle\}, \\ C_5 &= \{\langle 5,4,6\rangle, \langle 5,4,7\rangle, \langle 5,6,4\rangle, \langle 5,6,7\rangle, \langle 5,7,4\rangle, \langle 5,7,6\rangle\}, \\ C_6 &= \{\langle 6,4,5\rangle, \langle 6,4,7\rangle, \langle 6,5,4\rangle, \langle 6,5,7\rangle, \langle 6,7,4\rangle, \langle 6,7,5\rangle\}, \\ C_7 &= \{\langle 7,4,5\rangle, \langle 7,4,6\rangle, \langle 7,5,4\rangle, \langle 7,5,6\rangle, \langle 7,6,4\rangle, \langle 7,6,5\rangle\}, \end{aligned}$$

and the sets C_4, C_5, C_6, C_7 are pairwise disjoint. Let $A_0 = A \setminus \{1\}$. Then $A_0 = \{2,3\}$. Notice that there is an obvious bijection Ψ_4 from C_4 to

$$\begin{aligned} &\mathrm{inj}(A_0, B \setminus \{4\}) = \mathrm{inj}(\{2,3\},\{5,6,7\}) \\ &\quad = \{\langle \_,5,6\rangle, \langle \_,5,7\rangle, \langle \_,6,5\rangle, \langle \_,6,7\rangle, \langle \_,7,5\rangle, \langle \_,7,6\rangle\}, \end{aligned}$$

which is given by restricting each of the sequences in C_4 to the subset $\{2,3\} \subseteq \{1,2,3\}$; in other words, $\Psi_4(f) = f \restriction A_0$ for all $f \in C_4$. There are also similarly defined obvious bijections Ψ_5 from C_5 to $\mathrm{inj}(A_0, B \setminus \{5\})$, Ψ_6 from C_6 to $\mathrm{inj}(A_0, B \setminus \{6\})$, and Ψ_7 from C_7 to $\mathrm{inj}(A_0, B \setminus \{7\})$. Thus each of the four disjoint sets C_4, C_5, C_6, and C_7 is equinumerous to the set of injections from a 2-element set to a 3-element set. Hence by the multiplication rule, the set $C_4 \cup C_5 \cup C_6 \cup C_7$ has four times as many elements as the set of injections from a 2-element set to a 3-element set. In other words, $\mathrm{inj}(A, B)$ has four times as many elements as the set of injections from a 2-element set to a 3-element set.

For each $n \in \boldsymbol{\omega}$ and each $k \in \{0, \ldots, n\}$, the symbol $(n)_k$ denotes the product $n(n-1)\cdots(n-k+1)$. (This is fairly standard notation.) By convention, $(n)_0 = 1$. Note that $(n)_k = n!/(n-k)!$. Because of the result in the next exercise, $(n)_k$ is commonly read *n permute k*.

Exercise 10. (*The number of permutations of n objects taken k at a time.*) Show that for each $n \in \boldsymbol{\omega}$, for each $k \in \{0, \ldots, n\}$, for each set A, for each set B, if A has k elements and B has n elements, then $\mathrm{inj}(A, B)$ has $(n)_k$ elements. (This can be proved by induction on n. The case where $k = 0$ requires a special argument but is easy. In the inductive step, if $k \neq 0$, use the multiplication rule. The argument is similar to the proof of the exponentiation rule. If you get stuck, work through Example 14.9 and then try again.)

In combinatorics, a bijection from a set to itself is called *a permutation of the elements of the set*.

Exercise 11. (*The number of permutations of k objects.*) Let $k \in \boldsymbol{\omega}$ and let A and B be sets with k elements. Use the result of Exercise 10 to show that the set of bijections from A to B has $k!$ elements. In particular, the set of bijections from A to A has $k!$ elements. (Hint: By Exercise 8 in Section 13, $\mathrm{bij}(A, B) = \mathrm{inj}(A, B)$ because A and B are finite sets with the same number of elements.)

14.10 Remark. If we wish to determine the number of elements in a given finite set S, then one strategy is to see S as the union of a some pairwise disjoint indexed family of sets $(C_\beta)_{\beta \in B}$ such that each of the sets C_β has the same number of elements, say γ elements. Then by the multiplication rule, S has $n\gamma$ elements, where $n = \overline{\overline{B}}$. This strategy was the one suggested for the exercises on the exponentiation rule, the generalized multiplication rule, and the number of permutations of n objects taken k at a time.

A common variation on this strategy, which may be used to determine the number of elements in a given finite set $\mathscr{B}$, is to see $\mathscr{B}$ as the index set of some pairwise disjoint family of sets $(C_\beta)_{\beta \in \mathscr{B}}$ where again each C_β has the same number of elements, say γ elements, but this time the number of elements in the union $\bigcup_{\beta \in \mathscr{B}} C_\beta$ is known. Say this union has σ elements. Then by the multiplication rule, $\sigma = n\gamma$ where $n = \overline{\overline{\mathscr{B}}}$. Hence $\overline{\overline{\mathscr{B}}} = \sigma/\gamma$. This variation is illustrated in the next example and exercise.

14.11 Example. Suppose $Y = \{4,5,6\}$ and $A = \{1,2\}$. Let $\mathscr{B} = \mathscr{P}_2(Y)$, the set of 2-element subsets of Y. Then

$$\mathscr{B} = \big\{ \{4,5\}, \{4,6\}, \{5,6\} \big\}.$$

Each injection f from A to Y is a bijection from A to the range of f. The range of such an injection from A to Y is a 2-element subset of Y, since A has two elements. The possible values for the range of such an injection are the three elements of $\mathscr{P}_2(Y)$, and these three possibilities are mutually exclusive. Thus the set of injections from A to Y is

$$\mathrm{inj}(A, Y) = C_{\{4,5\}} \cup C_{\{4,6\}} \cup C_{\{5,6\}}$$

where

$$\begin{aligned} C_{\{4,5\}} &= \mathrm{bij}(A, \{4,5\}) = \{ \langle 4,5 \rangle, \langle 5,4 \rangle \}, \\ C_{\{4,6\}} &= \mathrm{bij}(A, \{4,6\}) = \{ \langle 4,6 \rangle, \langle 6,4 \rangle \}, \\ C_{\{5,6\}} &= \mathrm{bij}(A, \{5,6\}) = \{ \langle 5,6 \rangle, \langle 6,5 \rangle \}, \end{aligned}$$

and the three sets $C_{\{4,5\}}$, $C_{\{4,6\}}$, and $C_{\{5,6\}}$ are pairwise disjoint. To put it succinctly, there are two elements of $\mathrm{inj}(A, Y)$ for each element of $\mathscr{P}_2(Y)$, because for each $X \in \mathscr{P}_2(Y)$, there are two bijections from the 2-element set A to the 2-element set X.

Exercise 12. (*More about the number of combinations of n objects taken k at a time.*) Let $n \in \boldsymbol{\omega}$ and let $k \in \{0, \ldots, n\}$. Let Y be a set with n elements. To save writing, let $\mathscr{B} = \mathscr{P}_k(Y)$, the set of k-element subsets of Y, and let $A = \{1, \ldots, k\}$. (If $k = 0$, let $A = \emptyset$.) By Exercise 11, for each $X \in \mathscr{B}$, $\operatorname{bij}(A, X)$ has $k!$ elements.

(a) Prove that

$$\operatorname{inj}(A, Y) = \bigcup_{X \in \mathscr{B}} \operatorname{bij}(A, X).$$

(b) Prove that for all $X_1, X_2 \in \mathscr{B}$, if $X_1 \neq X_2$, then $\operatorname{bij}(A, X_1) \cap \operatorname{bij}(A, X_2) = \emptyset$.

(c) By Exercise 3, $\mathscr{B}$ has $\binom{n}{k}$ elements. Use parts (a) and (b) and the multiplication rule to show that

$$(n)_k = \binom{n}{k} \cdot k!.$$

Deduce that

$$\binom{n}{k} = \frac{n!}{(n-k)!k!} \tag{1}$$

(If you get stuck, work through Example 14.11 and try again.)

14.12 Remark. Earlier, in the section on induction, you were asked to derive the formula (1) from the formula

$$\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}$$

and you were asked to prove the latter formula by induction. This is the way Pascal proved (1). In contrast, Exercise 12 gives a combinatorial explanation for (1). Surprisingly, Pascal seems not to have been aware of this way of understanding (1).

Exercise 13. (*The inclusion-exclusion formula.*) Let A and B be finite sets. Show that

$$\overline{\overline{A \cup B}} = \overline{\overline{A}} + \overline{\overline{B}} - \overline{\overline{A \cap B}}.$$

(Hint: Consider the three disjoint sets $A \setminus B$, $A \cap B$, and $B \setminus A$.)

Exercise 14. (*The generalized inclusion-exclusion formula.*) Prove by induction that for each $n \in \mathbf{N}$, for all finite sets $A_1, \ldots, A_n$, we have

$$\overline{\overline{\bigcup_{i=1}^n A_i}} = \sum_i \overline{\overline{A_i}} - \sum_{i<j} \overline{\overline{A_i A_j}} + \sum_{i<j<k} \overline{\overline{A_i A_j A_k}} - + \cdots + (-1)^{n+1} \overline{\overline{A_1 \cdots A_n}},$$

where to save space, we have written $A_i A_j$ for $A_i \cap A_j$ and so on.

14.13 Remark. The formula in Exercise 14 may be written more succinctly as

$$\overline{\overline{\bigcup_{i=1}^n A_i}} = \sum_{I \neq \emptyset} (-1)^{\overline{\overline{I}}+1} \overline{\overline{\bigcap_{i \in I} A_i}},$$

where the index I of summation ranges over all nonempty subsets of the set $\{1, \ldots, n\}$. To see this, write $\mathscr{J}_m$ for $\mathscr{P}_m(\{1, \ldots, n\})$, the set of m-element subsets of $\{1, \ldots, n\}$, and notice that the sum on the right in Exercise 14 is

$$\begin{aligned} \sum_{m=1}^n (-1)^{m+1} \sum_{I \in \mathscr{J}_m} \overline{\overline{\bigcap_{i \in I} A_i}} &= \sum_{m=1}^n \sum_{I \in \mathscr{J}_m} (-1)^{m+1} \overline{\overline{\bigcap_{i \in I} A_i}} \\ = \sum_{m=1}^n \sum_{I \in \mathscr{J}_m} (-1)^{\overline{\overline{I}}+1} \overline{\overline{\bigcap_{i \in I} A_i}} &= \sum_{I \neq \emptyset} (-1)^{\overline{\overline{I}}+1} \overline{\overline{\bigcap_{i \in I} A_i}}, \end{aligned}$$

where the last step follows from the fact that each nonempty subset $I \subseteq \{1, \ldots, n\}$ belongs to exactly one of the sets $\mathscr{J}_1, \ldots, \mathscr{J}_n$.

The next exercise is concerned with the way to expand a product of n binomials as a sum.

Exercise 15.

(a) Show that for each $n \in \mathbf{N}$, for all $b_1, \ldots, b_n \in \mathbf{R}$, we have

$$\prod_{i=1}^{n}(1 + b_i) = \sum_{I} \prod_{i \in I} b_i,$$

where the index I of summation ranges over all subsets of the set $\{\, 1, \ldots, n \,\}$. (Note: If $I = \emptyset$, then $\prod_{i \in I} b_i = 1$ by convention. This makes sense because for each real number c, the product of c and $\prod_{i \in \emptyset} b_i$) should be c.)

(b) (*The generalized binomial theorem.*) More generally, show that for each $n \in \mathbf{N}$, for all real numbers $a_1, b_1, \ldots, a_n, b_n$, we have

$$\prod_{i=1}^{n}(a_i + b_i) = \sum_{I} \left[\left(\prod_{i \notin I} a_i \right) \left(\prod_{i \in I} b_i \right) \right],$$

where again the index I of summation ranges over all subsets of the set $\{\, 1, \ldots, n \,\}$ and where for each such I, the i in $\prod_{i \notin I} a_i$ ranges over the set $\{\, 1, \ldots, n \,\} \setminus I$.

Exercise 16. Explain how the ordinary binomial theorem

$$(a + b)^n = \sum_{k=1}^{n} \binom{n}{k} a^{n-k} b^k$$

follows from the generalized binomial theorem, Exercise 15(b).

Exercise 17. Use the result of Exercise 15(a) to give an alternative proof of the generalized inclusion-exclusion formula. (Hint: Given $n \in \mathbf{N}$ and finite sets $A_1, \ldots, A_n$, let $B = \bigcup_{i=1}^{n} A_i$. Verify that for each $x \in B$,

$$\begin{aligned} 1_B(x) &= 1 - 1_{B \setminus \cup_{i=1}^{n} A_i}(x) = 1 - 1_{\cap_{i=1}^{n} (B \setminus A_i)}(x) \\ &= 1 - \prod_{i=1}^{n} 1_{B \setminus A_i}(x) = 1 - \prod_{i=1}^{n} \left[1 - 1_{A_i}(x) \right]. \end{aligned}$$

Use the result of Exercise 15(a) to expand the last product. In the expression that you thereby obtain for $1_B(x)$, sum over all $x \in B$. In the resulting double sum, interchange the order of summation and use the fact that for each subset $S \subseteq B$, the number of elements in S is given by

$$\overline{\overline{S}} = \sum_{x \in B} 1_S(x).$$

You should get the generalized inclusion-exclusion formula in the form pointed out in Remark 14.13.)

Exercise 18. Let $n \in \mathbf{N}$.

(a) Let $J = \{\, 1, \ldots, n \,\}$. Recall that a permutation of J is a bijection from J to J. Let Ω be the set of all permutations of J. Let B be the set of all permutations of J that leave at least one element of J fixed. In other words, let

$$B = \{\, f \in \Omega : f(i) = i \text{ for some } i \in J \,\}.$$

Find the number of elements in B. (Hint: Use the generalized inclusion-exclusion formula.)

(b) Suppose n men put their hats in a sack and then each man chooses a hat from the sack at random and keeps it. Find the probability that at least one man gets his own hat back.

(c) With the same setting as in part (b), show that as n tends to ∞, the probability that *no* man gets his own hat back approaches the limit e^{-1}. (Hint: See what you get when you substitute $x = -1$ in the power series for e^x. You should remember what this power series is. If you do not remember it, look it up in a calculus book.)

Exercise 19. (*More about the number of permutations of k objects.*) Use induction on k to give a proof of the result of Exercise 11 without using the result of Exercise 10 or the result of Exercise 8 in Section 13.

Exercise 20. (*More about the number of permutations of n objects taken k at a time.*) Use the result of Exercise 19 to give an alternative proof the result of Exercise 10, along the lines of the argument in Exercise 12. (Hint: How many different ways are there of extending a k-permutation of n objects to an n-permutation of these objects?)

Exercise 21. Let $m, n \in \mathbf{N}$.

(a) Show that the number of surjections from $\{1, \ldots, m\}$ to $\{1, \ldots, n\}$ is

$$\sum_{k=0}^{n-1} (-1)^k \binom{n}{k} (n-k)^m. \tag{2}$$

(Hint: The number of such surjections is the number of functions from $\{1, \ldots, m\}$ to $\{1, \ldots, n\}$ minus the number of these that are not surjections. You can calculate the latter number by applying the generalized inclusion-exclusion formula with A_i equal to the set of all functions from $\{1, \ldots, m\}$ to $\{1, \ldots, n\} \setminus \{i\}$.)

(b) Deduce from part (a) that if $m < n$, then the sum (2) has the value 0.

(c) Deduce from part (a) that

$$\sum_{k=0}^{n-1} (-1)^k \binom{n}{k} (n-k)^n = n!.$$

Let us close this section with a few words about the history of combinatorics. The combinatorial rules were discovered in India long before they became known in the west. Around 500 B.C., in the medical work of Susruta, the value 63 was given for the number of combinations of six tastes (bitter, sour, saltish, astringent, sweet, hot), since taking the tastes one at a time, two at a time, etc., we obtain thus 6, 15, 20, 15, 6, and 1 combinations, which add up to 63. (This does not include the empty combination.) The precursor of a general rule for the number of combinations of n objects appeared around 300 B.C. in the work of the Jains, as did the fact that the number of permutations of six objects is $6! = 720$. By the time of Bhaskara (1150), the fact that the number of permutations of k objects is $k!$ was already standard. Earlier, in his *Ganita Sara Sangraha*, written in 850, the Jain mathematician Mahavira gave $(n)_k/k!$ for the number of combinations of n objects taken k at a time.

Section 15. Infinite Sets

Hilbert's Hotel. To illustrate some of the peculiar properties of infinite sets, the mathematician David Hilbert liked to tell the story of a hotel with infinitely many rooms. The rooms were numbered 1, 2, 3, and so on, without end. One day when all the rooms in Hilbert's Hotel were full, a weary traveller approached the receptionist and asked for a room. The receptionist told the traveller that all the rooms were taken but that he would move the guests around to make room for him. Here is how the receptionist achieved this without requiring any of the guests who were already there to share a room. He had all the guests come out into the hallway. Then he had each guest move into the next room. In other words, the guest who had been in room 1 moved into room 2, the guest who had been in room 2 moved into room 3, the guest who had been in room 3 moved into room 4, and so on. After all this moving, rooms 2, 3, 4, and so on, were all full but room 1 was available for the new guest. (If you are wondering where the guest in the last room moved to, the answer is that in Hilbert's Hotel, there is no last room. The rooms go on forever and for each of them, there is a next one, just as for each natural number n, there is a next natural number $n + 1$.)

The hotel was still full a few days later when a busload of tourists arrived at the hotel. There were infinitely many passengers on the bus and all of them wanted rooms of their own. The resourceful receptionist once again was able to solve this problem by moving the guests who were already there. He had each guest

move into the room whose number was twice as big as the number of the room the guest had been in when the bus arrived. In other words, for each natural number n, the guest in room n moved into room $2n$. Thus the guest in room 1 moved into room 2, the guest in room 2 moved into room 4, the guest in room 3 moved into room 6, and so on. After this moving, rooms 2, 4, 6, 8, and so on, were all full but the infinitely many odd-numbered rooms 1, 3, 5, 7, and so on, were available for the new arrivals, who were infinitely grateful for the accomodation.

Some time after that, infinitely many buses arrived at the hotel, each carrying infinitely many conventioneers. Once again the hotel was already full but the receptionist was able to accomodate all of these new arrivals. Here is how he did it. For each natural number n, he had the guest in room n move into room $1+2+\cdots+n$. In other words, the guest in room 1 stayed in room 1, the guest in room 2 moved into room $1+2=3$, the guest in room 3 moved into room $1+2+3=6$, and so on. Then rooms 1, 3, 6, 10, 15, and so on, were full but rooms 2, 4, 5, 7, 8, 9, 11, 12, 13, 14, and so on, were available for the new arrivals. Notice that these available rooms come in blocks. The first block consists of the single room 2. The second block consists of the two rooms 4 and 5. The third block consists of the three rooms 7, 8, and 9. The fourth block consists of the four rooms 11, 12, 13, and 14. For each natural number n, the n-th block consists of the n rooms $(1+\cdots+n)+1$ through $(1+\cdots+n)+(n+1)$. The first passenger from the first bus moved into room 2, the single room making up the first block. The first passenger from the second bus and the second passenger from the first bus moved into the two rooms making up the second block. The first passenger from the third bus, the second passenger from the second bus, and the third passenger from the first bus moved into the three rooms making up the third block. For each natural number n, the n rooms making up the n-th block of available rooms were filled by the first passenger from the n-th bus, the second passenger from the $(n-1)$-th bus, and so on, down to the n-th passenger from the first bus.

After these amazing feats of accomodation, word of the remarkable capacity of Hilbert's Hotel got around and one day, when as usual the hotel was already full, another bus with infinitely many passengers arrived at the hotel. This bus carried one passenger for each real number, unlike the previous buses which had carried one passenger for each natural number. This time, however, it proved to be impossible to accomodate more than a tiny portion of the new arrivals even though the guests who were already there willingly moved to make infinitely rooms available. The reason it was impossible to accomodate all the new arrivals lies in the fact that even though the set of natural numbers and 'the set of real numbers are both infinite sets, they do not have the same number of elements. The set of real numbers is much more infinite than the set of natural numbers. For the explanation of what this means and why it is so, read on.

15.1 Remark. Recall that if A and B are sets, to say that A is equinumerous to B (sometimes abbreviated as $A \approx B$) means that there exists a bijection from A to B. When we say that A and B have the same number of elements, we mean that A is equinumerous to B. When we discussed equinumerousness earlier, we concentrated on the case where the sets in question were finite. However the concept of equinumerousness applies equally well to the case where the sets are infinite and gives us a way to compare the number of elements in two sets even if they are infinite.

15.2 Warning. You might think that if two sets are infinite, then they have the same number of elements, just because they are both infinite. Very surprisingly, this turns out to be false! This point was already mentioned at the end of the Hilbert's Hotel story above. Later in this section, we shall prove it rigorously.

15.3 Example. The set $\boldsymbol{\omega} = \{0, 1, 2, \dots\}$ of whole numbers has the set $\mathbf{N} = \{1, 2, 3, \dots\}$ of natural numbers as a proper subset. Nevertheless, $\boldsymbol{\omega}$ is equinumerous to $\mathbf{N}$. To see this, let $f(n) = n+1$ for all $n \in \boldsymbol{\omega}$. Then f is a bijection from $\boldsymbol{\omega}$ to $\mathbf{N}$. This illustrates the fact that an infinite set may be equinumerous to a proper subset of itself. In contrast, by the rigidity property of finite sets, a finite set cannot be equinumerous to a proper subset of itself. In fact, by showing that $\boldsymbol{\omega}$ is equinumerous to a proper subset of itself, we have shown that $\boldsymbol{\omega}$ is an infinite set.

15.4 Example. Of course the function f in Example 15.3 not the only bijection from $\boldsymbol{\omega}$ to $\mathbf{N}$. For instance, another bijection from $\boldsymbol{\omega}$ to $\mathbf{N}$ can be defined by

$$g(n) = \begin{cases} n+2 & \text{if } n \text{ is even,} \\ n & \text{if } n \text{ is odd,} \end{cases}$$

for all $n \in \boldsymbol{\omega}$.

Exercise 1. Show that the interval $A = [1, \infty)$ is equinumerous to the interval $B = (1, \infty)$ by giving an example of a bijection f from A to B. (Hint: Use one simple formula to define f on $\mathbf{N}$ and a different, even simpler formula to define f on $A \setminus \mathbf{N}$.)

15.5 Example. Let $A = \{ 2, 4, 6, \dots \}$ be the set of even natural numbers and let $B = \{ 1, 3, 5, \dots \}$ be the set of odd natural numbers. Intuitively, one feels that there are exactly as many even natural numbers as odd natural numbers. To verify this, let $f(n) = n - 1$ for all $n \in A$. Thus $f(2) = 1$, $f(4) = 3$, $f(6) = 5$, and so on. Then f is a bijection from A to B, so the set A of even natural numbers is equinumerous to the set B of odd natural numbers.

15.6 Remark. Example 15.3, Example 15.4, and Exercise 1 are related to the first part of the Hilbert's Hotel story. The next example and the exercise which follows it are related to the second part of the Hilbert's Hotel story.

15.7 Example. Once again, let A be the set of even natural numbers and let B be the set of odd natural numbers. While it is not surprising that A has the same number of elements as B, it may be surprising to observe that each of these sets has the same number of elements as the set $\mathbf{N}$ of all natural numbers. It is easy to verify that this is the case. Just let $g(n) = 2n$ and $h(n) = 2n-1$ for all $n \in \mathbf{N}$. Then g is a bijection from $\mathbf{N}$ to A and h is a bijection from $\mathbf{N}$ to B. Thus $\mathbf{N}$ is equinumerous to A and $\mathbf{N}$ is also equinumerous to B. This provides two more illustrations of the fact that an infinite set may be equinumerous to a proper subset of itself.

Exercise 2. Show that the set $\mathbf{Z}$ of integers is equinumerous to the set $\mathbf{N}$ of natural numbers.

15.8 Example. Recall that a *perfect square* is a number which is the square of a natural number. Let $S = \{ n^2 : n \in \mathbf{N} \} = \{ 1, 4, 9, 16, 25, \dots \}$ be the set of all perfect squares. Then S is equinumerous to $\mathbf{N}$. To see this, let $f(n) = n^2$ for all $n \in \mathbf{N}$. Then f is a bijection from $\mathbf{N}$ to S. This was one of the examples discussed by Galileo (1564–1642) in his book *Dialogues Concerning Two New Sciences*, published in 1638. Galileo pointed out that in one sense the set of perfect squares is the same size as the set of natural numbers since the perfect squares and the natural numbers can be put into one-to-one correspondence by means of the bijection f, but in another sense the set of perfect squares is much smaller than the set of natural numbers since the farther out one goes in the set of natural numbers, the rarer perfect squares become. Ten percent of the natural numbers from 1 to 100 are perfect squares (because $100 = 10^2$). One percent of the natural numbers from 1 to 10,000 are perfect squares. One tenth of one percent of the natural numbers from 1 to 1,000,000 are perfect squares.

15.9 Remark. The next example is similar to the third part of the Hilbert's Hotel story.

15.10 Example. The set $\mathbf{N} \times \mathbf{N}$ of all ordered pairs of natural numbers is equinumerous to the set $\mathbf{N}$ of natural numbers because we may define a bijection g from $\mathbf{N} \times \mathbf{N}$ to $\mathbf{N}$ as follows:

$$g(1,1) = 1,$$

$$g(1,2) = 2, \quad g(2,1) = 3,$$

$$g(1,3) = 4, \quad g(2,2) = 5, \quad g(3,1) = 6,$$

$$g(1,4) = 7, \quad g(2,3) = 8, \quad g(3,2) = 9, \quad g(4,1) = 10,$$

and so on.

(In line ℓ of this definition of g, we define $g(x, y)$ for all $(x, y) \in \mathbf{N} \times \mathbf{N}$ such that $x + y = \ell + 1$.)

Exercise 3. In the preceding example, we described a way to define a bijection g from $\mathbf{N} \times \mathbf{N}$ to $\mathbf{N}$. The definition of g is clear from this description so it does not really matter that we did not give an explicit general formula for $g(x, y)$. However it is interesting that there is a very simple explicit general formula for $g(x, y)$. Find such a formula and explain why it is valid for all $(x, y) \in \mathbf{N} \times \mathbf{N}$. (Hint: The formula

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

is relevant.)

15.11 Example. Let $A = \{\, x \in \mathbf{Q} : x > 0 \,\}$ be the set of strictly positive rational numbers. Then A is equinumerous to the set $\mathbf{N}$ of natural numbers. This can be seen as follows. Each strictly positive rational number x can be expressed uniquely in the form $x = a/b$, where a and b are natural numbers that have no common factors, so that the fraction a/b is in lowest terms. We can list all such fractions in lowest terms by listing first those where $a + b = 2$, then those where $a + b = 3$, then those where $a + b = 4$, and so on, as follows:

$$\frac{1}{1},$$

$$\frac{1}{2}, \quad \frac{2}{1},$$

$$\frac{1}{3}, \quad \frac{3}{1},$$

$$\frac{1}{4}, \quad \frac{2}{3}, \quad \frac{3}{2}, \quad \frac{4}{1},$$

$$\frac{1}{5}, \quad \frac{5}{1},$$

$$\frac{1}{6}, \quad \frac{2}{5}, \quad \frac{3}{4}, \quad \frac{4}{3}, \quad \frac{5}{2}, \quad \frac{6}{1},$$

and so on.

For each $n \in \mathbf{N}$, let $f(n)$ be the n-th term in this list. Thus $f(1) = 1/1$, $f(2) = 1/2$, $f(3) = 2/1$, $f(4) = 1/3$, and so on. Then f is a bijection from $\mathbf{N}$ to A.

Exercise 4. Show that the set $\mathbf{Q}$ of all rational numbers is equinumerous to the set $\mathbf{N}$ of natural numbers.

15.12 Example. Consider two circles with the same center p but with different radii. Let C_1 be the smaller circle and let C_2 be the larger one. Then C_1 is equinumerous to C_2. To see this, for each point x on on C_1, let $f(x)$ be the point where the half-line from p through x meets C_2. (I recommend that you draw a picture to make sure that you understand the definition of f.) Then f is a bijection from C_1 to C_2. This was another of the examples discussed by Galileo in his book *Dialogues Concerning Two New Sciences*, which we already mentioned in Example 15.8.

15.13 Example. Let A be the interval $[0, 12]$ and let B be the interval $[0, 5]$. Then A is equinumerous to B since if we let $f(x) = 5x/12$ for all $x \in A$, then f is a bijection from A to B. This gives another example in which an infinite set is equinumerous to a proper subset of itself. It also shows that two intervals of different lengths can be equinumerous to each other. This example was mentioned by Bernhard Bolzano in his book *Paradoxes of the Infinite*, published in 1851. Much earlier, Galileo considered a similar example, with a geometric construction of a bijection between two line segments of different lengths, his book *Dialogues Concerning Two New Sciences*, which we already mentioned in Example 15.8 and Example 15.12.

Exercise 5. Let $a, b, c, d \in \mathbf{R}$ with $a < b$ and $c < d$. Show that $[a, b] \approx [c, d]$ by giving an example of a bijection from $[a, b]$ to $[c, d]$. Similarly, show that $(a, b) \approx (c, d)$, $(a, b] \approx (c, d]$, and $[a, b) \approx [c, d)$. (Recall that in this section, when we write "$\approx$" we mean "is equinumerous to.")

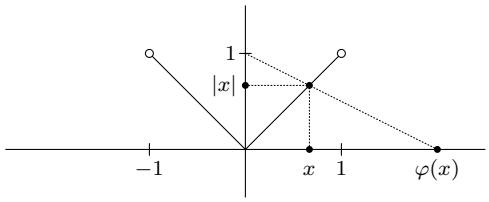
Exercise 6. Show that the interval $[0, 1)$ is equinumerous to the interval $(0, 1]$ by giving an example of a bijection from $[0, 1)$ to $(0, 1]$.

Exercise 7.

- **(a)** Show that the interval $(0, 1]$ is equinumerous to the interval $(0, 1)$ by giving an example of a bijection from $(0, 1]$ to $(0, 1)$. (Hint: This is similar to Exercise 1.)
- **(b)** Show similarly that $[0, 1]$ is equinumerous to $[0, 1)$.
- **(c)** Explain how it follows, from parts (a) and (b) and Exercise 6, that all four intervals $[0, 1]$, $[0, 1)$, $(0, 1]$, and $(0, 1)$ have the same number of elements.
- **(d)** For good measure, also show directly that the interval $[0, 1]$ is equinumerous to the interval $(0, 1)$, by giving an example of a bijection from $[0, 1]$ to $(0, 1)$.

15.14 Example. The unbounded interval $[1, \infty)$ is equinumerous to the bounded interval $(0, 1]$, because if we let $f(x) = 1/x$ for all $x \in [1, \infty)$, then f is a bijection from $[1, \infty)$ to $(0, 1]$. Similarly, the unbounded interval $(1, \infty)$ is equinumerous to the bounded interval $(0, 1)$.

15.15 Example. The bounded interval $(-1, 1)$ is equinumerous to the whole real line $\mathbf{R}$. To show this, we shall give an example of a bijection from $(-1, 1)$ to $\mathbf{R}$. For each value of x in the interval $(-1, 1)$, let $\varphi(x)$ be the x-coordinate of the point where the line through the points $(0, 1)$ and $(x, |x|)$ meets the x-axis, as shown in the following figure.[20]



It is geometrically clear that as x varies over the interval $(-1, 1)$, $\varphi(x)$ varies over the interval $(-\infty, \infty)$. Thus φ is a bijection from the interval $(-1, 1)$ to $\mathbf{R}$.

By the way, it is easy to work out a formula for φ. By similar triangles, for each value of x in the interval $(-1, 1)$, we have

$$\frac{\varphi(x) - 0}{1 - 0} = \frac{x - 0}{1 - |x|}.$$

Hence $\varphi(x) = x/(1 - |x|)$ for all $x \in (-1, 1)$. Thus we see that φ is the same bijection from $(-1, 1)$ to $\mathbf{R}$ that we already considered in Exercise 23 in Section 11.

Exercise 8. Show that the interval $(0, 1)$ is equinumerous to $\mathbf{R}$. (Hint: Use Exercise 5 and Example 15.15.)

Exercise 9. Let $a, b \in \mathbf{R}$ with $a < b$. By combining the results of the last few exercises and examples, show that each of the following intervals is equinumerous to the set $\mathbf{R}$ of all real numbers:

$$(a, b), \quad (a, b], \quad [a, b), \quad [a, b], \quad (a, \infty), \quad [a, \infty), \quad (-\infty, b), \quad (-\infty, b].$$

Thus any nondegenerate interval is equinumerous to $\mathbf{R}$.

The German mathematician Georg Cantor (1845–1918), who is considered to be the founder of modern set theory, seems to have been the first person to have considered the possibility that two infinite sets could have different numbers of elements. On November 29, 1873, Cantor wrote to Richard Dedekind (1831–1916), another German mathematician, to ask whether it was possible to define a one-to-one correspondence between the set $\mathbf{R}$ of all real numbers and the set $\mathbf{N}$ of all natural numbers. He remarked that one might think this to be impossible on the grounds that the set of natural numbers is discrete whereas the set of real numbers is not discrete. However he pointed that this was not sufficient reason to reject the possibility of a one-to-one correspondence between $\mathbf{R}$ and $\mathbf{N}$, because the set $\mathbf{Q}$ of rational numbers is not discrete and yet there is a one-to-one correspondence between $\mathbf{Q}$ and $\mathbf{N}$. (We saw this above. Cantor seems to have been the first person to notice that $\mathbf{Q}$ is equinumerous to $\mathbf{N}$.) Dedekind replied that he did not know the answer to Cantor's question. On December 2, 1873, Cantor wrote again to Dedekind to say that he had found the answer: There is no one-to-one correspondence between $\mathbf{R}$ and $\mathbf{N}$. We now turn to the explanation of this.

15.16 Cantor's Diagonal Lemma. *Let f be any function from $\mathbf{N}$ to the interval $(0, 1)$. Then there exists a number $y \in (0, 1)$ such that y does not belong to the range of f.*

Proof. We are given a function $f\colon \mathbf{N} \to (0, 1)$. We wish to find a number $y \in (0, 1)$ such that

$$y \notin \{\, f(1),\, f(2),\, f(3),\, f(4), \ldots \}.$$

[20] Note that this figure is not the graph of φ.

For each $n \in \mathbf{N}$ and each $k \in \mathbf{N}$, let x_{nk} be the k-th digit in the standard[21] decimal expansion of $f(n)$. Then

$$\begin{aligned} f(1) &= 0.x_{11}x_{12}x_{13}x_{14}\ldots, \\ f(2) &= 0.x_{21}x_{22}x_{23}x_{24}\ldots, \\ f(3) &= 0.x_{31}x_{32}x_{33}x_{34}\ldots, \\ f(4) &= 0.x_{41}x_{42}x_{43}x_{44}\ldots, \end{aligned}$$

and so on.

We shall define the number y by defining the digits in its decimal expansion so that they are different from the "diagonal" entries $x_{11}, x_{22}, x_{33}, x_{44}, \ldots$ that are highlighted in the display above. For each $n \in \mathbf{N}$, let

$$y_n = \begin{cases} 5 & \text{if } x_{nn} \neq 5, \\ 4 & \text{if } x_{nn} = 5. \end{cases}$$

Then for each $n \in \mathbf{N}$, $y_n \neq x_{nn}$. Now let y be the number whose standard decimal expansion is

$$y = 0.y_1y_2y_3y_4\ldots.$$

Then $y \in (0,1)$. In fact, $0.444\ldots \leq y \leq 0.555\ldots$. To see that y is not in the range of f, note that for each $n \in \mathbf{N}$, $y \neq f(n)$ (because the numbers y and $f(n)$ differ in their n-th decimal place; in other words, $y_n \neq x_{nn}$). ■

15.17 Remark. Obviously, Cantor's diagonal lemma gets its name from the important role that the "diagonal" entries $x_{11}, x_{22}, x_{33}, x_{44}, \ldots$ play in its proof. By the way, in the proof of Cantor's diagonal lemma, there are many other ways that we could have defined the digits $y_1, y_2, y_3, y_4, \ldots$. The main thing is that they should be defined so that $y_1 \neq x_{11}$, $y_2 \neq x_{22}$, $y_3 \neq x_{33}$, $y_4 \neq x_{44}$, and so on. Also, we should be careful to define them so that the decimal expansion $0.y_1y_2y_3y_4\ldots$ is a standard decimal expansion. In other words, this decimal expansion should not end in an infinite string of 9's. This is the case for the way that we defined the y_n's, because we chose none of them to be 9. This matters so that we can deduce $y \neq f(n)$ from $y_n \neq x_{nn}$.

Incidentally, Cantor's original proof of his diagonal lemma in 1873 was more complicated. The proof that we have presented, which gave the lemma its name, is the one that Cantor published in 1891 in the same paper where he proved his "generalized diagonal lemma," which we shall discuss later.

15.18 Theorem. (Cantor, 1873.) *The set* $\mathbf{R}$ *of real numbers is not equinumerous to the set* $\mathbf{N}$ *of natural numbers.*

Proof. Suppose $\mathbf{R}$ is equinumerous to $\mathbf{N}$. We shall show that this assumption leads to a contradiction. We know that the interval $(0,1)$ is equinumerous to $\mathbf{R}$. Hence $(0,1)$ is equinumerous to $\mathbf{N}$, by transitivity of equinumerousness. Thus $\mathbf{N}$ is equinumerous to $(0,1)$, by symmetry of equinumerousness. Hence there is a bijection f from $\mathbf{N}$ to $(0,1)$. But then in particular f is a surjection from $\mathbf{N}$ to $(0,1)$. Even more particularly, f is a function from $\mathbf{N}$ to $(0,1)$. Then by Cantor's diagonal lemma, there exists a number $y \in (0,1)$ such that y is not in the range of f. Hence f is not a surjection from $\mathbf{N}$ to $(0,1)$. Thus we have reached a contradiction. Therefore $\mathbf{R}$ must not be equinumerous to $\mathbf{N}$. ■

15.19 Definitions. Let A be a set.

- **(a)** To say that A *is denumerable* means that A is equinumerous to $\mathbf{N}$.
- **(b)** To say that A *is countable* means that A is finite or denumerable.
- **(c)** To say that A *is uncountable* means that A is not countable.

15.20 Example. Each of the sets $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{N} \times \mathbf{N}$, and $\mathbf{Q}$ is denumerable. The set $\mathbf{R}$ is uncountable.

[21] Some real numbers have two decimal expansions. For instance $1/2 = 0.5$ and $1/2 = 0.499999\cdots$. The standard decimal expansion of a real number is the one that does not end with an infinite string of 9's.

Denumerable sets are also called *countably infinite*. Any uncountable set is infinite, so uncountable sets are also called *uncountably infinite*. Note that a countable set need not be finite, contrary to what might be suggested by the everyday language usage of the word.[22]

As we shall see, denumerable sets are the smallest infinite sets, in the sense that any infinite subset of a denumerable set is denumerable and any infinite set has a denumerable subset. The proof that any infinite set has a denumerable subset uses the axiom of choice.

Higher Orders of Infinity. As we have seen, the set of real numbers is a more infinite set than the set of natural numbers, in the sense that while both are infinite and the set of natural numbers is (equinumerous to) a subset of the set of real numbers, the set of natural numbers is not equinumerous to the whole set of real numbers. Cantor discovered that the possible orders of infinity of infinite sets go on forever, in the sense that for each infinite set, there is another infinite set such that the former is equinumerous to a subset of the latter but not equinumerous to the whole latter set. We shall now discuss this discovery of Cantor's.

15.21 Definitions. Let A and B be sets.

(a) To say that *the cardinality of A is less than or equal to the cardinality of B* (denoted $\overline{\overline{A}} \leq \overline{\overline{B}}$) means that A is equinumerous to a subset of B.

(b) To say that *the cardinality of A is strictly less than the cardinality of B* (denoted $\overline{\overline{A}} < \overline{\overline{B}}$) means that A is equinumerous to a subset of B but A is not equinumerous to B.

15.22 Example. The cardinality of $\mathbf{N}$ is strictly less than the cardinality of $\mathbf{R}$.

15.23 Remark. In Definition 15.21, the notation $\overline{\overline{A}}$ may be read "the cardinality of A." When A is finite, we have already defined the cardinality of A to be the number of elements in A. However notice that we have not yet defined what is meant by the cardinality of an infinite set. We have only defined how to compare the cardinalities of two sets. In this spirit, we shall also say *the cardinality of A is equal to the cardinality of B* (denoted $\overline{\overline{A}} = \overline{\overline{B}}$) to mean A is equinumerous to B (denoted $A \approx B$).

15.24 Remark. Let A and B be sets. Then $\overline{\overline{A}} \leq \overline{\overline{B}}$ iff there exists an injection from A to B.

Proof. ($\Rightarrow$). Suppose $\overline{\overline{A}} \leq \overline{\overline{B}}$. Then there is a subset $C \subseteq B$ such A is equinumerous to C. Since A is equinumerous to C, there is a bijection f from A to C. Then in particular, f is function from A to C and f is an injection. Since f is a function from A to C and since $C \subseteq B$, f is a function from A to B. Thus f is an injection from A to B.

($\Leftarrow$). Conversely, suppose there is an injection f from A to B. Let $C = \mathrm{Rng}(f)$. Then $C \subseteq B$, because f is a function from A to B. Now any function is a surjection from its domain to its range. Hence any injection is a bijection from its domain to its range. In particular, f is a bijection from A to C. Thus A is equinumerous to the subset $C \subseteq B$. ■

15.25 Example. Let A be any set. Then $\overline{\overline{A}} \leq \overline{\overline{\mathscr{P}(A)}}$.

Proof. For each $x \in A$, let $h(x) = \{ x \}$. Then $h \colon A \to \mathscr{P}(A)$. Note that for all $x_1, x_2 \in A$, if $h(x_1) = h(x_2)$, then $\{ x_1 \} = \{ x_2 \}$, so $x_1 \in \{ x_2 \}$, so $x_1 = x_2$. Thus h is an injection from A to $\mathscr{P}(A)$. Hence $\overline{\overline{A}} \leq \overline{\overline{\mathscr{P}(A)}}$, by Remark 15.24. ■

15.26 Cantor's Generalized Diagonal Lemma. *Let A be a set and let f be a function on A such that for each $x \in A$, $f(x)$ is a set. Then there exists a subset $C \subseteq A$ such that C does not belong to the range of f.*

Proof. Let $C = \{ x \in A : x \notin f(x) \}$. Obviously $C \subseteq A$. It remains to show that $C \notin \mathrm{Rng}(f)$. Suppose $C \in \mathrm{Rng}(f)$. Then $C = f(x_0)$ for some $x_0 \in A$. Now either $x_0 \in C$ or $x_0 \notin C$.

Case 1. Suppose $x_0 \in C$. Then by the definition of C, $x_0 \notin f(x_0)$. But $f(x_0) = C$. Hence $x_0 \notin C$. Thus $x_0 \in C$ and $x_0 \notin C$, which is a contradiction.

[22] A word of caution: some books define *denumerable* and/or *countable* in slightly different ways. If in doubt, check the definitions in whatever book you are reading.

Case 2. Suppose $x_0 \notin C$. Recall that $C = f(x_0)$. Hence $x_0 \notin f(x_0)$. Thus $x_0 \in A$ and $x_0 \notin f(x_0)$, so by the definition of C, $x_0 \in C$. Hence $x_0 \notin C$ and $x_0 \in C$, which is a contradiction.

Thus in either case we get a contradiction. Therefore $C \notin \mathrm{Rng}(f)$. ■

15.27 Example. To help us understand the proof Cantor's generalized diagonal lemma, let us see what C would be in a simple particular case. Let $A = \{\,1, 2, 3\,\}$ and let f be the function on A defined by

$$\begin{aligned} f(1) &= \{\,2, 3\,\} \\ f(2) &= \{\,1, 2, 7, 9\,\} \\ f(3) &= \{\,1, 2\,\} \end{aligned}$$

Then for each $x \in A$, $f(x)$ is a set. As in the proof of Cantor's generalized diagonal lemma, let

$$C = \{\, x \in A : x \notin f(x)\,\}.$$

Then $1 \in C$, because $1 \notin f(1) = \{\,2, 3\,\}$. Also, $2 \notin C$, because $2 \in f(2) = \{\,1, 2, 7, 9\,\}$. And $3 \in C$, because $3 \notin f(3) = \{\,1, 2\,\}$. Thus $C = \{\,1, 3\,\}$. Now

$$\{\,1, 3\,\} \notin \big\{\,\{\,2, 3\,\}, \{\,1, 2, 7, 9\,\}, \{\,1, 2\,\}\,\big\}.$$

In other words, $C \notin \{\, f(1), f(2), f(3)\,\}$. But this is not an accident. It is an inevitable consequence of the way C was defined. We have $C \neq f(1)$ because $1 \in C$ and $1 \notin f(1)$. We have $C \neq f(2)$ because $2 \notin C$ and $2 \in f(2)$. And we have $C \neq f(3)$ because $3 \in C$ and $3 \notin f(3)$.

15.28 Theorem. (Cantor, 1891.) *Any set has strictly smaller cardinality than its power set.*

Proof. Consider any set A. We wish to show that $\overline{\overline{A}} < \overline{\overline{\mathscr{P}(A)}}$. We saw in Example 15.25 that $\overline{\overline{A}} \leq \overline{\overline{\mathscr{P}(A)}}$. It remains to show that $\overline{\overline{A}} \neq \overline{\overline{\mathscr{P}(A)}}$. Suppose $\overline{\overline{A}} = \overline{\overline{\mathscr{P}(A)}}$. We shall derive a contradiction from this assumption. Since we are assuming that $\overline{\overline{A}} = \overline{\overline{\mathscr{P}(A)}}$, there is a bijection f from A to $\mathscr{P}(A)$. Then in particular, f is a surjection from A to $\mathscr{P}(A)$, so the range of f is $\mathscr{P}(A)$. Now f is a function on A and for each $x \in A$, we have $f(x) \in \mathscr{P}(A)$, so $f(x) \subseteq A$, so $f(x)$ is a set. Hence by Cantor's generalized diagonal lemma, there is a subset $C \subseteq A$ such that C does not belong to the range of f. But $C \in \mathscr{P}(A)$ because $C \subseteq A$. Hence C does belong to the range of f, because the range of f is $\mathscr{P}(A)$. Thus $C \in \mathrm{Rng}(f)$ and $C \notin \mathrm{Rng}(f)$. This is a contradiction. Hence it must be that $\overline{\overline{A}} \neq \overline{\overline{\mathscr{P}(A)}}$. ■

15.29 Remark. From the proof of Theorem 15.28, we see that for each set A, there is no surjection from A to $\mathscr{P}(A)$.

15.30 Remark. By Theorem 15.28, we see that $\overline{\overline{\mathbf{N}}} < \overline{\overline{\mathscr{P}(\mathbf{N})}}$. As we shall see later, $\overline{\overline{\mathscr{P}(\mathbf{N})}} = \overline{\overline{\mathbf{R}}}$. Hence Theorem 15.28, which Cantor published in 1891, may be regarded as a generalization of his earlier 1873 result that $\overline{\overline{\mathbf{N}}} < \overline{\overline{\mathbf{R}}}$.

15.31 Remark. If A is a finite set, then we can see without Theorem 15.28 that $\overline{\overline{A}} < \overline{\overline{\mathscr{P}(A)}}$. Indeed, if $\overline{\overline{A}} = n$, where $n \in \boldsymbol{\omega}$, then $\overline{\overline{\mathscr{P}(A)}} = 2^n$ and it is easy to prove by induction that for each $n \in \boldsymbol{\omega}$, $n < 2^n$. It is when A is an infinite set that Theorem 15.28 tells us something that was not obvious before. In particular, it tells us that

$$\overline{\overline{\mathbf{N}}} < \overline{\overline{\mathscr{P}(\mathbf{N})}} < \overline{\overline{\mathscr{P}(\mathscr{P}(\mathbf{N}))}} < \overline{\overline{\mathscr{P}(\mathscr{P}(\mathscr{P}(\mathbf{N})))}} < \cdots . \tag{1}$$

Thus we see that there is an unending series of infinite sets of greater and greater orders of infinity.

15.32 Remark. Perhaps I should warn you that the inequalities (1) suggest more than we have proved yet. If A, B, and C are sets such that

$$\overline{\overline{A}} < \overline{\overline{B}} \qquad \text{and} \qquad \overline{\overline{B}} < \overline{\overline{C}},$$

then you would naturally expect that $\overline{\overline{A}} < \overline{\overline{C}}$. This is correct, but we need the Schroeder-Bernstein Theorem (**forward reference** below) to prove it.[23] inf.schrbern

Russell's Paradox. In May of 1901, it occurred to the English philosopher Bertrand Russell (1872–1970) to apply Cantor's argument that $\overline{\overline{A}} < \overline{\overline{\mathscr{P}(A)}}$ in the case where A is the "set of all sets." By thinking about the proof of Cantor's generalized diagonal lemma and reducing it to its essentials, Russell was led to consider the "set"

$$C = \{\, x : x \text{ is a set and } x \notin x \,\}$$

of all sets that are not members of themselves.[24] He then argued that either $C \in C$ or $C \notin C$. If $C \in C$, then $C \notin C$ by the definition of C. If $C \notin C$, then $C \in C$ by the definition of C. Thus in either case, we reach a contradiction. This was baffling to Russell, because he could find nothing wrong with the assumptions that he had made.

Resolution of Russell's Paradox. The resolution of the Russell's paradox that has come to be accepted is to say that the so-called set C is not a set at all. As we said at the beginning of Section 10, a set is a collection of objects considered as an object in its own right. More precisely, a set is a collection of elements of the universe of discourse of set theory, that is itself an element the universe of discourse of set theory. The collection C is a subcollection of the universe of discourse of set theory but not an element of this universe of discourse. Notice that this does resolve Russell's paradox, since in the second case in the argument of Russell's paradox, where $C \notin C$, in order to reach the contradictory conclusion that $C \in C$, we made (implicit) use of the assumption that C was a set.

The Barber Paradox. A paradox which is analogous to Russell's paradox is the so-called *Barber Paradox*. Russell stated the following version of the barber paradox:

> A man of Seville is shaved by the barber of Seville if and only if he does not shave himself. Who shaves the barber of Seville?

Either the barber shaves himself or he does not. If the barber does shave himself, then the barber does not shave him, so he does not shave himself, since he is the barber. If the barber does not shave himself, then the barber shaves him, so he does shave himself. Thus in either case, we reach a contradiction. But this argument assumed implicitly that the barber of Seville is a man of Seville. If the barber is a woman, for instance, then there is no contradiction. Likewise, the argument of Russell's paradox assumed implicitly that the collection C is a set. If C is not a set, then there is no contradiction and Russell's paradox evaporates.

The Halting Problem. The sort of reasoning used in Russell's paradox and the barber paradox can be used to answer other interesting questions. Here is one:

> Is there a computer program which can examine any other computer program and determine whether it will terminate?

The answer is "no." For suppose A is such a computer program. Consider the following (informally written) computer program, which we shall call B:

> If A says B will terminate, then go into an infinite loop. If A says B will not terminate, then stop.

---

[23] I am indebted to my colleague Andrzej Derdzinksi for this remark, as well as for the following observation. In the special case that is relevant to (1), it is possible to avoid use of the Schroeder-Bernstein theorem as follows. Given sets A and B with $\overline{\overline{A}} \le \overline{\overline{B}}$, we would like to know that $\overline{\overline{A}} < \overline{\overline{\mathscr{P}}}(B)$. Clearly $\overline{\overline{A}} \le \overline{\overline{\mathscr{P}}}(B)$. Suppose $\overline{\overline{A}} = \overline{\overline{\mathscr{P}}}(B)$. Then there is a bijection h from A to $\mathscr{P}(B)$. Since $\overline{\overline{A}} \le \overline{\overline{B}}$, there is a injection f from A to B. Let E be the range of f. Then f^{-1} is a bijection from E to A. Since $\overline{\overline{A}} = \overline{\overline{\mathscr{P}}}(B)$, A cannot be empty. ($\mathscr{P}(B)$ is not empty, because B belongs to it.) Let $p \in A$. Define $g\colon B \to A$ by letting $g(y) = f^{-1}(y)$ if $y \in E$ and $g(y) = p$ if $y \in B \setminus E$. Then g is a surjection from B to A, so $h \circ g$ is a surjection from B to $\mathscr{P}(B)$. But as we saw in the proof of Theorem 15.28, for any set B, there does not exist a surjection from B to $\mathscr{P}(B)$.

[24] As Russell put it later, some sets are members of themselves and some are not. It may seem hard to think of a set that is a member of itself, but as examples of such sets, Russell said that the set of all sets is a set, and so is a member of itself, and the set of all not-teapots is a not-teapot, and so is a member of itself. However, in modern set theory, these would not be regarded as valid examples of sets. Furthermore, it is more to the point to emphasize that whether sets that are members of themselves exist or not is entirely irrelevant to the argument of Russell's paradox.

Evidently, A fails to correctly determine whether B terminates. Hence A does not have the property it was assumed to have. Therefore no such program A can exist. This result was observed by the British mathematician Alan Turing in 1936. Turing is considered by many to have been the father of theoretical computer science. During World War II (1939–1945), Turing was one of the leaders of the remarkably successful British efforts to break German codes. His contributions were decisive in some of the key battles of the war and it has been said that he contributed as much as any man to the allied victory.

Axioms for Set Theory.

As Russell's paradox shows, it is important to specify the basic assumptions, or axioms, for set theory. While it would not be appropriate to attempt too formal a treatment of axiomatic set theory in this book, we shall now informally describe and discuss the axioms for set theory.

The universe of discourse of set theory is a collection $\mathbf{V}$ that is considered to consist of all of the objects that are needed in mathematics. Some subcollections of $\mathbf{V}$ are themselves elements of $\mathbf{V}$ and some are not. A set is a subcollection of $\mathbf{V}$ that is itself an element of $\mathbf{V}$. It is possible but not essential to work with the assumption that every object belonging to $\mathbf{V}$ is a set.

- *The Axiom of Extensionality.* Sets that have the same elements are equal. In other words, for all sets A and B, if for each x, we have $x \in A$ iff $x \in B$, then we have $A = B$.

It is also axiomatic that equal sets have the same elements and that equal objects are elements of the same sets, but these are considered to be axioms of logic rather than axioms of set theory itself, since they are special cases of the general principle that equal objects have the same properties. (To say that $x = y$ means that the letters "x" and "y" stand for the same object, so if $x = y$ then certainly x and y should have the same properties.)

- *The Axiom of Separation.* Given any property and any set, there is a set (unique by the axiom of extensionality) consisting of all the elements of the given set having the given property. In other words, given any property $P(x)$, we have that for each set A, the collection $\{\, x \in A : P(x) \,\}$ is a set. The property $P(x)$ may involve other free variables besides x. If it does, then the set $\{\, x \in A : P(x) \,\}$ depends on the values of these variables.

Note that the axiom of separation does not say that given any property $P(x)$, the collection $\{\, x : P(x) \,\}$ is a set. Indeed, as Russell's paradox shows, if $P(x)$ is the property "x is a set and $x \notin x$", then the collection $\{\, x : P(x) \,\}$ is not a set.

The axiom of separation was introduced in 1908 by the German mathematician Ernst Zermelo (1871–1953), as a substitute for the naive idea that for any property $P(x)$, one can form that the set of all objects x which have the property $P(x)$. As we have seen, this naive idea had to be rejected because it leads to contradictions such as Russell's paradox.

Exercise 10.

(a) Let A be a set. Use the axiom of separation to show that there is a subset $C \subseteq A$ such that $C \notin A$. (Hint: Let $C = \{\, x \in A : x \text{ is a set and } x \notin x \,\}$. Obviously $C \subseteq A$. Adapt the argument of Russell's paradox to show that $C \notin A$.)

(b) Show that the universe of discourse $\mathbf{V}$ of set theory is not a set. (Earlier we mentioned that the notion of a set to which every object belongs leads to difficulties. What you are asked to show here makes precise what we meant by this.)

The axiom of separation also shows that for all sets A and B, the collections $A \cap B = \{\, x \in A : x \in B \,\}$ and $A \setminus B = \{\, x \in A : x \notin B \,\}$ are sets. Similarly, for each nonempty set $\mathscr{M}$ all of whose elements are themselves sets, the collection

$$\bigcap \mathscr{M} = \{\, x : x \in A \text{ for all } A \in \mathscr{M} \,\}$$

is a set, because

$$\bigcap \mathscr{M} = \{\, x \in A_0 : x \in A \text{ for all } A \in \mathscr{M} \,\}$$

where A_0 is any fixed element of the nonempty set $\mathscr{M}$.

- *The Axiom of Replacement.* Given any property $P(x, y)$, if for each x, there exists a unique y such that $P(x, y)$, then for each set A, the collection

$$\{\, y : \text{there exists } x \in A \text{ such that } P(x, y) \,\},$$

  obtained by replacing each $x \in A$ by the unique y such that $P(x, y)$, is a set. The property $P(x, y)$ may involve other free variables besides x and y. If it does, then the resulting set depends on the values of these variables.

It is not difficult to show that the axiom of replacement implies the axiom of separation. This is why some advanced books do not bother to include the axiom of separation among the axioms of set theory.

- *The Axiom of Unordered Pairs.* For each object x and each object y, the collection $\{\, x, y \,\}$ is a set. In particular, for each object x, the collection $\{\, x \,\} = \{\, x, x \,\}$ is a set.

The existence of the empty set follows from the axiom of unordered pairs and the axiom of separation. Here is how to see this. It is enough to show that there exists at least one set A, for then the collection $A \setminus A$ is empty. By the axiom of separation, this collection is a set. To show that there exists at least one set A, we first note that it is implicit in the axioms and rules of inference of logic that the universe of discourse is nonempty (because for any property $P(x)$, $(\forall x)P(x)$ implies $(\exists x)P(x)$.) Hence we can let x be an object belonging to the universe of discourse. Then we can let A be the collection $\{\, x \,\}$. By the axiom of unordered pairs, A is a set.

- *The Axiom of Unions.* For each set $\mathscr{M}$ all of whose elements are themselves sets, the collection

$$\bigcup \mathscr{M} = \{\, x : x \in A \text{ for some } A \in \mathscr{M} \,\}$$

  is a set. In particular, for each set A and each set B, the collection $A \cup B = \bigcup \{\, A, B \,\}$ is a set.
- *The Power Set Axiom.* For each set A, the collection $\mathscr{P}(A) = \{\, B : B \subseteq A \,\}$ is a set.
- *The Axiom of Infinity.* There exists at least one set A such that $\emptyset \in A$ and for each $x \in A$, x is a set and $x \cup \{\, x \,\} \in A$.

We recall that one way to define the whole numbers is to define 0 to be the empty set, 1 to be $\{\, 0 \,\} = 0 \cup \{\, 0 \,\}$, 2 to be $\{\, 0, 1 \,\} = 1 \cup \{\, 1 \,\}$, 3 to be $\{\, 0, 1, 2 \,\} = 2 \cup \{\, 2 \,\}$, and so on. The axiom of infinity is exactly what is needed to show that the collection of whole numbers, defined in this way, is a set.

- *The Axiom of Regularity.* This axiom serves to guarantee that all sets are built up from the empty set and from the basic objects that are not sets (if we allow such objects). The precise statement of the axiom of regularity need not concern us, since it is almost never needed in the applications of set theory in mathematics. Let us just mention that one consequence of the axiom of regularity is that no set can be an element of itself.

The version of set theory with the axioms we have now listed is called *Zermelo-Fraenkel set theory*, or *ZF* for short, after Ernst Zermelo and the German (later Israeli) logician Abraham Fraenkel (1891–1965), who were the main contributors to this axiomatization of set theory. Note that *ZF* does not include the axiom of choice. Zermelo-Fraenkel set theory together with the axiom of choice is called *ZFC* for short. Experience has shown that *ZFC* is a suitable axiomatic basis for practically all of modern mathematics. When we speak of the usual assumptions of set theory, we shall mean either *ZF*, if we exclude the axiom of choice, or *ZFC*, if we include the axiom of choice.

When we introduced the concept of a set, at the beginning of Section 10, we said that a *set* is a collection of objects, considered as an object in its own right. This statement may help us to understand what we mean by the word *set*, but it is not a definition of this word in the mathematical sense, because it does not define this word in terms of more basic concepts. In fact, there have to be some *primitive* concepts that cannot be defined in terms of more basic ones. In the set-theoretic approach to mathematics, the primitive concepts are the notion of *equality*, the notion of *set*, and the notion of *membership*, $\in$. In principle, all other mathematical concepts can be defined in terms of these three primitive concepts, but these primitive concepts cannot be explicitly defined. Instead of defining them, we must be content with listing the basic assumptions that we believe to be true about them. These basic assumptions are the axioms of set theory that we have outlined above, together with the axioms of logic.

Exercise 11. Let A and B be sets.

(a) Let $b \in B$. Show that the collection $A \times \{ b \} = \{ (x, b) : x \in A \}$ is a set. (Hint: Apply the axiom of replacement, taking $P(x, y)$ to be the property "$y = (x, b)$.")

(b) Show that the collection $\mathscr{M} = \{ A \times \{ b \} : b \in B \}$ is a set. (Hint: Apply the axiom of replacement again, but in a different way.)

(c) Show that the Cartesian product $A \times B = \{ (x, y) : x \in A \text{ and } y \in B \}$ is a set. (Hint: Apply the axiom of unions.)

Section 16. More About Infinite Sets

16.1 Proposition. *Let D be a set. Then D is denumerable iff D can be written as $D = \{ d_1, d_2, d_3, \dots \}$ where $d_1, d_2, d_3, \dots$ are distinct.*

Proof. Suppose D is denumerable. Then D is equinumerous to $\mathbf{N}$ so there exists a bijection from $\mathbf{N}$ to D. Let f be such a bijection and let $d_1 = f(1)$, $d_2 = f(2)$, $d_3 = f(3)$, and so on. Then $d_1, d_2, d_3, \dots$ are distinct because f is one-to-one, and $D = \{ d_1, d_2, d_3, \dots \}$ because f is onto D.

Conversely, suppose D can be written as $D = \{ d_1, d_2, d_3, \dots \}$ where $d_1, d_2, d_3, \dots$ are distinct. Let $f(n) = d_n$ for all $n \in \mathbf{N}$. Then f is one-to-one because $d_1, d_2, d_3, \dots$ are distinct, and the range of f is D because $D = \{ d_1, d_2, d_3, \dots \}$. Thus f is a bijection from $\mathbf{N}$ to D, so D is equinumerous to $\mathbf{N}$. ■

16.2 Reminder. As we saw in Exercise 4(b) in Section 7, each nonempty subset of $\mathbf{N}$ has a least element.

16.3 Theorem. *Any infinite subset of $\mathbf{N}$ is denumerable.*

Proof. Let C be an infinite subset of $\mathbf{N}$. We wish to show that C is denumerable. Now any nonempty subset of $\mathbf{N}$ has a least element. Since C is infinite, C is not empty, so C has a least element. Let c_1 be the least element of C. Now since C is infinite, C is not a subset of a finite set, so for each finite set F, $C \setminus F$ is not empty. Thus $C \setminus \{ c_1 \}$ is not empty, so it has a least element. Let c_2 be the least element of $C \setminus \{ c_1 \}$. If $n \in \mathbf{N}$ and if $c_1, \dots, c_n$ have already been defined in this way, then $C \setminus \{ c_1, \dots, c_n \}$ is not empty, so we can let c_{n+1} be the least element of $C \setminus \{ c_1, \dots, c_n \}$. Continuing this way, we define a sequence $\langle c_1, c_2, c_3, \dots \rangle$ of distinct elements of C such that c_1 is the least element of C and for each $n \in \mathbf{N}$, c_{n+1} is the least element of $C \setminus \{ c_1, \dots, c_n \}$.

Now c_1 is the least element of C, so certainly each element of $\{ c_1 \}$ is strictly less than each element of $C \setminus \{ c_1 \}$. Next, c_2 is the least element of $C \setminus \{ c_1 \}$, so each element of $\{ c_1, c_2 \}$ is strictly less than each element of $C \setminus \{ c_1, c_2 \}$. Continuing in this way, we see that for each $n \in \mathbf{N}$, each element of $c_1, \dots, c_n$ is strictly less than each element of $C \setminus \{ c_1, \dots, c_n \}$. (We could easily give a formal proof of this by induction but I think that in this case, the informal argument we just gave is more enlightening.)

Note that for each $n \in \mathbf{N}$, $c_n < c_{n+1}$, because $c_n \in \{ c_1, \dots, c_n \}$ and $c_{n+1} \in C \setminus \{ c_1, \dots, c_n \}$. By induction, it follows that for each $n \in \mathbf{N}$, we have $c_n \geq n$. To see this, observe that $c_1 \geq 1$ and for each $n \in \mathbf{N}$, if $c_n \geq n$, then $c_{n+1} \geq c_n + 1 \geq n + 1$.

Let $D = \{ c_1, c_2, c_3, \dots \}$. Then D is a denumerable subset of C. We claim that $C = D$. Suppose not. Then $C \setminus D$ is a nonempty subset of $\mathbf{N}$, so it has a least element, say m. Now $c_m \geq m$. Hence the set of all $n \in \mathbf{N}$ such that $c_n \geq m$ is not empty, so this set has a least element, say n_0. By the definition of n_0, each element of $\{ c_1, \dots, c_{n_0 - 1} \}$ is strictly less than m, so $m \in C \setminus \{ c_1, \dots, c_{n_0 - 1} \}$. But $m \notin D$. Hence $m < c_{n_0}$. But since $m \in C$, this contradicts the fact that c_{n_0} is the least element of $C \setminus \{ c_1, \dots, c_{n_0 - 1} \}$. ■

16.4 Corollary. *A subset of a countable set is countable.*

Proof. Consider any countable set A and any subset $B \subseteq A$. We wish to show that B is countable. Either B is finite or B is infinite. If B is finite, then B is countable. Consider the case where B is infinite. Then A is infinite too, since $B \subseteq A$. Hence A is denumerable, since A is infinite and countable. Since A is denumerable, there is a bijection f from A to $\mathbf{N}$. Let $C = f[B]$. Then C is equinumerous to B, since $f \restriction B$ is a bijection from B to C. Hence C is an infinite subset of $\mathbf{N}$, so by Theorem 16.3, C is denumerable. Hence B is denumerable too, since B is equinumerous to A. ■

16.5 Lemma. *Let B be a nonempty countable set. Then there is a surjection from $\mathbf{N}$ to B.*

Proof. Either B is denumerable or B is nonempty and finite. In the case where B is denumberable, there is actually a bijection from $\mathbf{N}$ to B. Consider the case where B is nonempty and finite. Let n be the number of elements in B. Then $n \in \mathbf{N}$ and there is a bijection f from $\{\,1, \ldots, n\,\}$ to B. Define $g\colon \mathbf{N} \to B$ by $g(k) = f(k)$ if $k \leq n$ and $g(k) = f(n)$ if $k > n$. Then g is a surjection from $\mathbf{N}$ to B. ■

16.6 Proposition. *Let A and B be sets. Suppose B is countable and there is a surjection from B to A. Then A is countable and $\overline{\overline{A}} \leq \overline{\overline{B}}$.*

Proof. Let g be a surjection from B to A. If B is empty, then A is empty, so A is countable and $\overline{\overline{A}} \leq \overline{\overline{B}}$. Consider the case where B is not empty. Then since B is countable and nonempty, there exists a surjection f from $\mathbf{N}$ to B, by Lemma 16.5. Let $h = g \circ f$. Then h is a surjection from $\mathbf{N}$ to A. For each $x \in A$, we have $x \in \mathrm{Rng}(h)$, so there exists $n \in \mathbf{N}$ such that $h(n) = x$, so $h^{-1}[\{\,x\,\}]$ is a nonempty subset of $\mathbf{N}$, so it has a least element. Define $\gamma : A \to \mathbf{N}$ by letting $\gamma(x)$ be the least element of $h^{-1}[\{\,x\,\}]$, for each $x \in A$. Then $h(\gamma(x)) = x$ for each $x \in A$. Let $\beta = f \circ \gamma$. Then $\beta\colon A \to B$ and for each $x \in A$, we have $g(\beta(x)) = g(f(\gamma(x)) = (g \circ f)(\gamma(x)) = h(\gamma(x)) = x$. Thus β is a right inverse for g. In particular, β is an injection from A to B, by Theorem 13.40. Hence $\overline{\overline{A}} \leq \overline{\overline{B}}$. ■

16.7 Remark. Proposition 16.6 generalizes Exercise 11 in Section 13.

16.8 Proposition. *Let C be a set. Then the following are equivalent:*

(a) *C is countable and nonempty.*

(b) *C can be written as $C = \{\,c_1, c_2, c_3, \ldots\,\}$ where $c_1, c_2, c_3, \ldots$ are not necessarily distinct.*

(c) *There exists a surjection from $\mathbf{N}$ to C.*

Proof. (a)⇒(b). Suppose C is countable. Then either C is denumerable or C is finite. If C is denumerable, then as we saw above, C can be written as $C = \{\,c_1, c_2, c_3, \ldots\,\}$ where $c_1, c_2, c_3, \ldots$ are distinct. If C is finite, then since C is not empty, C can be written as $C = \{\,c_1, \ldots, c_n\,\}$ where n is the number of elements in C and where $c_1, \ldots, c_n$ are distinct, so $C = \{\,c_1, c_2, c_3, \ldots\,\}$ where $c_k = c_n$ for all $k \in \mathbf{N}$ with $k > n$ (so $c_1, c_2, c_3, \ldots$ are not distinct).

(b)⇒(c). Suppose C can be written as $C = \{\,c_1, c_2, c_3, \ldots\,\}$ where $c_1, c_2, c_3, \ldots$ are not necessarily distinct. Let $f(n) = c_n$ for all $n \in \mathbf{N}$. Then f is a surjection from $\mathbf{N}$ to C. (But f is not necessarily an injection because $c_1, c_2, c_3, \ldots$ are not necessarily distinct.)

(c)⇒(a). Suppose there exists a surjection from $\mathbf{N}$ to C. Then C is countable, by Proposition 16.6. ■

Exercise 1. Let A and B be countable sets.

(a) Show that $A \cup B$ is countable.

(b) Show that $A \times B$ is countable.

16.9 Theorem. *Let A be a set. Then the following are equivalent.*

(a) *A has a denumerable subset.*

(b) *A is equinumerous to a proper subset of itself.*

Proof. (a)⇒(b). Suppose A has a denumerable subset, say D. Since D is denumerable, D can be written as $D = \{\,d_1, d_2, d_3, \ldots\,\}$ where $d_1, d_2, d_3, \ldots$ are distinct. Let $B = A \setminus \{\,d_1\,\}$. Then B is a proper subset of A. Let

$$f(x) = \begin{cases} x & \text{if } x \notin D, \\ d_{n+1} & \text{if } x = d_n \text{ where } n \in \mathbf{N}, \end{cases}$$

for all $x \in A$. Then f is a bijection from A to B. Hence A is equinumerous to the proper subset B.

(b)⇒(a). Suppose A is equinumerous to a proper subset of itself. Let B be a proper subset of A such that A is equinumerous to B. Let f be a bijection from A to B. Since B is a proper subset of A, $A \setminus B$ is not empty. Let $d_1 \in A \setminus B$. Let $d_2 = f(b_1)$, $d_3 = f(b_2)$, $d_4 = f(b_3)$, and so on. We claim that $d_1, d_2, d_3, d_4, \ldots$ are distinct. To see this, first note that $d_2 \neq d_1$ because $d_1 \notin B$ and $d_2 \in B$ (because B is the range of f and d_2 is in the range of f, since $d_2 = f(d_1)$). Next, $d_3 \neq d_1$ for a similar reason and $d_3 \neq d_2$ because $d_3 = f(d_2)$, $d_2 = f(d_1)$, $d_2 \neq d_1$, and f is one-to-one. Continuing in this way, we can prove by induction that for each $n \in \mathbf{N}$, $d_{n+1} \notin \{\,d_1, \ldots, d_n\,\}$. This proves the claim. Let $D = \{\,d_1, d_2, d_3, \ldots\,\}$. Then D is a denumerable subset of A. ■

Exercise 2. Write out in detail the proof by induction that is sketched in the proof of (b)⇒(a) of Theorem 16.9.

The proof of Theorem 16.9 used some of the same ideas as the Hilbert's Hotel story. The same is true of the proof of the next result.

16.10 Theorem. *Let A be a set and let C be a nonempty countable set disjoint from A. If A has a denumerable subset, then $A \cup C$ is equinumerous to A, and conversely.*

Proof. Suppose A has a denumerable subset, say D. Since D is denumerable, D may be written as $D = \{ d_1, d_2, d_3, \dots \}$ where $d_1, d_2, d_3, \dots$ are distinct. Since C is nonempty and countable, either C is nonempty and finite or C is denumerable.

Case 1. Suppose C is nonempty and finite. Then for some $n \in \mathbf{N}$, we have $C = \{ c_1, \dots, c_n \}$ where $c_1, \dots, c_n$ are distinct. For all $x \in A \cup C$, let

$$f(x) = \begin{cases} d_k & \text{if } x = c_k \text{ where } k \in \{ 1, \dots, n \}, \\ d_{n+k} & \text{if } x = d_k \text{ where } k \in \mathbf{N}, \\ x & \text{if } x \in A \setminus D. \end{cases}$$

Thus $f(c_1) = d_1, \dots, f(c_n) = d_n$, $f(d_1) = d_{n+1}$, $f(d_2) = d_{n+2}$, and so on. Then f is a bijection from $A \cup C$ to A.

Case 2. Suppose C is denumerable. Then we may write C as $C = \{ c_1, c_2, c_3, \dots \}$ where $c_1, c_2, c_3, \dots$ are distinct. For all $x \in A \cup C$, let

$$f(x) = \begin{cases} d_{2k-1} & \text{if } x = c_k \text{ where } k \in \mathbf{N}, \\ d_{2k} & \text{if } x = d_k \text{ where } k \in \mathbf{N}, \\ x & \text{if } x \in A \setminus D. \end{cases}$$

Thus $f(c_1) = d_1$, $f(c_2) = d_3$, $f(c_3) = d_5$, and so on, and $f(d_1) = d_2$, $f(d_2) = d_4$, $f(d_3) = d_6$, and so on. Then f is a bijection from $A \cup C$ to A.

Thus in either case, $A \cup C$ is equinumerous to A.

Conversely, suppose $A \cup C$ is equinumerous to A. Then there exists a bijection f from $A \cup C$ to A. Let $B = f[A]$, the image of A under f, and let $g = f \restriction A$, the restriction of f to A. Then B is a subset of A and since g is a bijection from A to B, A is equinumerous to B. Now $f[A]$ and $f[C]$ are disjoint because f is one-to-one and A and C are disjoint. Furthermore, $f[C]$ is a subset of A. Hence $f[A] \neq A$. Thus $B = f[A]$ is a proper subset of A. Since A is equinumerous to the proper subset B, it follows that A has a denumerable subset, by Theorem 16.9. ■

Exercise 3. Use Theorem 16.10 to show that the set of irrational numbers is equinumerous to the set of real numbers.

16.11 Remark. Let $\mathbf{P}$ denote the set of irrational numbers. (This is just temporary notation.) By Exercise 3, $\mathbf{P}$ is equinumerous to $\mathbf{R}$. Hence $\mathbf{P}$ is uncountable. But as we know, the set $\mathbf{Q}$ of rational numbers is countable. Thus there is no one-to-one correspondence between $\mathbf{P}$ and $\mathbf{Q}$. This might appear to be in conflict with the fact that between any two distinct rational numbers, there is an irrational number, and vice versa. In reality, though, there is no conflict. Rational numbers and irrational numbers do not alternate like even numbers and odd numbers, and there is no such thing as two successive rational numbers or two successive irrational numbers. Indeed, between any two distinct real numbers, there is a countable infinity of rational numbers and an uncountable infinity of irrational numbers.

16.12 Proposition. *Let A be an infinite set. Then for each $n \in \boldsymbol{\omega}$, A has a subset with n elements.*

Proof. Let $P(n)$ be the sentence

there exists a subset $B \subseteq A$ such that B has n elements.

Then what we want to prove is that for each $n \in \boldsymbol{\omega}$, $P(n)$ is true. We shall do this by induction.

BASE CASE: First note that $P(0)$ is true, because $\emptyset \subseteq A$ and $\emptyset$ has 0 elements.

INDUCTIVE STEP: Now let $n \in \boldsymbol{\omega}$ such that $P(n)$ is true. Then we may pick a subset $B \subseteq A$ such that B has n elements. Since A is not finite, $A \neq B$, so we can pick $t \in A$ such that $t \notin B$. Then $B \cup \{\, t \,\}$ is a subset of A with $n+1$ elements. Thus $P(n+1)$ is true.

CONCLUSION: Therefore, by induction, for each $n \in \boldsymbol{\omega}$, $P(n)$ is true. ■

Exercise 4. Let A be a finite set and let B be an infinite set. Show that A is equinumerous to a subset of B.

Exercise 5. Prove the converse of Proposition 16.12. In other words, let A be a set such that for each $n \in \boldsymbol{\omega}$, A has a subset with n elements. Show that A is infinite.

16.13 Theorem. (Dedekind, 1887.) *Each infinite set has a denumerable subset.*

Proof. Consider any infinite set S. For each $n \in \mathbf{N}$, let B_n be the set of injections from $\{\, 1, \ldots, n \,\}$ to S. By Proposition 16.12, for each $n \in \mathbf{N}$, there exists a subset of S with n elements. It follows that for each $n \in \mathbf{N}$, there exists a bijection from $\{\, 1, \ldots, n \,\}$ to a subset of S. Hence for each $n \in \mathbf{N}$, there exists an injection from $\{\, 1, \ldots, n \,\}$ to S. In other words, for each $n \in \mathbf{N}$, we have $B_n \neq \emptyset$. Hence by the axiom of choice, there exists a choice function Φ for the family $\langle\, B_n \,\rangle_{n \in \mathbf{N}}$. In other words, there exists a function Φ, whose domain is $\mathbf{N}$, such that for each $n \in \mathbf{N}$, $\Phi(n) \in B_n$. Let $f_n = \Phi(n)$ for all $n \in \mathbf{N}$. Then for each $n \in \mathbf{N}$, f_n is an injection from $\{\, 1, \ldots, n \,\}$ to S. Let $y_1 = f_1(1)$ and for each $n \in \mathbf{N}$, if $y_1, \ldots, y_n$ have already been defined, let $y_{n+1} = f_{n+1}(k)$ where k is the least element of $\{\, 1, \ldots, n, n+1 \,\}$ such that $f_{n+1}(k) \notin \{\, y_1, \ldots, y_n \,\}$. (Such a k must exist: The set $\{\, f_{n+1}(1), \ldots, f_{n+1}(n), f_{n+1}(n+1) \,\}$ has $n+1$ elements because f_{n+1} is an injection from $\{\, 1, \ldots, n, n+1 \,\}$ to S.) Then $y_1, y_2, y_3, \ldots$ are distinct elements of S (because for each $n \in \mathbf{N}$, $y_{n+1} \notin \{\, y_1, \ldots, y_n \,\}$). Hence if we let $D = \{\, y_1, y_2, y_3, \ldots \,\}$, then D is a denumerable subset of S. ■

16.14 Remark. To prove things about infinite sets, it often happens that one must use the axiom of choice. Theorem 16.13 is one of the earliest examples of this. In fact, when Dedekind proved this result, the axiom of choice had not yet been explicitly formulated and it did not occur to anyone that a new principle was being used. However, the use of the axiom of choice is not avoidable here. It can be shown that if one uses only the usual assumptions of set theory without the axiom of choice, then it is impossible to prove that every infinite set has a denumerable subset.

16.15 Remark. It follows from Theorem 16.9 and Theorem 16.13 that each infinite set is equinumerous to a proper subset of itself. However this result depends on the axiom of choice since Theorem 16.13 does. In contrast, Theorem 16.9 does not depend on the axiom of choice. Similarly, it follows from Theorem 16.10 and Theorem 16.13 that if A is an infinite set and C is a countable set, then $A \cup C$ is equinumerous to A, but this depends on the axiom of choice whereas Theorem 16.10 does not.

16.16 Remark. The proof of Theorem 16.13 used only the so-called *countable axiom of choice*, which asserts that each sequence $\langle\, B_n \,\rangle_{n \in \mathbf{N}}$ of nonempty sets has a choice function. We recall that the full axiom of choice asserts that each family $\langle\, B_\alpha \,\rangle_{\alpha \in A}$ of nonempty sets has a choice function, even if the index set A of the family is uncountable.

16.17 Remark (*Optional*). The proof of Theorem 16.13 that we have presented is essentially the one that was presented by Dedekind. In many books one finds the following alternative proof:

> Consider any infinite set S. Since S is infinite, S is not empty, so we may choose $y_1 \in S$. For each $n \in \mathbf{N}$, if $y_1, \ldots, y_n$ are distinct elements of S that have already been chosen, then $S \setminus \{\, y_1, \ldots, y_n \,\}$ is not empty (because S is infinite), so we may choose $y_{n+1} \in S \setminus \{\, y_1, \ldots, y_n \,\}$. Continuing in this way, we construct an infinite sequence $\langle\, y_1, y_2, y_3, \ldots \,\rangle$ of distinct elements of S. Let $D = \{\, y_1, y_2, y_3, \ldots \,\}$. Then D is a denumerable subset of S.

This alternative proof is simpler than Dedekind's, but this greater simplicity is achieved through the use of a stronger choice principle. Dedekind's proof depends on the countable axiom of choice to justify the making of denumerably many simultaneous independent choices (to produce the f_n's), whereas the alternative proof

depends on the so-called *principle of dependent choice* to justify the making of denumerably many successive choices where at stage n, we choose y_{n+1} in a way that depends on how $y_1, \dots, y_n$ have already been chosen, without having any rule at our disposal for choosing a specific y_{n+1}.

The principle of dependent choice may be formulated in general as follows: For each set S and each set Σ of finite sequences of elements of S, if Σ contains at least one sequence of length 1 and Σ is such that for each sequence $\langle y_1, \dots, y_n \rangle$ of length n which belongs to Σ, there exists $y \in S$ such that the sequence $\langle y_1, \dots, y_n, y \rangle$ belongs to Σ, then there exists an infinite sequence $\langle y_1, y_2, y_3, \dots \rangle$ such that for each $n \in \mathbf{N}$, the finite sequence $\langle y_1, \dots, y_n \rangle$ belongs to Σ.

In the context of the usual assumptions of set theory, the principle of dependent choice is strictly intermediate in strength between the axiom of choice and the countable axiom of choice. The axiom of choice implies the principle of dependent choice, but not conversely. The principle of dependent choice implies the countable axiom of choice, but not conversely. The first part of each of these assertions is easy to prove, but the proofs of the "not conversely" parts are very difficult and beyond the scope of this book. It is probably fair to say that in most applications of the axiom of choice in reasonably "concrete" situations, either the countable axiom of choice or the principle of dependent choice is sufficient. It is mainly in very abstract situations that the full axiom of choice is needed.

Here is a proof that the axiom of choice implies the principle of dependent choice. Consider any set S and any set Σ of finite sequences of elements of S, such that Σ contains at least one sequence of length 1 and such that for each sequence $\langle y_1, \dots, y_n \rangle$ of length n which belongs to Σ, there exists $y \in S$ such that the sequence $\langle y_1, \dots, y_n, y \rangle$ belongs to Σ. For each finite sequence $\langle y_1, \dots, y_n \rangle$ belonging to Σ, let $S_{\langle y_1, \dots, y_n \rangle}$ be the set of all $y \in S$ such that $\langle y_1, \dots, y_n, y \rangle$ belongs to Σ. Then

$$\left\langle S_{\langle y_1, \dots, y_n \rangle} \right\rangle_{\langle y_1, \dots, y_n \rangle \in \Sigma}$$

is a family of nonempty sets. Let Ψ be a choice function for this family. Then let $y_1 \in S$ such that the sequence $\langle y_1 \rangle$ of length 1 belongs to Σ and for each $n \in \mathbf{N}$, if $y_1, \dots, y_n$ have already been defined, let $y_{n+1} = \Psi(\langle y_1, \dots, y_n \rangle)$. Continuing in this way, we construct an infinite sequence $\langle y_1, y_2, y_3, \dots \rangle$ such that for each $n \in \mathbf{N}$, the finite sequence $\langle y_1, \dots, y_n \rangle$ belongs to Σ.

Finally, here is a proof that the principle of dependent choice implies the countable axiom of choice. Let $\langle B_n \rangle_{n \in \mathbf{N}}$ be any sequence of nonempty sets. Let $S = \bigcup_{n \in \mathbf{N}} B_n$ and let Σ be the set of all finite sequences $\langle y_1, \dots, y_n \rangle$ of elements of S such that $y_1 \in B_1, \dots, y_n \in B_n$. Since $B_1 \neq \emptyset$, there exists $y_1 \in B_1 \subseteq S$ such that $\langle y_1 \rangle \in \Sigma$. If $\langle y_1, \dots, y_n \rangle \in \Sigma$, then since $B_{n+1} \neq \emptyset$, there exists $y \in B_{n+1} \subseteq S$ such that $\langle y_1, \dots, y_n, y \rangle \in \Sigma$. Hence by the principle of dependent choice, there exists an infinite sequence $\langle y_1, y_2, y_3, \dots \rangle$ of elements of S such that for each $n \in \mathbf{N}$, $\langle y_1, \dots, y_n \rangle \in \Sigma$. Let $f(n) = y_n$ for all $n \in \mathbf{N}$. Then f is a choice function for $\langle B_n \rangle_{n \in \mathbf{N}}$.

16.18 Proposition. *The union of a countable collection of countable sets is countable.*

Proof. Let $\mathscr{C}$ be a countable collection of countable sets and let $B = \bigcup \mathscr{C}$. We wish to show that B is countable. Without loss of generality, we may suppose that $\emptyset \notin \mathscr{C}$, because if $\mathscr{C}_1 = \mathscr{C} \setminus \{\emptyset\}$, then $\mathscr{C}_1$ is countable too and $B = \bigcup \mathscr{C}_1$. Also, we may as well assume that $\mathscr{C} \neq \emptyset$, because if $\mathscr{C} = \emptyset$, then $B = \bigcup \mathscr{C} = \emptyset$, so B is trivially countable. Thus we need only consider the case where $\mathscr{C}$ is a nonempty countable collection of nonempty countable sets. Then $\mathscr{C}$ can be written as

$$\mathscr{C} = \{ C_1, C_2, C_3, \dots \}$$

where $C_1, C_2, C_3, \dots$ are not necessarily distinct. Then $B = \bigcup_{n \in \mathbf{N}} C_n$. For each $n \in \mathbf{N}$, C_n is a nonempty countable set, so we can choose a surjection φ_n from $\mathbf{N}$ to C_n. (We can do this by the following argument which uses the countable axiom of choice: For each $n \in \mathbf{N}$, let S_n be the set of surjections from $\mathbf{N}$ to C_n. Then each S_n is nonempty. Let Φ be a choice function for $\langle S_n \rangle_{n \in \mathbf{N}}$ and for each $n \in \mathbf{N}$, let $\varphi_n = \Phi(n)$.) Let $f(n, m) = \varphi_n(m)$ for all $n, m \in \mathbf{N}$. Then f is a surjection from $\mathbf{N} \times \mathbf{N}$ to B. Now we know that $\mathbf{N} \times \mathbf{N}$ is denumerable. Hence B is countable, by Proposition 16.6. ■

16.19 Remark. The preceding proof used the axiom of choice. It can be shown that under the usual assumptions of set theory without the axiom of choice, it is impossible to prove in general that the union of a countable collection of countable sets is countable. In fact, under the usual assumptions of set theory without the axiom of choice, it is impossible to prove that the real line $\mathbf{R}$, which we know is uncountable, is not the union of a countable collection of countable sets.

16.20 Remark. In Remark 16.19, when we said that in set theory without the axiom of choice, it is impossible to prove that the union of a countable collection of countable sets is countable, we should really have said that it is impossible to prove this provided set theory is consistent. Since a false statement implies anything, if set theory is inconsistent, then any statement that can be formulated in set theory can be proved in set theory. This caveat also applies to other statements we make below about the impossibility of proving various things in set theory.

It is fair to say that most mathematicians hope that set theory is consistent and believe that it is. However, this belief has to be taken on faith. If set theory were inconsistent, then as just mentioned, in set theory, one could prove any statement expressible in set theory, including the consistency of set theory. In 1931, the Austrian mathematician Kurt Gödel (1906–1978) showed that this is the only way the consistency of set theory could be provable in set theory. In fact, he showed that in any reasonable sufficiently rich formal system, such as set theory, one cannot prove the consistency of that system within the system itself, unless the system is actually inconsistent. This result is known as *Gödel's second incompleteness theorem*.

Exercise 6. Let A be a countable set. To avoid trivialities, assume that A is not empty.

(a) Show that for each $n \in \mathbf{N}$, A^n is countable.

(b) Show that $\bigcup_{n\in\mathbf{N}} A^n$ is countable.

16.21 Remark. If you did part (b) of Exercise 6 by appealing to Proposition 16.18, then your solution used the axiom of choice. However, by a refinement of the natural solution to part (a), it is not difficult to show without using the axiom of choice that there is a sequence of functions $\langle\, \varphi_n \,\rangle_{n\in\mathbf{N}}$ such that for each $n \in \mathbf{N}$, φ_n is a surjection from $\mathbf{N}$ to A^n. Using this, one can prove part (b) without using the axiom of choice, by imitating the proof of Proposition 16.18. Thus one does not always need to use the axiom of choice to show that the union of a countable collection of countable sets is countable.

16.22 Definition. To say that a real number is *algebraic* means that it is a root of a nonconstant polynomial with rational coefficients.

16.23 Remark. Every rational number is algebraic, since if r is rational, then r is a root of the polynomial $x - r$ which has rational coefficients 1 and $-r$. But there are also irrational numbers that are algebraic. For instance, $\sqrt{2}$ is algebraic, since it is a root of the polynomial $x^2 - 2$.

Exercise 7. Show that the set of algebraic numbers is countably infinite. (Hint: Show that the set of nonconstant polynomials with rational coefficients is countable. Then recall that such each polynomial has only finitely many roots, since a polynomial of degree $n \geq 1$ has at most n roots.)

16.24 Definition. To say that a real number is *transcendental* means that it is not algebraic.

Exercise 8. Show that the set of transcendental numbers is uncountable.

16.25 Remark. The result in the preceding exercise was Cantor's first application of his discovery that $\mathbf{R}$ is uncountable. Earlier Liouville (1844) had shown that transcendental numbers exist, by giving specific but artificial examples of such numbers. Hermite (1873) had shown that e is transcendental and later Lindemann (1882) showed that π is transcendental. Cantor (1874) proved the remarkable result that *most* real numbers are transcendental, since the set of transcendental numbers is uncountably infinite whereas the set of algebraic numbers is just countably infinite.

Exercise 9. Show that the set of transcendental numbers is equinumerous to the set of real numbers. (Hint: By Exercise 8, there exist transcendental numbers. Let x be a transcendental number. Show that for each $n \in \mathbf{N}$, nx is a transcendental number. Hence the set of transcendental numbers has a denumerable subset. Now apply the appropriate theorem.)

Binary Expansions. We have already discussed decimal expansions in Example 12.19. Binary expansions are like these, except that they are in base 2 rather than base 10. Here we shall summarize without proof the basic facts about binary expansions. (We shall review the reasons for them later.) If $b_1, b_2 \ldots, b_n \in \{\, 0, 1 \,\}$, then in base 2,

$$(0.b_1b_2\ldots b_n)_2 = \frac{b_1}{2^1} + \frac{b_2}{2^2} + \cdots + \frac{b_n}{2^n}.$$

The subscript 2 at the end of the notation $(0.b_1b_2\dots b_n)_2$ is to indicate that base 2 is intended. If $b_1, b_2, b_3, \dots \in \{0,1\}$, then to say that a number $x \in [0,1)$ has the binary expansion $(0.b_1b_2b_3\dots)_2$ means that for each $n \in \mathbf{N}$,

$$(0.b_1b_2\dots b_n)_2 \le x \le (0.b_1b_2\dots b_n)_2 + \frac{1}{2^n}.$$

Each number $x \in [0,1)$ has a unique binary expansion not ending in repeating 1's. This is called the standard binary expansion of x.[25]

16.26 Theorem. $\mathbf{R} \approx \{0,1\}^{\mathbf{N}} \approx \mathscr{P}(\mathbf{N})$

Proof. By Proposition 14.6, we know that for each set A, the set $\mathscr{P}(A)$ of all subsets of A is equinumerous to the set $\{0,1\}^A$ of functions from A to $\{0,1\}$, because each subset $S \subseteq A$ corresponds to its indicator function 1_S, which is a function from A to $\{0,1\}$. In particular, the set $\mathscr{P}(\mathbf{N})$ of all subsets of $\mathbf{N}$ is equinumerous to the set $\{0,1\}^{\mathbf{N}}$ of all infinite sequences of 0's and 1's.

It remains to show that $\mathbf{R} \approx \{0,1\}^{\mathbf{N}}$. Since $\mathbf{R} \approx [0,1)$, it is equivalent to show that $[0,1) \approx \{0,1\}^{\mathbf{N}}$. To show this, we shall use binary expansions. For each $x \in [0,1)$, let

$$f(x) = \langle\, b_1, b_2, b_3, \dots \rangle$$

where $(0.b_1b_2b_3\dots)_2$ is the standard binary expansion of x. Then f is an injection from $[0,1)$ to $\{0,1\}^{\mathbf{N}}$, because different numbers have different binary expansions. However, f is not onto $\{0,1\}^{\mathbf{N}}$. The range of f is the set B of all infinite sequences of 0's and 1's that do not end in repeating 1's. Since f is a bijection from $[0,1)$ to B, we have $[0,1) \approx B$. Let $C = \{0,1\}^{\mathbf{N}} \setminus B$. Then C is the set of all infinite sequences of 0's and 1's that do end in repeating 1's. Now B has a denumerable subset and C is denumerable. Hence $B \approx B \cup C$, by Theorem 16.10. But $B \cup C = \{0,1\}^{\mathbf{N}}$, so $B \approx \{0,1\}^{\mathbf{N}}$. Since $[0,1) \approx B$ and $B \approx \{0,1\}^{\mathbf{N}}$, we have $[0,1) \approx \{0,1\}^{\mathbf{N}}$. ■

Exercise 10. Let B and C be as in the preceding proof.

(a) Justify the assertion that B has a denumerable subset by exhibiting such a subset.

(b) Justify the assertion that C is denumerable. (Hint: Use the result of Exercise 6(b).)

Exercise 11. Let A_1, A_2, B_1, B_2 be sets such that $A_1 \approx B_1$ and $A_2 \approx B_2$. Show that $A_1 \times A_2 \approx B_1 \times B_2$.

After Cantor had discovered that the infinite sets $\mathbf{R}$ and $\mathbf{N}$ have different numbers of elements, it naturally occurred to him to wonder how many different possibilities there were for the number of elements in an infinite set. (This was many years before his discovery that the sets $\mathbf{N}$, $\mathscr{P}(\mathbf{N})$, $\mathscr{P}(\mathscr{P}(\mathbf{N}))$, and so on, all have different cardinalities.) On January 5, 1874, just about one month after his discovery that $\mathbf{R}$ is not equinumerous to $\mathbf{N}$, Cantor wrote to Dedekind to ask whether the set of points on a curve is equinumerous to the set of points on a surface. For instance, is the real line $\mathbf{R}$ equinumerous to the Cartesian plane $\mathbf{R}^2$? Cantor thought not. Dedekind was not able to answer Cantor's question. Cantor himself was unable to answer it for about three and a half years. Perhaps the reason it took him so long to find the answer is that it turned out to be the opposite of what he expected. Very surprisingly, $\mathbf{R}$ *is* equinumerous to $\mathbf{R}^2$. Cantor communicated the proof of this to Dedekind in a letter dated June 20, 1877. Dedekind pointed out an error in Cantor's original proof. The error was related to the fact that certain real numbers have two different decimal expansions.[26] Cantor was able to replace his original flawed proof with a correct but more complicated one. With the help of Theorem 16.26, we are in a position to give a correct proof that is similar in spirit and simplicity to Cantor's original proof.

16.27 Theorem. (Cantor, 1877.) *The real line* $\mathbf{R}$ *is equinumerous to the Cartesian plane* $\mathbf{R}^2$.

Proof. Recall that $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$. Let $S = \{0,1\}^{\mathbf{N}}$. By Theorem 16.26, $\mathbf{R} \approx S$. Hence by Exercise 11, $S \times S \approx \mathbf{R} \times \mathbf{R}$. Therefore it suffices to show that $S \approx S \times S$. For each ordered pair (a,b) of sequences

[25] Some numbers have two binary expansions, a standard one ending in repeating 0's and an alternative one ending in repeating 1's. For instance, $1/2$ has the standard binary expansion $(0.1000\dots)_2$ and the alternative binary expansion $(0.0111\dots)_2$. The numbers in $[0,1)$ that have two binary expansions are the ones of the form $m/2^n$ where $n \in \mathbf{N}$ and $m \in \{1, 2, \dots, 2^n - 1\}$. All other numbers in $[0,1)$ have just one binary expansion.

[26] See Example 12.19 and the associated footnote.

$a = \langle\, a_1, a_2, a_3, \ldots \rangle$ and $b = \langle\, b_1, b_2, b_3, \ldots \rangle$ belonging to S, let $f(a, b)$ be the sequence that results from interleaving the terms of the sequences a and b; in other words, let

$$f(a, b) = \langle\, a_1, b_1, a_2, b_2, a_3, b_3, \ldots \rangle\,.$$

Then f is a bijection from $S \times S$ to S. Hence $S \times S \approx S$. ■

Exercise 12. Verify that the function f in the preceding proof is a bijection from $S \times S$ to S.

Exercise 13. Prove that for each $n \in \mathbf{N}$, $\mathbf{R}^n \approx \mathbf{R}$.

Exercise 14. Prove that the set $\mathbf{R}^{\mathbf{N}}$ of infinite sequences of real numbers is equinumerous to the set $\mathbf{R}$ of real numbers. (Hint: As in the proof of Theorem 16.27, let $S = \{\, 0, 1 \,\}^{\mathbf{N}}$, the set of infinite sequences of 0's and 1's. Since $\mathbf{R} \approx S$, it suffices to show that $S^{\mathbf{N}} \approx S$. By appropriately interleaving terms, an infinite sequence of infinite sequences of 0's and 1's can be mapped to a single infinite sequence of 0's and 1's. In this way, one can define a bijection from $S^{\mathbf{N}}$ to S.)

16.28 Remark. The discovery that $\mathbf{R}^n$ is equinumerous to $\mathbf{R}$ led Cantor to express scepticism about the validity of the notion of dimension. Dedekind exerted a moderating influence on Cantor's scepticism by pointing out that the one-to-one correspondence that Cantor had found between $\mathbf{R}^n$ and $\mathbf{R}$ was not continuous if $n \geq 2$. Dedekind conjectured that if $m, n \in \mathbf{N}$ and if there is a bijection f from $\mathbf{R}^m$ to $\mathbf{R}^n$ such that both $f\colon \mathbf{R}^m \to \mathbf{R}^n$ and $f^{-1}\colon \mathbf{R}^n \to \mathbf{R}^m$ are continuous, then $m = n$. Many mathematicians, including Cantor himself, tried to prove this. The first correct proof was published by the Dutch mathematician L. E. J. Brouwer in 1911, some 34 years after Dedekind formulated the conjecture.

The Continuum Hypothesis. Cantor published his proof that $\mathbf{R}^n$ is equinumerous to $\mathbf{R}$ in a paper that appeared in 1878. In the same paper, he expressed the belief that there were only two possibilities for the number of elements in an infinite subset of $\mathbf{R}$. Specifically, he conjectured that any infinite subset of $\mathbf{R}$ is equinumerous either to $\mathbf{N}$ or to $\mathbf{R}$. This conjecture has come to be known as the *continuum hypothesis*. Cantor tried repeatedly to prove his continuum hypothesis, but never succeeded. In 1938, the Austrian mathematician Kurt Gödel (1906–1978) showed that it is impossible to disprove the continuum hypothesis on the basis of the usual assumptions of set theory, including the axiom of choice. However, Gödel did not prove the continuum hypothesis. He just showed that it cannot be disproved. In 1963, the American mathematician Paul Cohen (1934–2007) showed that it is impossible to prove the continuum hypothesis on the basis of the usual assumptions of set theory, including the axiom of choice. Thus the continuum hypothesis can neither be proved nor disproved.[27] The remarkable effectiveness of mathematics as a problem-solving tool has had an enormous influence in shaping our modern technological world, but mathematics cannot answer all questions — not even all mathematical questions.

The Independence of the Axiom of Choice. At the same that Gödel and Cohen proved their results about the continuum hypothesis, they also proved analogous results about the axiom of choice. Specifically, Gödel showed that the axiom of choice cannot be disproved and Cohen showed that it cannot be proved, on the basis of the usual assumptions of set theory. Thus, like the continuum hypothesis, the axiom of choice is independent of the usual assumptions of set theory. Cohen's work introduced a powerful new method for the proof of independence results. This method was subsequently applied by many logicians to prove other such results, including some that we have already mentioned, such as the fact that the countable axiom of choice does not imply the principle of dependent choice, which in turn does not imply the axiom of choice, and the fact that without the axiom of choice one cannot prove that the union of a countable collection of countable sets is countable.

[27] One caveat should be mentioned. As is customary, we are assuming that the usual axioms of set theory are consistent. No one seriously believes that they are not, but they cannot be proved to be consistent. Since a false statement implies anything, if the usual axioms of set theory were not consistent, then they could be used to prove any statement of set theory, including both the continuum hypothesis and its negation. This caveat also applies in the discussion of the independence of the axiom of choice and to the earlier assertions of unprovability that we made in Remark 16.14 and Remark 16.17.

Ternary Expansions. We have already discussed decimal and binary expansions. Ternary expansions are like these except that they are in base 3 rather base 10 or base 2. Here we shall summarize without proof the basic facts about ternary expansions. If $t_1, t_2, \ldots, t_n \in \{0, 1, 2\}$, then in base 3,

$$(0.t_1t_2\ldots t_n)_3 = \frac{t_1}{3^1} + \frac{t_2}{3^2} + \cdots + \frac{t_n}{3^n}.$$

The subscript 3 at the end of the notation $(0.t_1t_2\ldots t_n)_3$ is to indicate that base 3 is intended. If $t_1, t_2, t_3, \cdots \in \{0, 1, 2\}$, then to say that a number $x \in [0, 1]$ has the ternary expansion $(0.t_1t_2t_3\ldots)_3$ means that for each $n \in \mathbf{N}$,

$$(0.t_1t_2\ldots t_n)_3 \leq x \leq (0.t_1t_2\ldots t_n)_3 + \frac{1}{3^n}.$$

For each sequence $\langle t_1, t_2, t_3, \ldots \rangle$ belonging to $\{0, 1, 2\}^{\mathbf{N}}$, there is a unique number $x \in [0, 1]$ having the ternary expansion $(0.t_1t_2t_3\ldots)_3$. Conversely, each number $x \in [0, 1]$ has such a ternary expansion. However the numbers of the form $m/3^n$, where $n \in \mathbf{N}$ and $m \in \{1, 2, \ldots, 3^n - 1\}$, have two such ternary expansions, a standard one ending in repeating 0's and an alternative one ending in repeating 2's. Any other number in $[0, 1]$ has exactly one such ternary expansion, and it does not end in repeating 0's or repeating 2's, except for 0 and 1, which have the ternary expansions $(0.000\ldots)_3$ and $(0.222\ldots)_3$ respectively.

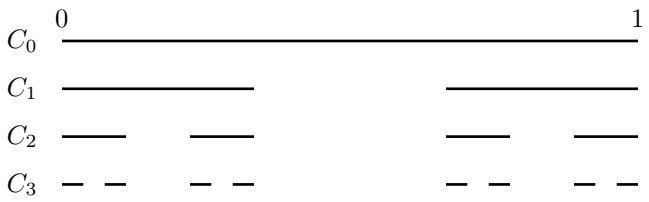
The Cantor Set. Intervals are among the simplest subsets of $\mathbf{R}$. Much more complicated subsets of $\mathbf{R}$ are imaginable. Cantor was one of the first people to realize just how complicated a subset of $\mathbf{R}$ can be. He began producing examples of complicated subsets of $\mathbf{R}$ even before his discovery that $\mathbf{R}$ is uncountable. But the most famous such example that Cantor produced was introduced in a single paragraph near the end of a long paper that he published in 1883. This example has come to be called the *Cantor set*. The Cantor set is constructed as follows. Let

$$\begin{aligned}
&C_0 = [0, 1],\\
&C_1 = [0, 1/3] \cup [2/3, 1],\\
&C_2 = [0, 1/9] \cup [2/9, 1/3] \cup [2/3, 7/9] \cup [8/9, 1],\\
&\text{and so on.}
\end{aligned}$$

The set C_1 is obtained by removing the open middle-third interval $(1/3, 2/3)$ from C_0. Note that C_1 is the union of 2 disjoint closed intervals each of length $1/3$. The set C_2 is obtained by removing the open middle-third of each of these intervals from C_1. For each $n \in \boldsymbol{\omega}$, C_n is the union of 2^n disjoint closed intervals each of length $1/3^n$ and the set C_{n+1} is obtained by removing the open middle-third of each of these intervals from C_n. In this way we construct a decreasing sequence

$$C_0 \supseteq C_1 \supseteq C_2 \supseteq C_3 \supseteq \cdots$$

of subsets of $[0, 1]$. The following figure illustrates the first four of these sets as they would appear if sketched on a number line.



The Cantor set C is defined to be the intersection of these sets; in other words,

$$C = \bigcap_{n=0}^{\infty} C_n.$$

Because of the way the sets $C_0, C_1, C_2, C_3, \dots$ get smaller and smaller, one might be tempted to think that C is empty. But this is far from the case. In fact, C is equinumerous to $\mathbf{R}$. This follows from an alternative description of C in terms of ternary expansions. We shall now outline this alternative description. Note that the numbers belonging to the interval $[0, 1/3]$ are the ones which have a ternary expansion $(0.t_1t_2t_3\dots)_3$ with $t_1 = 0$. Note also that the numbers belonging to the interval $[2/3, 1]$ are the ones which have a ternary expansion $(0.t_1t_2t_3\dots)_3$ with $t_1 = 2$. Hence C_1 is the set of numbers in $[0, 1]$ that have a ternary expansion $(0.t_1t_2t_3\dots)_3$ with $t_1 \in \{\, 0, 2 \,\}$. Similarly, C_2 is the set of numbers in $[0, 1]$ that have a ternary expansion $(0.t_1t_2t_3\dots)_3$ with $t_1 \in \{\, 0, 2 \,\}$ and $t_2 \in \{\, 0, 2 \,\}$. For each $n \in \mathbf{N}$, C_n is the set of numbers in $[0, 1]$ that have a ternary expansion $(0.t_1t_2t_3\dots)_3$ with $t_1, t_2, \dots, t_n \in \{\, 0, 2 \,\}$. Hence the Cantor set C is the set of numbers in $[0, 1]$ which have a ternary expansion $(0.t_1t_2t_3\dots)_3$ such that for each $k \in \mathbf{N}$, $t_k \in \{\, 0, 2 \,\}$. In other words, C is the set of numbers in $[0, 1]$ which have a ternary expansion $(0.t_1t_2t_3\dots)_3$ such that for each $k \in \mathbf{N}$, $t_k \neq 1$. Let $T = \{\, 0, 2 \,\}^{\mathbf{N}}$ be the set of all infinite sequences of 0's and 2's and let

$$f(t_1, t_2, t_3, \dots) = (0.t_1t_2t_3\dots)_3$$

for all $\langle\, t_1, t_2, t_3, \dots \,\rangle \in T$. It is not difficult to show that f is a bijection from T to C. Hence $T \approx C$. Let $B = \{\, 0, 1 \,\}^{\mathbf{N}}$ be the set of all infinite sequences of 0's and 1's. Then $B \approx T$ because if we let

$$g(b_1, b_2, b_3, \dots) = \langle\, 2b_1, 2b_2, 2b_3, \dots \,\rangle$$

for all $\langle\, b_1, b_2, b_3, \dots \,\rangle \in B$, then g is a bijection from B to T. Now by Theorem 16.26, $\mathbf{R} \approx B$. Hence $\mathbf{R} \approx C$ as we set out to show.

Without going into details, and even without precisely defining all our terms, let us mention some other noteworthy properties of the Cantor set C. The Cantor set C is "perfect," in the sense that it is equal to its set of limit points. The Cantor set C is "nowhere dense," in the sense that each nondegenerate interval, no matter how small, contains points which are not limit points of the Cantor set. For each $n \in \mathbf{N}$, $C \subseteq C_n$ and the total length of C_n is $(2/3)^n$ because C_n the union of 2^n disjoint intervals each of length $1/3^n$. Note that $(2/3)^n \to 0$ as $n \to \infty$. Hence the "total length" of the Cantor set C is 0. How astonishing it is that such a small set can have the same number of elements as the whole real line $\mathbf{R}$.

The Schroeder-Bernstein Theorem. Cantor considered it intuitively evident that if A and B are sets such that $\overline{\overline{A}} \leq \overline{\overline{B}}$ and $\overline{\overline{B}} \leq \overline{\overline{A}}$, then $\overline{\overline{A}} = \overline{\overline{B}}$. In fact, though, this requires proof. The first person to supply a proof seems to have been Dedekind, in 1887. However, Dedekind never published his proof and the result has come to be named after Schroeder and Bernstein, who proved it several years later, independently of Dedekind and of each other.

16.29 Theorem. (Schroeder, 1896; Bernstein, 1896.) *Let A and B be sets. Suppose $\overline{\overline{A}} \leq \overline{\overline{B}}$ and $\overline{\overline{B}} \leq \overline{\overline{A}}$. Then $\overline{\overline{A}} = \overline{\overline{B}}$.*

Proof. Since $\overline{\overline{A}} \leq \overline{\overline{B}}$, there is an injection f from A to B. Since $\overline{\overline{B}} \leq \overline{\overline{A}}$, there is an injection g from B to A. To show that $\overline{\overline{A}} = \overline{\overline{B}}$, we must show that there is a bijection h from A to B. We shall construct h by letting h agree with f on a certain subset of A and letting h agree with g^{-1} on the rest of A. Let $A_0 = A$, $B_0 = B$, and for each $n \in \boldsymbol{\omega}$, if A_n and B_n have already been defined, let $A_{n+1} = g[B_n]$ and $B_{n+1} = f[A_n]$. Then

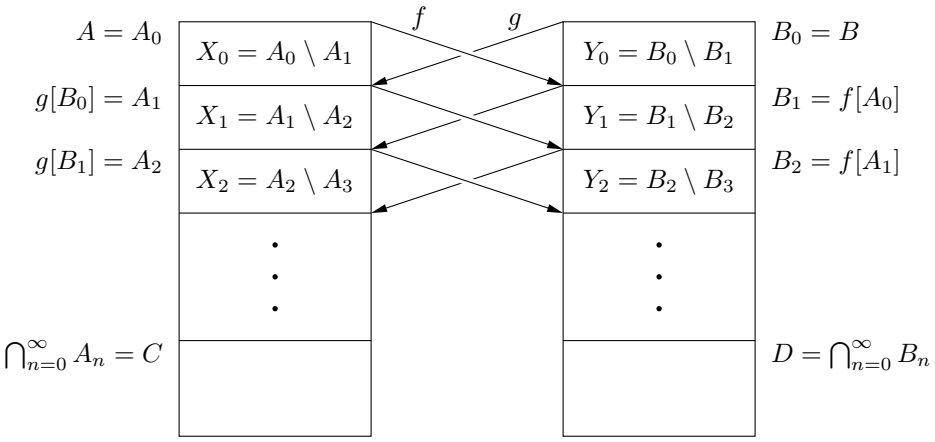
$$A_0 \supseteq A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots$$

and

$$B_0 \supseteq B_1 \supseteq B_2 \supseteq B_3 \supseteq \cdots .$$

Let $C = \bigcap_{n=0}^{\infty} A_n$, let $D = \bigcap_{n=0}^{\infty} B_n$, and for each $n \in \boldsymbol{\omega}$, let $X_n = A_n \setminus A_{n+1}$ and let $Y_n = B_n \setminus B_{n+1}$. The following figure schematically depicts the sets A and B, the injections f and g, and the sets A_n, B_n,

C, D, X_n, and Y_n.



For each $n \in \boldsymbol{\omega}$, $f \restriction A_n$ is a bijection from A_n to B_{n+1} and $g \restriction B_n$ is a bijection from B_n to A_{n+1}. Hence $f \restriction C$ is a bijection from C to D and for each $n \in \boldsymbol{\omega}$, $f \restriction X_n$ is a bijection from X_n to Y_{n+1} and $g^{-1} \restriction X_{n+1}$ is a bijection from X_{n+1} to Y_n. For all $x \in A$, let

$$h(x) = \begin{cases} f(x) & \text{if } x \in X_n \text{ where } n \in \boldsymbol{\omega} \text{ and } n \text{ is even,} \\ g^{-1}(x) & \text{if } x \in X_n \text{ where } n \in \boldsymbol{\omega} \text{ and } n \text{ is odd,} \\ f(x) & \text{if } x \in C. \end{cases}$$

Then h is a bijection from A to B. Hence $\overline{\overline{A}} = \overline{\overline{B}}$. ■

Exercise 15. Let the notation be as in the proof of the Schroeder-Bernstein theorem.

- **(a)** Verify that for each $n \in \boldsymbol{\omega}$, $f \restriction A_n$ is a bijection from A_n to B_{n+1} and $g \restriction B_n$ is a bijection from B_n to A_{n+1}.
- **(b)** Verify $f \restriction C$ is a bijection from C to D.
- **(c)** Verify that for each $n \in \boldsymbol{\omega}$, $f \restriction X_n$ is a bijection from X_n to Y_{n+1} and $g^{-1} \restriction X_{n+1}$ is a bijection from X_{n+1} to Y_n.
- **(d)** Verify that h is a bijection from A to B.
- **(e)** Explain why the proof of the Schroeder-Bernstein theorem would still work if for $x \in C$, we let $h(x)$ be $g^{-1}(x)$ instead $f(x)$.

Exercise 16. Let A be a subset of $\mathbf{R}$ which contains a nondegenerate interval I. Prove that A is equinumerous to $\mathbf{R}$. (Hint: Use the Schroeder-Bernstein theorem.)

16.30 Remark. The condition in the preceding exercise is sufficient for a subset $A \subseteq \mathbf{R}$ to be equinumerous to $\mathbf{R}$, but not necessary. As we have seen, the Cantor set is a subset of $\mathbf{R}$ which is equinumerous to $\mathbf{R}$ but contains no nondegenerate interval.

16.31 Remark. It can be shown that for any two sets A and B, either $\overline{\overline{A}} \leq \overline{\overline{B}}$ or $\overline{\overline{B}} \leq \overline{\overline{A}}$. However, unlike the Schroeder-Bernstein theorem, this result depends on the axiom of choice and in fact is equivalent to the axiom of choice, in the context of the usual assumptions of set theory. We shall return to this point later.

16.32 Remark. Let A and B be sets and suppose that there is a surjection f from B onto A. Then it seems intuitively clear that $\overline{\overline{A}} \leq \overline{\overline{B}}$. We have already seen in Proposition 16.6 that this is true if B is countable. However, if B is uncountable, then the natural proof of this uses the axiom of choice, as follows. For each $\alpha \in A$, let $C_\alpha = f^{-1}[\{\alpha\}]$. Then $\langle C_\alpha \rangle_{\alpha \in A}$ is an indexed family of subsets of B. Since f is a surjection from B to A, each C_α is nonempty. Hence by the axiom of choice, there is a choice function g for the family $\langle C_\alpha \rangle_{\alpha \in A}$. Then $g\colon A \to B$, because for each $\alpha \in A$, $g(\alpha) \in C_\alpha \subseteq B$. Also, for each $\alpha \in A$, we have $g(\alpha) \in C_\alpha = f^{-1}[\{\alpha\}]$, so $f(g(\alpha)) \in \{\alpha\}$, so $f(g(\alpha)) = \alpha$. Hence g is an injection, because for all $\alpha_1, \alpha_2 \in A$, if $g(\alpha_1) = g(\alpha_2)$, then $\alpha_1 = f(g(\alpha_1)) = f(g(\alpha_2)) = \alpha_2$. Thus g is an injection from A to B. Therefore $\overline{\overline{A}} \leq \overline{\overline{B}}$.

Section 17. Relations

Informally, a "relation" links certain objects to certain other objects. To completely describe a particular relation, it suffices to say which ordered pairs (x, y) of objects are such that the object x is linked to the object y. Accordingly, it is customary to adopt the following formal mathematical definition of a relation.

17.1 Definition. To say that R *is a relation* means that R is a set of ordered pairs.

17.2 Example. Let A be the set of people who are currently alive in the world and let

$$R = \{\, (x, y) : x \in A,\ y \in A, \text{ and } x \text{ is the mother of } y \,\}.$$

Then R is a relation.

17.3 Example. Let $S = \{\, (x, y) : x \text{ and } y \text{ are natural numbers and } x < y \,\}$. Then S is a relation.

17.4 Example. Let A be the set of all web pages on the world wide web. Let

$$L = \{\, (x, y) : x \in A,\ y \in A, \text{ and } x \text{ links to } y \,\}.$$

Then L is a relation.

17.5 Definition. Let R be a relation. To say that x *has the relation* R *to* y (denoted $x\ R\ y$) means that $(x, y) \in R$.

17.6 Example. Let R and A be as in Example 17.2. If $x, y \in A$, then to write $x\ R\ y$ means the same thing as to write "x is the mother of y."

17.7 Example. Let S be as in Example 17.3. If x and y are natural numbers, then to write $x\ S\ y$ means the same thing as to write $x < y$. (Of course, this holds true only in a context where S has been defined in this way.)

17.8 Example. Let L and A be as in Example 17.4. If x and y are web pages, then to write $x\ L\ y$ means the same thing as to say "x links to y."

17.9 Definition. Let R be a relation. The *domain of* R (denoted $\mathrm{Dom}(R)$) is the set of all x such that for some y, we have $x\ R\ y$; in other words,

$$\mathrm{Dom}(R) = \{\, x : x\ R\ y \text{ for some } y \,\}.$$

17.10 Definition. Let R be a relation. The *range of* R (denoted $\mathrm{Rng}(R)$) is the set of all y such that for some x, we have $x\ R\ y$; in other words,

$$\mathrm{Rng}(R) = \{\, y : x\ R\ y \text{ for some } x \,\}.$$

17.11 Example. Let A and R be as in Example 17.2. Then the domain of R is the set of all mothers in the world and the range of R is the set of all people in the world whose mothers are currently alive.

17.12 Example. Let S be as in Example 17.3. Then the domain of S is the set $\mathbf{N} = \{\, 1, 2, 3, \ldots \,\}$ of natural numbers and the range of S is the set $\{\, 2, 3, 4, \ldots \,\}$.

Exercise 1. For each of the relations R defined below, find the domain of R and the range of R.

(a) $R = \{\, (x, y) : x \text{ and } y \text{ are integers and } x < y \,\}$.
(b) $R = \{\, (x, y) : x, y \in [0, \infty) \text{ and } x < y \,\}$.
(c) $R = \{\, (x, y) : x, y \in (0, \infty) \text{ and } x < y \,\}$.
(d) $R = \{\, (x, y) : x, y \in [0, \infty) \text{ and } x \leq y \,\}$.

17.13 Definition. Let A and B be sets. To say that R *is a relation between* A *and* B means that R is a relation, the domain of R is a subset of A, and the range of R is a subset of B.

17.14 Example. Let M be the set of all men in the world, let W be the set of all women in the world, and let

$$H = \{\, (x, y) : x \in M,\ y \in W, \text{ and } x \text{ is the husband of } y \,\}.$$

Then H is a relation between M and W. The domain of H is the set of all married men in the world and the range of H is the set of all married women in the world.

17.15 Example. Let A and B be sets, let f be a function from A to B, and let

$$G = \{\, (x, y) : x \in A \text{ and } y = f(x) \,\}.$$

Then G is a relation between A and B. The domain of G is A, the same as the domain of f. The range of G is the same as the range of f. We recall that G is the graph of the function f and that according to one approach to the concept of a function, G is actually the same thing as f.

17.16 Remark. We have specified each relation that we have considered above by explicitly writing out the set of ordered pairs that it is equal to. In common mathematical language, however, one usually specifies a relation in a more succinct way. Let us illustrate this way by an example. Let M and W be as in Example 17.14. Then the relation H there would usually be specified by saying "Let H be the relation between M and W defined by $x\ H\ y$ iff x is the husband of y."

17.17 Example. Let A be a set and let $\mathscr{B}$ be a set of sets. To say that R is the relation between A and $\mathscr{B}$ defined by $a\ R\ B$ iff $a \in B$, means that

$$R = \{\, (a, B) : a \in A,\ B \in \mathscr{B}, \text{ and } a \in B \,\}.$$

17.18 Definition. Let A be a set. To say that R *is a relation on* A means that R is a relation and both the domain and the range of R are subsets of A.

17.19 Example. Let A be a set and let $E = \{\, (x, x) : x \in A \,\}$. Then E is a relation on A. Note that

$$E = \{\, (x, y) : x \in A,\ y \in A, \text{ and } x = y \,\}.$$

In other words, E is the relation on A defined by $x\ E\ y$ iff $x = y$. For this reason, E is called *the relation of equality on* A.

17.20 Remark. Let A and B be sets. Note that R is a relation between A and B iff R is a subset of $A \times B$, the Cartesian product of A and B. Similarly, R is a relation on A iff R is a subset of $A \times A$, the Cartesian product of A with itself.

Exercise 2. Let $A = \{\, 1, 2, 3 \,\}$. How many relations on A are there? (Do not try to list them all. It would take too long.)

17.21 Definition. Let R be a relation. To say that R *is transitive* means that for all x, y, and z, if $x\ R\ y$ and $y\ R\ z$, then $x\ R\ z$.

17.22 Definition. Let R be a relation. To say that R *is symmetric* means that for all x and y, if $x\ R\ y$, then $y\ R\ x$.

17.23 Definition. Let R be a relation. To say that R *is antisymmetric* means that for all x and y, if $x\ R\ y$ and $y\ R\ x$, then $x = y$.

17.24 Definition. Let A be a set and let R be a relation on A. To say that R *is reflexive on* A means that for each $x \in A$, we have $x\ R\ x$.

Exercise 3. Let A be a set and let R be the relation of equality on A. Determine whether R is transitive or not, symmetric or not, antisymmetric or not, and reflexive on A or not.

Exercise 4. Let R be the relation on $\mathbf{N}$ defined by $x\ R\ y$ iff $x \leq y$. Determine whether R is transitive or not, symmetric or not, antisymmetric or not, and reflexive on $\mathbf{N}$ or not.

Exercise 5. Let R be the relation on $\mathbf{N}$ defined by $x\ R\ y$ iff $x < y$. Determine whether R is transitive or not, symmetric or not, antisymmetric or not, and reflexive on $\mathbf{N}$ or not.

Exercise 6. Let A be the set of people who are currently alive in the world. For each of the relations R on A defined below, determine whether R is transitive or not, symmetric or not, antisymmetric or not, and reflexive on A or not.

(a) $x\ R\ y$ iff x is a brother of y.
(b) $x\ R\ y$ iff x is a sibling of y.
(c) $x\ R\ y$ iff x is at least as tall as y.
(d) $x\ R\ y$ iff x is strictly taller than y.
(e) $x\ R\ y$ iff x and y have the same paternal grandmother.
(f) $x\ R\ y$ iff x knows y.
(g) $x\ R\ y$ iff x knows of y.
(h) $x\ R\ y$ iff x likes y.

Equivalence Relations.

17.25 Definition. Let A be a set. To say that R *is an equivalence relation on* A means that R is a relation on A and R is reflexive on A, symmetric, and transitive.

To remember the definition of an equivalence relation, it may help to remember the letters RST which are the first letters of the three words *reflexive*, *symmetric*, and *transitive*.

17.26 Example. Let A be a set. One of the simplest examples of an equivalence relation on A is the relation of equality on A. Recall that this is the relation E on A defined by $x\ E\ y$ iff $x = y$. Another very simple example of an equivalence relation on A is the relation F on A defined by $x\ F\ y$ iff $x, y \in A$. The two relations E and F are the most extreme examples of equivalence relations on A. On the one hand, two elements of A have the relation E to each other only if they are equal. On the other hand, any two elements of A have the relation F to each other.

Exercise 7. Let A, E, and F be as in Example 17.26. Let R be any relation on A. Show that $R \subseteq F$ and that if R is reflexive on A, then $E \subseteq R$.

17.27 Example. Let $\mathscr{M}$ be a set of sets. Let R be the relation on $\mathscr{M}$ defined by $A\ R\ B$ iff A is equinumerous to B. As we know, equinumerousness is reflexive, symmetric, and transitive. Hence R is an equivalence relation on $\mathscr{M}$.

Exercise 8. Let $m \in \mathbf{Z}$ and let C be the relation on $\mathbf{Z}$ defined by $x\ C\ y$ iff m divides $y - x$. Show that C is an equivalence relation on $\mathbf{Z}$. (You may recall that C is the relation of congruence modulo m that we discussed earlier. The standard notation for $x\ C\ y$ in this example is $x \equiv y \mod m$.)

Exercise 9. Let A be a set and let f be a function whose domain is A. Let R be the relation on A defined by $x\ R\ y$ iff $f(x) = f(y)$. Show that R is an equivalence relation on A.

17.28 Remark. As we shall see, all equivalence relations may be viewed as arising in the way described in Exercise 9, in the sense that for each set A and each equivalence relation R on A, there exists a function f whose domain is A such that for all $x, y \in A$, we have $x\ R\ y$ iff $f(x) = f(y)$.

Exercise 10. Let A, E, and F be as in Example 17.26. Find functions g and h on A such that for all $x, y \in A$, we have $x\ E\ y$ iff $g(x) = g(y)$, and $x\ F\ y$ iff $h(x) = h(y)$.

Exercise 11. Let $m \in \mathbf{N}$ and let C be as in Exercise 8. We may define functions q and r on $\mathbf{Z}$ by letting $q(x)$ and $r(x))$ be the quotient and remainder that result when x is divided by m, for each $x \in \mathbf{Z}$. (To be precise, for each $x \in \mathbf{Z}$, we let $(q(x), r(x))$ be the unique ordered pair such that $q(x) \in \mathbf{Z}$, $r(x) \in \{\, 0, \ldots, m-1 \,\}$, and $x = q(x)m + r(x)$.) Show that for all $x, y \in \mathbf{Z}$, we have $x\ C\ y$ iff $r(x) = r(y)$.

17.29 Definition. Let A be a set, let R be an equivalence relation on A, and let $x \in A$. Then the *R-equivalence class of x* (denoted $[x]_R$) is the set of all $y \in A$ such that $x\ R\ y$; in other words,

$$[x]_R = \{\, y \in A : x\ R\ y \,\}.$$

If no confusion is likely to result, the notation $[x]_R$ is often shortened to $[x]$.

Exercise 12. Let A, E, and F be as in Example 17.26.
(a) For each $x \in A$, what is $[x]_E$?
(b) For each $x \in A$, what is $[x]_F$?

17.30 Example. Let C be the relation of congruence modulo 2 on $\mathbf{Z}$. In other words, let C be as in Exercise 8 with $m = 2$. From Exercise 8, we know that C is an equivalence relation on $\mathbf{Z}$. For each $x \in \mathbf{Z}$, x is even iff $x\ C\ 0$, and x is odd iff $x\ C\ 1$. Hence there are exactly two C-equivalence classes. They are the set

$$[0]_C = \{\, 2q : q \in \mathbf{Z} \,\} = \{\, \ldots, -4, -2, 0, 2, 4, \ldots \,\}$$

of even integers, and the set

$$[1]_C = \{\, 2q + 1 : q \in \mathbf{Z} \,\} = \{\, \ldots, -3, -1, 1, 3, 5, \ldots \,\}$$

of odd integers.

Exercise 13. Let C be the relation of congruence modulo 3 on $\mathbf{Z}$. In other words, let C be as in Exercise 8 with $m = 3$. (Then by Exercise 8, C is an equivalence relation on $\mathbf{Z}$.) Find all the C-equivalence classes.

Exercise 14. Let A be a set, let f be a function whose domain is A, and let R be the relation on A defined by $x\ R\ y$ iff $f(x) = f(y)$. By Exercise 9, R is an equivalence relation on A. Show that for each $x \in A$, we have $[x]_R = f^{-1}[\{\, f(x) \,\}]$.

17.31 The Fundamental Theorem on Equivalence Classes. *Let A be a set and let R be an equivalence relation on A. For each $x \in A$, let $[x] = [x]_R$, the R-equivalence class of x. Then:*
(a) *For each $x \in A$, we have $x \in [x]$ (so in particular, $[x] \neq \emptyset$).*
(b) *For all $x, y \in A$, if $x\ R\ y$, then $[x] = [y]$.*
(c) *For all $x, y \in A$, if it is not the case that $x\ R\ y$, then $[x] \cap [y] = \emptyset$.*

Proof. (a). Consider any $x \in A$. Then $x\ R\ x$, because R is reflexive on A. Hence $x \in [x]$.

(b). Consider any $x, y \in A$. Suppose $x\ R\ y$. Then $y\ R\ x$ too, because R is symmetric. We wish to show that $[x] = [y]$. To show this, we shall show that each of the sets $[x]$ and $[y]$ is a subset of the other. Let $z \in [x]$. Then $x\ R\ z$. Hence $y\ R\ z$, because $y\ R\ x$, $x\ R\ z$, and R is transitive. Thus $z \in [y]$. This shows that $[x] \subseteq [y]$. Now let $z \in [y]$. Then $y\ R\ z$. Hence $x\ R\ z$, because $x\ R\ y$, $y\ R\ z$, and R is transitive. This shows that $[y] \subseteq [x]$. Hence $[x] = [y]$, because $[x]$ and $[y]$ are sets, $[x] \subseteq [y]$, and $[y] \subseteq [x]$.

(c). Consider any $x, y \in A$. We wish to show that if it is not the case that $x\ R\ y$, then $[x] \cap [y] = \emptyset$. By contraposition, it is equivalent to show that if $[x] \cap [y] \neq \emptyset$, then $x\ R\ y$. Suppose $[x] \cap [y] \neq \emptyset$. We wish to show that $x\ R\ y$. Since $[x] \cap [y] \neq \emptyset$, we can pick $z \in [x] \cap [y]$. Then $x\ R\ z$, because $z \in [x]$. Similarly, $y\ R\ z$, because $z \in [y]$. Hence $z\ R\ y$, because R is symmetric. But then $x\ R\ y$ as desired, because $x\ R\ z$, $z\ R\ y$, and R is transitive. ■

17.32 Definition. Let A be a set. To say that Π *is a partition of* A means that Π is a pairwise-disjoint collection of nonempty sets whose union is A.

17.33 Remark. Let A be a set. Then Π is a partition of A iff Π is a collection of nonempty subsets of A such that each element of A belongs to exactly one element of Π.

Exercise 15.
(a) List all the partitions of the empty set.
(b) List all the partitions of the set $\{\, 1 \,\}$.
(c) List all the partitions of the set $\{\, 1, 2 \,\}$.
(d) List all the partitions of the set $\{\, 1, 2, 3 \,\}$.

17.34 Definition. Let A be a set and let R be an equivalence relation on A. Then the *quotient of A by R* (denoted A/R) is the collection of R-equivalence classes of elements of A; in other words,

$$A/R = \{\, [x]_R : x \in A \,\}.$$

17.35 The Fundamental Theorem on Equivalence Relations. *Let A be a set. Then there is a natural one-to-one correspondence between equivalence relations on A and partitions of A. More specifically:*

- **(a)** *Let R be an equivalence relation on A. Let $\Pi = A/R$. Then Π is a partition of A. Moreover, for all $x, y \in A$, we have $x \mathrel{R} y$ iff x and y belong to the same element of Π.*
- **(b)** *Let Π be a partition of A. Let R be the relation on A defined by $x \mathrel{R} y$ iff x and y belong to the same element of Π. Then R is an equivalence relation on A. Moreover, $\Pi = A/R$.*

Proof. (a). Let R be an equivalence relation on A and let $\Pi = A/R$. As usual, let us write $[x]$ for $[x]_R$. Then $\Pi = \{\, [x] : x \in A \,\}$, by the definition of A/R. For each $x \in A$, we have $[x] \subseteq A$, by the definition of $[x]$, and we have $x \in [x]$, by Theorem 17.31(a). Hence each element of Π is a nonempty subset of A and each element of A belongs to at least one element of Π. It follows that Π is a collection of nonempty sets and that the union of Π is A. It remains to show that any two distinct elements of Π are disjoint. Let P_1 and P_2 be distinct elements of Π. Since $P_1, P_2 \in \Pi$, we can pick $x_1, x_2 \in A$ such that $P_1 = [x]$ and $P_2 = [x_2]$. We wish to show that $[x_1] \cap [x_2] = \emptyset$. Since P_1 and P_2 are distinct, $[x_1] \neq [x_2]$. Hence by Theorem 17.31(b), it is not the case that $x_1 \mathrel{R} x_2$. But then, by Theorem 17.31(c), $[x_1] \cap [x_2] = \emptyset$, as desired.

(b). Let Π be a partition of A and let R be the relation on A defined by $x \mathrel{R} y$ iff x and y belong to the same element of Π. Since Π is a partition of A, each element of A belongs to exactly one element of Π. Define a function f on A by letting $f(x)$ be the unique element of Π to which x belongs, for each $x \in A$. Then for all $x, y \in A$, we have $x \mathrel{R} y$ iff $f(x) = f(y)$. Hence by Exercise 9, R is an equivalence relation on A. As usual, let us write $[x]$ for $[x]_R$. To show that the set Π is equal to the set A/R, we shall show that each of these two sets is a subset of the other. Let $P \in \Pi$. Then P is a nonempty subset of A. Let $x \in P$. Then $x \in A$. Now for each $y \in A$, we have $y \in [x]$ iff $x \mathrel{R} y$ iff $y \in P$. Hence the sets $[x]$ and P have the same elements, so $[x] = P$. Thus $P \in A/R$. This shows that $\Pi \subseteq A/R$. Now let $Q \in A/R$. Then $Q = [x]$ for some $x \in A$. Let P be the unique element of Π to which x belongs. Then for each $y \in A$, we have $y \in Q$ iff $x \mathrel{R} y$ iff $y \in P$. Hence the sets Q and P have the same elements, so $Q = P$. Thus $Q \in \Pi$. This shows that $A/R \subseteq \Pi$. ■

Exercise 16. Let $E_0 = 1$ and for each $n \in \mathbf{N}$, let E_n be the number of equivalence relations on the n-element set $\{\, 1, \ldots, n \,\}$. Show that for each $n \in \boldsymbol{\omega}$, we have

$$E_{n+1} = \sum_{k=0}^{n} \binom{n}{k} E_k.$$

(Hint: By Theorem 17.35, the number of equivalence relations on a set is the same as the number of partitions of the set.)

The next result fulfills the promise that we made in Remark 17.28.

17.36 Theorem. *Let A be a set and let R be an equivalence relation on A. As usual, write $[x]$ for $[x]_R$. Define a function f from A to A/R by $f(x) = [x]$ for all $x \in A$. Then f is a surjection from A to A/R. Moreover, for all $x, y \in A$, we have $x \mathrel{R} y$ iff $f(x) = f(y)$.*

Proof. Since $f(x) = [x]$ for all $x \in A$ and since $A/R = \{\, [x] : x \in A \,\}$, we have $A/R = \{\, f(x) : x \in A \,\}$. Thus the range of f is A/R. Hence f is a surjection from A to A/R. Now let us show that for all $x, y \in A$, we have $x \mathrel{R} y$ iff $f(x) = f(y)$. Consider any $x, y \in A$. In view of the way f was defined, what we wish to show is that $x \mathrel{R} y$ iff $[x] = [y]$. By Theorem 17.31(b), we know that if $x \mathrel{R} y$, then $[x] = [y]$. Conversely, suppose $[x] = [y]$. We wish to show that $x \mathrel{R} y$. In other words, we wish to show that $y \in [x]$. But by Theorem 17.31(a), we know that $y \in [y]$. Since $[x] = [y]$, it follows that $y \in [x]$, as desired. ■

17.37 Remark. Given a set A and an equivalence relation R on A, the function f from A to A/R defined, as in Theorem 17.36, by $f(x) = [x]_R$ for all $x \in A$, is called *the canonical surjection from A to A/R*.

The next result is the prototype of a class of results that are called *homomorphism theorems*. You will learn more about these if you take a course in abstract algebra.

17.38 Theorem. *Let A and B be sets and let h be a function from A to B. Then there is a set C such that h can be expressed as $h = g \circ f$ where f is a surjection from A to C and g is an injection from C to B.*

Proof. Let R be the relation on A defined by $x\ R\ y$ iff $h(x) = h(y)$. By Exercise 9, R is an equivalence relation on A. We shall show that we can take C to be A/R. Let f be the canonical surjection from A to A/R. Define $g\colon A/R \to B$ by $g([x]) = h(x)$ for all $x \in A$. (Of course, by $[x]$ we mean $[x]_R$.) Note that g is well-defined, because for all $x_1, x_2 \in A$, if $[x_1] = [x_2]$, then $x_1\ R\ x_2$, so $h(x_1) = h(x_2)$. Also, g is an injection, because for all $x_1, x_2 \in A$, if $g([x_1]) = g([x_2])$, then $h(x_1) = h(x_2)$, so $x_1\ R\ x_2$, so $[x_1] = [x_2]$. Finally, $h = g \circ f$, because for all $x \in A$, $(g \circ f)(x) = g(f(x)) = g([x]) = h(x)$. ■

Partial Order Relations.

17.39 Definition. Let A be a set. To say that R *is a partial order relation on* A means that R is a relation on A and R is reflexive on A, antisymmetric, and transitive.

To remember the definition of a partial order relation on A, it may help to remember the letters RAT which are the first letters of the three words *reflexive*, *antisymmetric*, and *transitive*. By the way, sometimes the phrase "partial order relation" is shortened to *order relation*.

17.40 Example. Let R be the relation on the set $\boldsymbol{\omega} = \{\,0, 1, 2, \dots\,\}$ of whole numbers, defined by $x\ R\ y$ iff $x \leq y$. Then R is a partial order relation on $\boldsymbol{\omega}$.

17.41 Example. Let A be a set of sets and let S be the relation on A defined by $x\ S\ y$ iff $x \subseteq y$. Then S is a partial order relation on A.

17.42 Remark. According to one way of defining the whole numbers, $0 = \emptyset$, $1 = \{\,0\,\}$, $2 = \{\,0, 1\,\}$, $3 = \{\,0, 1, 2\,\}$, and so on. If this definition is adopted, then for all $x, y \in \boldsymbol{\omega}$, we have $x \leq y$ iff $x \subseteq y$. Thus the partial order relation R in Example 17.40 may be viewed as a special case of the partial order relation S in Example 17.41.

17.43 Example. Let D be the relation on $\boldsymbol{\omega}$ defined by $x\ D\ y$ iff x divides y. Then D is a partial order relation on $\boldsymbol{\omega}$. Note that D is different from the partial order relation R on $\boldsymbol{\omega}$ that we considered in Example 17.40. For instance, $3\ R\ 7$ but it is not the case that $3\ D\ 7$, and $3\ D\ 0$ but it is not the case that $3\ R\ 0$.

17.44 Example. Let D' be the relation on the set $\mathbf{Z}$ of integers, defined by $x\ D'\ y$ iff x divides y. Then D' is not a partial order relation on $\mathbf{Z}$ because it is not antisymmetric. For instance, $3\ D'\ {-3}$ and ${-3}\ D'\ 3$, but $3 \neq -3$.

17.45 Definition. Let A be a set. To say that R *is a total order relation on* A means that R is a partial order relation on A and for all $x, y \in A$, we have $x\ R\ y$ or $y\ R\ x$.

17.46 Remark. Let A be a set, let R be a partial order relation on A, and let $x, y \in A$. To say that x *and* y *are comparable* (or more specifically, R*-comparable*) means that $x\ R\ y$ or $y\ R\ x$. In terms of this terminology, the partial order relation R on A is a total order relation on A when every two elements of A are R-comparable.

17.47 Remark. The usual order relation on the real line $\mathbf{R}$ is a total order relation. For this reason, another name for a total order relation is a *linear order relation*.

17.48 Example. Let R be as in Example 17.40 and let D be as in Example 17.43. As we already remarked, both R and D are partial order relations on A. We now point out that R is a total order relation on $\boldsymbol{\omega}$ but D is not. To see that D is not a total order relation on $\boldsymbol{\omega}$, note for instance that neither of the numbers 4 and 6 divides the other, so 4 and 6 are not D-comparable.

Exercise 17. Let $A = \mathscr{P}(\{\,1, 2\,\})$ and let S be the relation on A defined by $x\ S\ y$ iff $x \subseteq y$. Then S is a partial order relation on A. (This is a special case of Example 17.41.) Show that S is not a total order relation on A.

Exercise 18. Let $A = \{\, 1, 2 \,\}$.

(a) List all the partial order relations on A. (The usual order relation on A is $R = \{\, (1,2) \,\} \cup E$, where $E = \{\, (1,1), (2,2) \,\}$ is the relation of equality on A, but there are other partial order relations on A. Each of them is a superset of E because a partial order relation on A is reflexive on A. Hence each of them can be written in the form $S \cup E$ for some set $S \subseteq (A \times A) \setminus E$. This can help you to save writing.)

(b) Which of the partial order relations that you found in part (a) are total order relations?

Exercise 19. Let $A = \{\, 1, 2, 3 \,\}$.

(a) List all the total order relations on A.

(b) List all the partial order relations on A that are not total order relations.

17.49 Definition. A *partially ordered set* is an ordered pair (A, R) such that A is a set and R is a partial order relation on A.

17.50 Definition. A *totally ordered set* is an ordered pair (A, R) such that A is a set and R is a total order relation on A.

17.51 Remark. Another name for a totally ordered set is a *linearly ordered set*.

17.52 Remark. It is common to use the notation $\leq$ to denote a partial order relation, even when one does not mean the usual order relation of numbers. Thus one might say "Let $(A, \leq)$ be a partially ordered set," without meaning that A is a set of numbers or that $\leq$ is the usual order relation of numbers. Of course, when the notation $\leq$ is used in this way, you must determine from the context what is meant by $\leq$ and you must not let the familiar properties of order for numbers trick you into making unjustified assumptions that may not hold for a general partial order relation. For example, a general partial order relation need not be a total order relation.

17.53 Remark. When the notation $\leq$ is used to denote a partial order relation, the notation $<$ is also commonly used to denote the relation defined by $x < y$ iff $x \leq y$ and $x \neq y$.

The next two definitions and the exercise based on them may be omitted without significant loss of continuity.

17.54 Definition. Let S be a relation. To say that S *is antireflexive* means that for each x, it is not the case that $x \, S \, x$.

17.55 Definition. To say that S *is a strict partial order relation* means that S is a relation and S is transitive and antireflexive.

Exercise 20. Let A be a set. Show that there is a natural one-to-one correspondence between partial order relations on A and strict partial order relations on A. More specifically:

(a) Let $\leq$ be a partial order relation on A and let $<$ be the relation on A defined by $x < y$ iff $x \leq y$ and $x \neq y$. Show that $<$ is a strict partial order relation on A and that for all $x, y \in A$, we have $x \leq y$ iff $x < y$ or $x = y$. (By the way, the relation $<$ is called *the strict partial order relation corresponding to the partial order relation* $\leq$.)

(b) Let $<$ be a strict partial relation on A and let $\leq$ be the relation on A defined by $x \leq y$ iff $x < y$ or $x = y$. Show that $\leq$ is a partial order relation on A and that for all $x, y \in A$, we have $x < y$ iff $x \leq y$ and $x \neq y$.

17.56 Definition. Let $(A, \leq)$ be a partially ordered set and let B be a subset of A. To say that c *is a least element of* B means that $c \in B$ and for each $x \in B$, $c \leq x$.

Exercise 21. Let $(A, \leq)$ be a partially ordered set and let B be a subset of A. Formulate a definition for d *is a greatest element of* B.

17.57 Example. Consider the totally ordered set $(\mathbf{R}, \leq)$, where $\leq$ is the usual order relation on the set $\mathbf{R}$ of real numbers. Let $B = [0, 1)$. Then 0 is a least element of B but B has no greatest element.

Exercise 22. Let $(\mathbf{R}, \leq)$ and B be as in Example 17.57. Prove the assertion that B has no greatest element.

17.58 Proposition. *Let $(A, \leq)$ be a partially ordered set and let B be a subset of A. Then:*

(a) *B has at most one least element.*

(b) *B has at most one greatest element.*

Proof. We shall leave the proof of (b) as an exercise. Let us prove (a). Let c_1 and c_2 be least elements of B. We wish to show that $c_1 = c_2$. For $i = 1, 2$, we have $c_i \in B$ and for each $x \in B$, $c_i \leq x$. Hence $c_1 \leq c_2$, because $c_2 \in B$ and for each $x \in B$, $c_1 \leq x$. Similarly, $c_2 \leq c_1$, because $c_1 \in B$ and for each $x \in B$, $c_2 \leq x$. Since $c_1 \leq c_2$ and $c_2 \leq c_1$, we have $c_1 = c_2$ because $\leq$ is antisymmetric. ■

Exercise 23. Prove Proposition 17.58(b).

17.59 Remark. Proposition 17.58 gives the right to speak of *the* least element of a set, and *the* greatest element of a set, whenever these exist.

17.60 Remark. A least element is also called a *minimum*. A greatest element is also called a *maximum*. Let $(A, \leq)$ be a partially ordered set and let B be a subset of A. If B has a least element, then it has only one, by Proposition 17.58(a), and we write $\min B$ for the least element, or minimum, of B. If B has a greatest element, then it has only one, by Proposition 17.58(b), and we write $\max B$ for the greatest element, or maximum, of B.

Exercise 24. Let R be as in Example 17.40 and let D be as in Example 17.43. As we know, R and D are two different partial order relations on $\boldsymbol{\omega}$. Accordingly, we shall write *R-least* to mean least with respect to the order relation R, *D-least* to mean least with respect to the order relation D, and so on.

(a) Does $\boldsymbol{\omega}$ have an R-least element? If so, what is it? Does $\boldsymbol{\omega}$ have an R-greatest element?

(b) Does $\boldsymbol{\omega}$ have a D-least element? If so, what is it? Does $\boldsymbol{\omega}$ have a D-greatest element? If so, what is it?

Exercise 25. Let C be a set and let $A = \mathscr{P}(C)$, the set of all subsets of C. Let S be the relation on A defined by $x \, S \, y$ iff $x \subseteq y$. Then, as was pointed out in Example 17.41, S is a partial order relation on A.

(a) Find the S-least and the S-greatest element of A.

(b) Let $B = \{\, x \in A : x \neq \emptyset \,\}$. Suppose C has two or more elements. Show that B has no S-least element.

Exercise 26. Let $(A, \leq)$ be a totally ordered set.

(a) Prove that each finite nonempty subset of A has a greatest element. (Hint: Prove by induction that for each $n \in \mathbf{N}$, for each subset $B \subseteq A$, if B has n elements, then B has a greatest element.) Similarly, each finite nonempty subset of A has a least element.

(b) Prove that for each $n \in \mathbf{N}$, for each subset $B \subseteq A$, if B has n elements, then B may be written as $B = \{\, b_1, \ldots, b_n \,\}$ where $b_1 < \cdots < b_n$.

Exercise 27. Let $(A, \leq)$ be a partially ordered set. Prove that if each finite nonempty subset of A has a greatest element, then $(A, \leq)$ is totally ordered.

17.61 Definition. Let $(A, \leq)$ be a partially ordered set and let B be a subset of A. To say that *ℓ is a lower bound for B in A* means that $\ell \in A$ and for each $x \in B$, $\ell \leq x$.

Exercise 28. Let $(A, \leq)$ be a partially ordered set and let B be a subset of A. Formulate a definition for *u is an upper bound for B in A*.

Exercise 29. Compare and contrast the notions of *least element* and *lower bound*. Do the same for the notions of *greatest element* and *upper bound*.

17.62 Definition. Let $(A, \leq)$ be a partially ordered set and let B be a subset of A. To say that *ℓ_0 is a greatest lower bound for B in A* means that ℓ_0 is a lower bound for B in A and for each lower bound ℓ for B in A, we have $\ell \leq \ell_0$.

Exercise 30. Let $(A, \leq)$ be a partially ordered set and let B be a subset of A. Formulate a definition for *u_0 is a least upper bound for B in A*.

17.63 Proposition. *Let $(A, \leq)$ be a partially ordered set and let B be a subset of A. Then:*

(a) *There is at most one greatest lower bound for B in A.*

(b) *There is at most one least upper bound for B in A.*

Proof. Let $L = \{\, \ell \in A : \ell \text{ is a lower bound for} B \text{ in } A \,\}$, the set of lower bounds for B in A. It is clear that a greatest lower bound for B in A is the same thing as a greatest element of L. By Proposition 17.58(b), L has at most one greatest element, so there is at most one greatest lower bound for B in A. Similarly, there is at most one least upper bound for B in A, because the set of upper bounds for B in A has at most one least element. ■

17.64 Remark. A greatest lower bound is also called an *infimum*. A least upper bound is also called a *supremum*. Let $(A, \leq)$ be a partially ordered set and let B be a subset of A. If B has a greatest lower bound in A, then it has only one, by Proposition 17.63(a), and we write $\inf B$ for the greatest lower bound, or infimum, of B in A. If B has a least upper bound in A, then it has only one, by Proposition 17.63(b), and we write $\sup B$ for the least upper bound, or supremum, of B in A.

17.65 Example. Consider the totally ordered set $(\mathbf{R}, \leq)$, where $\leq$ is the usual order relation on the set $\mathbf{R}$ of real numbers. Let $B = [0, 1)$. Then $0 = \min B = \inf B$ and $1 = \sup B$, but $\max B$ is undefined since B has no greatest element, or maximum.

Exercise 31. Let $(A, \leq)$ be a partially ordered set and let B be a subset of A.

(a) Show that if c is a least element of B, then c is a greatest lower bound for B in A.

(b) Show that if d is a greatest element of B, then d is a least upper bound for B in A.

(c) A greatest lower bound for B in A need not be a least element of B, because it need not belong to B. Show that if ℓ_0 is a greatest lower bound for B in A and $\ell_0 \in B$, then ℓ_0 is the least element of B.

(d) A least upper bound for B in A need not be a greatest element of B, because it need not belong to B. Show that if u_0 is a least upper bound for B in A and $u_0 \in B$, then u_0 is the greatest element of B.

17.66 Definition. A *lattice* is a partially ordered set $(A, \leq)$ such that for all $x, y \in A$, the set $\{\, x, y \,\}$ has a greatest lower bound and a least upper bound in A.

17.67 Example. Let $(A, \leq)$ be a totally ordered set. Then $(A, \leq)$ is a lattice. To see this, consider any $x, y \in A$. Then either $x \leq y$ or $y \leq x$, because $\leq$ is a total order relation. If $x \leq y$, then x is the least element of $\{\, x, y \,\}$ and y is the greatest element of $\{\, x, y \,\}$, so x is the greatest lower bound for $\{\, x, y \,\}$ and y is the least upper bound for $\{\, x, y \,\}$. Similarly, if $y \leq x$, then y is the greatest lower bound for $\{\, x, y \,\}$ and x is the least upper bound for $\{\, x, y \,\}$.

17.68 Example. A lattice need not be a totally ordered set. Consider the partially ordered set $(\boldsymbol{\omega}, D)$ where D is the relation on $\boldsymbol{\omega}$ defined by $x \, D \, y$ iff x divides y. Then $(\boldsymbol{\omega}, D)$ is a lattice. For all $x, y \in \boldsymbol{\omega}$, $\inf\{\, x, y \,\}$ is the highest common factor of x and y and $\sup\{\, x, y \,\}$ is the lowest common multiple of x and y. For instance, $\inf\{\, 4, 6 \,\} = 2$ and $\sup\{\, 4, 6 \,\} = 12$. However, as we pointed out in Example 17.48, D is not a total order relation.

17.69 Remark. Let $(A, \leq)$ be a lattice and let $x, y \in A$. Then it is common to write $x \wedge y$ for $\inf\{\, x, y \,\}$ and $x \vee y$ for $\sup\{\, x, y \,\}$. (Earlier, we used $\wedge$ and $\vee$ to mean "and" and "or." Here we have a different use of this notation, but one that is somewhat related to our earlier use of it, as the next exercise shows.)

Exercise 32. Let C be a set and let $A = \mathscr{P}(C)$, the set of all subsets of C. Let S be the relation on A defined by $x \, S \, y$ iff $x \subseteq y$. Then, as was pointed out in Example 17.41, S is a partial order relation on A. Show that in fact, the partially ordered set (A, S) is a lattice. More specifically, show that for all $x, y \in A$, $x \wedge y = x \cap y$ and $x \vee y = x \cup y$.

17.70 Definition. A *complete lattice* is a partially ordered set $(A, \leq)$ such that each subset of A has a greatest lower bound and a least upper bound in A.

Exercise 33. Let C be a set and let $A = \mathscr{P}(C)$, the set of all subsets of C. Let S be the relation on A defined by $x\ S\ y$ iff $x \subseteq y$. Then, as was pointed out in Exercise 32, the partially ordered set (A, S) is a lattice. Show that in fact, (A, S) is a complete lattice. More specifically, show that if B is a nonempty subset of A, then $\inf B = \cap B$ and $\sup B = \cup B$.

17.71 Proposition. *Let $(A, \leq)$ be a complete lattice. Then A has a least element and a greatest element. In particular, A is not empty.*

Proof. Since $\emptyset \subseteq A$, $\emptyset$ has a least upper bound and a greatest lower bound in A. But every element of A is an upper bound for $\emptyset$ in A, so the least upper bound for $\emptyset$ in A is the least element of A. Similarly, the greatest lower bound for $\emptyset$ in A is the greatest element of A. ■

Exercise 34. Let $(A, \leq)$ be a partially ordered set such that each subset of A has a greatest lower bound in A. Show that $(A, \leq)$ is a complete lattice. (Hint: Let $B \subseteq A$. To show that B has a least upper bound in A, consider the greatest lower bound of the set of upper bounds of B.)

17.72 Definition. A *conditionally complete lattice* is a partially ordered set $(A, \leq)$ such that each nonempty subset of A which has a lower bound in A has a greatest lower bound in A and each nonempty subset of A which has an upper bound in A has a least upper bound in A.

17.73 Example. Consider the totally ordered set $(\mathbf{R}, \leq)$, where $\leq$ is the usual order relation on the set $\mathbf{R}$ of real numbers. Then $(\mathbf{R}, \leq)$ is a conditionally complete lattice. This is known as *the completeness property of* $\mathbf{R}$. We shall have more to say about this important property later.

17.74 Example. Consider the totally ordered set $(\mathbf{Q}, \leq)$, where $\leq$ is the usual order relation on the set $\mathbf{Q}$ of rational numbers. Then $(\mathbf{Q}, \leq)$ is not a conditionally complete lattice. For instance, the set $B = \{\, x \in \mathbf{Q} : x^2 < 2 \,\}$ is nonempty and bounded above in $\mathbf{Q}$, but has no least upper bound in $\mathbf{Q}$. The reason for this, essentially, is that $\sqrt{2}$ is not a rational number.

Exercise 35. Let $(A, \leq)$ be a partially ordered set such that each nonempty subset of A which has an upper bound in A has a least upper bound in A. Show that $(A, \leq)$ is a conditionally complete lattice. (Hint: This is similar to Exercise 34.)

Section 18. Well-Ordered Sets and The Magic Words "And So On"

18.1 Definition. Let X be a set. To say that R *is a well-ordering of* X means that R is a partial order relation on X such that each nonempty subset of X has a least element with respect to R.

18.2 Definition. A *well-ordered set* is an ordered pair (X, R) such that X is a set and R is a well-ordering of X.

18.3 Example. Let $\leq$ be the usual order relation on the set $\boldsymbol{\omega}$ of whole numbers. Then $\leq$ is a well-ordering of $\boldsymbol{\omega}$. (This fact is equivalent to the principle of mathematical induction. See Exercise 4 in Section 7 and the remark that follows it.) Now let R be the order relation on $\boldsymbol{\omega}$ that is suggested by the following list:

$$0, 2, 4, \ldots, 1, 3, 5, \ldots$$

More precisely, let R be the relation on $\boldsymbol{\omega}$ defined by $x\,R\,y$ iff either x and y are both even and $x \leq y$, or x and y are both odd and $x \leq y$, or x is even and y is odd. Then R is also a well-ordering of $\boldsymbol{\omega}$. However, the well-orderings $\leq$ and R are essentially different. For instance, under the ordering $\leq$, each element of $\boldsymbol{\omega}$ which has predecessors has a largest predecessor. However, under the ordering R, there is an element of $\boldsymbol{\omega}$, namely 1, which has predecessors but has no largest predecessor.

18.4 Remark. Let $(X, \leq)$ be a well-ordered set. Then $\leq$ is a total order relation on X.

Proof. Let $x, y \in X$. We wish to show that either $x \leq y$ or $y \leq x$. Now since $\leq$ is a well-ordering, the set $\{\, x, y \,\}$ has a least element. If this least element is x, then $x \leq y$. If this least element is y, then $y \leq x$. ■

18.5 Example. Let $\leq$ be the usual order relation on the set $\mathbf{Z}$ of integers. Then $\leq$ is not a well-ordering of $\mathbf{Z}$. For instance, the set $\mathbf{Z}$ itself has no least element. However, $\leq$ is a total order relation on $\mathbf{Z}$. Thus, although every well-ordering is a total order relation, not every total order relation is a well-ordering.

The main reason why well-orderings are important is that a well-ordering of a set may be viewed as describing a way of counting the elements of the set one after another, even if the set is infinite.[28] We now turn to a partial explanation of this.

Let X be a set and let $\leq$ be a well-ordering of X. If we think of $\leq$ as describing a way of counting the elements of X one after another, then for all $x, y \in X$, we may think of the assertion $x \leq y$ as expressing the idea that the element x was counted before the element y was. Let $\mathscr{M}$ be the set of nonempty subsets of X. For each $A \in \mathscr{M}$, let $f(A)$ be the least element of A (with respect to $\leq$). Then f is a choice function for $\mathscr{M}$. If we think of $\leq$ as describing a way of counting the elements the X one after another, then $f(X)$ is the first element of X, $f(X \setminus \{ f(X) \})$ is the second element of X, and so on. In general, for each nonempty set $A \subseteq X$, $f(A)$ is the element of A that was counted first. Notice that the choice function f has the following property:

$$\text{For all } A, B \in \mathscr{M}, \text{ if } A \subseteq B \text{ and } f(B) \in A, \text{ then } f(B) = f(A) \tag{1}$$

or in other words, if the first element of B that was counted happens to belong to the smaller set A, then this element is also the first element of A that was counted. We started with the well-ordering $\leq$ and from it we got the choice function f. However, if we start with a choice function f having the property (1), then it arises in this way from a unique well-ordering. This is the content of the next exercise.

Exercise 1. Let X be a set, let $\mathscr{M}$ be the set of nonempty subsets of X, and let f be a choice function for $\mathscr{M}$ having the property (1) above. Show that there is a unique well-ordering $\leq$ of X such that for each $A \in \mathscr{M}$, $f(A)$ is the least element of A with respect to $\leq$. (Hint: Uniqueness is easy. To prove existence, define a relation $\leq$ on X by $x \leq y$ iff $x = f(\{ x, y \})$ and show that $\leq$ is such a well-ordering of X.)

An Intuitive Approach to Well-Ordering a Set.

Let X be a set. If X is nonempty, choose $a_0 \in X$. If $\{ a_0 \}$ is a proper subset of X, choose $a_1 \in X \setminus \{ a_0 \}$. If $\{ a_0, a_1 \}$ is a proper subset of X, choose $a_2 \in X \setminus \{ a_0, a_1 \}$. And so on. If by this procedure we succeed in choosing distinct elements $a_n \in X$ for each $n \in \boldsymbol{\omega}$, and if $\{ a_0, a_1, a_2, \dots \}$ is a proper subset of X, then we might elect to continue as follows. Choose $a_{\boldsymbol{\omega}} \in X \setminus \{ a_0, a_1, a_2, \dots \}$. Next, if $\{ a_0, a_1, a_2, \dots, a_{\boldsymbol{\omega}} \}$ is a proper subset of X, choose $a_{\boldsymbol{\omega}+1} \in X \setminus \{ a_0, a_1, a_2, \dots, a_{\boldsymbol{\omega}} \}$. If $\{ a_0, a_1, a_2, \dots, a_{\boldsymbol{\omega}}, a_{\boldsymbol{\omega}+1} \}$ is a proper subset of X, choose $a_{\boldsymbol{\omega}+2} \in X \setminus \{ a_0, a_1, a_2, \dots, a_{\boldsymbol{\omega}}, a_{\boldsymbol{\omega}+1} \}$. And so on. Continuing in this way, selecting new elements of X one by one, then gathering together the elements we have chosen, then resuming to select new elements of X one by one, and so on ad infinitum, one might imagine that we would eventually use up all the elements of X, and that this would give a well-ordering of X. Cantor believed this to be the case and said so in a letter to Dedekind dated August 3, 1899. But the crux of the matter is to give a precise meaning to the words "and so on."

Rigorous Proof that Every Set Can Be Well-Ordered.

Zermelo (1904) gave the first fully satisfactory proof that any set can be well-ordered. In 1908, Zermelo published a second proof of this well-ordering theorem. We shall now present a version of the latter proof, in a form that will be useful to prove a number of other important results.

First, let us reformulate the intuitive idea above in slightly different notation. Let f be a choice function for the set of all nonempty subsets of our set X. Thus for each $S \subseteq X$, if $S \neq \emptyset$, then $f(S) \in S$. The axiom of choice guarantees the existence of such a choice function. Define $\varphi\colon \mathscr{P}(X) \to \mathscr{P}(X)$ by

$$\varphi(A) = \begin{cases} A \cup \{ f(X \setminus A) \} & \text{if } A \text{ is a proper subset of } X, \\ X & \text{if } A = X, \end{cases}$$

for all $A \subseteq X$. Then the sets $\{ a_0 \}$, $\{ a_0, a_1 \}$, $\{ a_0, a_1, a_2 \}$, and so on, that we described before, may be written respectively as $A_1 = \varphi(\emptyset)$, $A_2 = \varphi(A_1)$, $A_3 = \varphi(A_2)$, and so on, where $a_0 = f(X)$, $a_1 = f(X \setminus \{ a_0 \})$, $a_2 = f(X \setminus \{ a_0, a_1 \})$, and so on, as long as the choice function f is being applied to a

[28] The two well-orderings of the infinite set $\boldsymbol{\omega}$ that are mentioned in Example 18.3 illustrate two essentially different ways of counting the elements of $\boldsymbol{\omega}$ one after another. And it is easy to imagine many other ways.

nonempty set. For completeness, it is also natural to define A_0 to be $\emptyset$. If X has n elements, where $n \in \boldsymbol{\omega}$, then $A_0, A_1, \ldots, A_n$ are all distinct but $A_n = A_{n+1} = A_{n+2} = \cdots = X$. If X is infinite, then the sets $A_0, A_1, A_2, \ldots$ are all distinct and we may elect to form their union, which we shall denote by $A_{\boldsymbol{\omega}}$. Then we may form $A_{\boldsymbol{\omega}+1} = \varphi(A_{\boldsymbol{\omega}})$, $A_{\boldsymbol{\omega}+2} = \varphi(A_{\boldsymbol{\omega}} + 1)$, and so on. So far, all we have done is change the notation and point out explicitly the use of the axiom of choice. We have not begun to make precise what is meant by the words "and so on." To make this precise, we first need some definitions.

18.6 Definition. Let $\mathscr{C}$ be a set of sets. To say that $\mathscr{C}$ *is a chain* means that $\mathscr{C}$ is totally ordered by set inclusion, or in other words that for all $A, B \in \mathscr{C}$, we have $A \subseteq B$ or $B \subseteq A$.

18.7 Definition. Let $\mathscr{H}$ be a set of sets and let $\varphi\colon \mathscr{H} \to \mathscr{H}$ such that for each $A \in \mathscr{H}$, we have $A \subseteq \varphi(A)$. To say that $\mathscr{G}$ *is a φ-tower* will mean that

(a) $\mathscr{G} \subseteq \mathscr{H}$;
(b) $\emptyset \in \mathscr{G}$;
(c) for each $A \in \mathscr{G}$, we have $\varphi(A) \in \mathscr{G}$;
(d) for each chain $\mathscr{C} \subseteq \mathscr{G}$, we have $\bigcup \mathscr{C} \in \mathscr{G}$.

18.8 The "And So On" Theorem. *Let $\mathscr{H}$ be a set of sets and let $\varphi\colon \mathscr{H} \to \mathscr{H}$ such that for each $A \in \mathscr{H}$, we have $A \subseteq \varphi(A)$. Suppose that $\mathscr{H}$ is itself a φ-tower. Then*:

(a) *There is a smallest φ-tower $\mathscr{F} \subseteq \mathscr{H}$;*
(b) *For all $A, B \in \mathscr{F}$, if A is a proper subset of B, then $\varphi(A) \subseteq B$;*
(c) *For all $A, B \in \mathscr{F}$, either $A \subseteq B$ or $\varphi(B) \subseteq A$;*
(d) *$\mathscr{F}$ is a chain;*
(e) *$\mathscr{F}$ is closed under arbitrary unions;*
(f) *$\mathscr{F}$ has a largest element, namely $X = \bigcup \mathscr{F}$;*
(g) *For each $B \in \mathscr{F}$, either B is a proper subset of $\varphi(B)$ or $B = X$.*
(h) *$\mathscr{F}$ is well-ordered by set inclusion.*

Proof. (a) Let $\mathscr{F} = \{\, A \in \mathscr{H} : A \in \mathscr{G} \text{ for each } \varphi\text{-tower } \mathscr{G} \,\}$. Obviously $\mathscr{F} \subseteq \mathscr{H}$ and for each φ-tower $\mathscr{G} \subseteq \mathscr{H}$, $\mathscr{F} \subseteq \mathscr{G}$. Thus to complete the proof of (a), it suffices to show that $\mathscr{F}$ is a φ-tower. We have $\emptyset \in \mathscr{F}$, because $\emptyset \in \mathscr{H}$ (since $\mathscr{H}$ is a φ-tower) and because $\emptyset \in \mathscr{G}$ for each φ-tower $\mathscr{G}$. Let $A \in \mathscr{F}$. Then $A \in \mathscr{H}$, so $\varphi(A) \in \mathscr{H}$. Let $\mathscr{G}$ be a φ-tower. Then $A \in \mathscr{G}$. Hence $\varphi(A) \in \mathscr{G}$. This holds for each φ-tower $\mathscr{G}$. Thus $\varphi(A) \in \mathscr{F}$. Finally, let $\mathscr{C} \subseteq \mathscr{F}$ such that $\mathscr{C}$ is a chain. Then $\mathscr{C} \subseteq \mathscr{H}$, so $\bigcup \mathscr{C} \in \mathscr{H}$, since $\mathscr{H}$ is a φ-tower. Let $\mathscr{G}$ be a φ-tower. Then $\mathscr{F} \subseteq \mathscr{G}$, so $\mathscr{C} \subseteq \mathscr{G}$. Hence $\bigcup \mathscr{C} \in \mathscr{G}$. This holds for each φ-tower $\mathscr{G}$. Thus $\bigcup \mathscr{C} \in \mathscr{F}$. Therefore $\mathscr{F}$ is a φ-tower, as desired.

(b) Let

$$\mathscr{B} = \{\, B \in \mathscr{F} : \text{for each } A \in \mathscr{F}, \text{ if } A \text{ is a proper subset of } B, \text{ then } \varphi(A) \subseteq B \,\}$$

and for each $B \in \mathscr{F}$, let

$$\mathscr{A}_B = \{\, A \in \mathscr{F} : A \subseteq B \text{ or } \varphi(B) \subseteq A \,\}.$$

Let $B \in \mathscr{B}$. We claim that $\mathscr{A}_B = \mathscr{F}$. By (a), it suffices to show that $\mathscr{A}_B$ is a φ-tower. Of course $\mathscr{A}_B \subseteq \mathscr{F}$ and, since $\emptyset \subseteq B$, $\emptyset \in \mathscr{A}_B$. Let $A \in \mathscr{A}_B$ and let us show that $\varphi(A) \in \mathscr{A}_B$. Since $B \in \mathscr{B}$, if A is a proper subset of B, then $\varphi(A) \subseteq B$. Since $A \in \mathscr{A}_B$, either $A \subseteq B$ or $\varphi(B) \subseteq A$. If $A \subseteq B$, then either A is a proper subset of B or $A = B$. If A is a proper subset of B, then $\varphi(A) \subseteq B$, because $B \in \mathscr{B}$, so $\varphi(A) \in \mathscr{A}_B$. If $A = B$, then $\varphi(A) = \varphi(B)$, so $\varphi(B) \subseteq \varphi(A)$, so $\varphi(A) \in \mathscr{A}_B$. If $\varphi(B) \subseteq A$, then $\varphi(B) \subseteq \varphi(A)$, so $\varphi(A) \in \mathscr{A}_B$. Thus in any case, $\varphi(A) \in \mathscr{A}_B$. This holds for each $A \in \mathscr{A}_B$. Now consider any chain $\mathscr{C} \subseteq \mathscr{A}_B$ and let us show that $\bigcup \mathscr{C} \in \mathscr{A}_B$. Now either $A \subseteq B$ for each $A \in \mathscr{C}$, in which case $\bigcup \mathscr{C} \subseteq B$, or there exists $A \in \mathscr{C}$ such that $A \not\subseteq B$, in which case, since $A \in \mathscr{A}_B$, we have $\varphi(B) \subseteq A$, so since $A \subseteq \bigcup \mathscr{C}$, we have $\varphi(B) \subseteq \bigcup \mathscr{C}$. Thus $\bigcup \mathscr{C} \subseteq B$ or $\varphi(B) \subseteq \bigcup \mathscr{C}$. Hence $\bigcup \mathscr{C} \in \mathscr{A}_B$. This holds for each chain $\mathscr{C} \subseteq \mathscr{A}_B$. This completes the proof that $\mathscr{A}_B$ is a φ-tower, so $\mathscr{A}_B = \mathscr{F}$, as claimed.

Next, we claim that $\mathscr{B} = \mathscr{F}$. By (a), it suffices to show that $\mathscr{B}$ is a φ-tower. Of course $\mathscr{B} \subseteq \mathscr{H}$. Now $\emptyset \in \mathscr{B}$, because $\emptyset \in \mathscr{F}$ and for each $A \in \mathscr{F}$, the conditional sentence "if A is a proper subset of $\emptyset$, then $\varphi(A) \subseteq \emptyset$" is true, because the antecedent in it, namely the statement "A is a proper subset of $\emptyset$," is false. Let $B \in \mathscr{B}$ and let us show that $\varphi(B) \in \mathscr{B}$. Since $B \in \mathscr{B}$, we have $\mathscr{A}_B = \mathscr{F}$, by the previous claim. Let

$A \in \mathscr{F}$. Then $A \in \mathscr{A}_B$. Suppose A is a proper subset of $\varphi(B)$. We wish to show that $\varphi(A) \subseteq \varphi(B)$. Since $B \in \mathscr{B}$, if A is a proper subset of B, then $\varphi(A) \subseteq B$. Since $B \in \mathscr{B}$ and $A \in \mathscr{A}_B$, we have $A \subseteq B$ or $\varphi(B) \subseteq A$. But we are assuming that A is a proper subset of $\varphi(B)$, so it is not the case that $\varphi(B) \subseteq A$. Thus we have $A \subseteq B$, so either A is a proper subset of B or $A = B$. If A is a proper subset of B, then since $B \in \mathscr{B}$, we have $\varphi(A) \subseteq B$, so since $B \subseteq \varphi(B)$, we have $\varphi(A) \subseteq \varphi(B)$. If $A = B$, then $\varphi(A) = \varphi(B)$, so $\varphi(A) \subseteq \varphi(B)$. Thus in any case, $\varphi(A) \subseteq \varphi(B)$. This holds for each $A \in \mathscr{F}$ such that A is a proper subset of $\varphi(B)$. It follows that $\varphi(B) \in \mathscr{B}$, as desired. Now consider any chain $\mathscr{C} \subseteq \mathscr{B}$ and let us show that $\bigcup \mathscr{C} \in \mathscr{B}$. Let $A \in \mathscr{F}$. Suppose A is a proper subset of $\bigcup \mathscr{C}$. Then $\bigcup \mathscr{C} \not\subseteq A$, so there exists $B \in \mathscr{C}$ such that $B \not\subseteq A$. Since $B \in \mathscr{B}$, we have $\mathscr{A}_B = \mathscr{F}$ by the previous claim, so $A \in \mathscr{A}_B$, so $A \subseteq B$ or $\varphi(B) \subseteq A$. But $B \subseteq \varphi(B)$ and $B \not\subseteq A$, so $\varphi(B) \not\subseteq A$. Hence $A \subseteq B$, so since $B \not\subseteq A$, A is a proper subset of B, so since $B \in \mathscr{B}$, $\varphi(A) \subseteq B$. But $B \in \mathscr{C}$, so $B \subseteq \bigcup \mathscr{C}$. Thus $\varphi(A) \subseteq \bigcup \mathscr{C}$. This holds for each $A \in \mathscr{F}$ such that A is a proper subset of $\bigcup \mathscr{C}$. It follows that $\bigcup \mathscr{C} \in \mathscr{B}$, as desired. This completes the proof that $\mathscr{B}$ is a φ-tower and establishes the claim that $\mathscr{B} = \mathscr{F}$. By the definition of $\mathscr{B}$, this proves (b).

(c) follows from (b) and the fact, established in the proof of (b), that $\mathscr{A}_B = \mathscr{F}$ for each $B \in \mathscr{B} = \mathscr{F}$.

(d) Let $A, B \in \mathscr{F}$. Then by (c), $A \subseteq B$ or $\varphi(B) \subseteq A$. But $B \subseteq \varphi(B)$. Hence $A \subseteq B$ or $B \subseteq A$. Thus $\mathscr{F}$ is a chain, which proves (d).

(e) For each $\mathscr{U} \subseteq \mathscr{F}$, since $\mathscr{F}$ is a chain, so is $\mathscr{U}$, so since $\mathscr{F}$ is a φ-tower, $\bigcup \mathscr{U} \in \mathscr{F}$.

(f) Let $X = \bigcup \mathscr{F}$. Since $\mathscr{F}$ is closed under arbitrary unions, $X \in \mathscr{F}$. Of course $A \subseteq X$ for each $A \in \mathscr{F}$. Thus X is the largest element of $\mathscr{F}$.

(g) Now let $B \in \mathscr{F}$ and let us show that either B is a proper subset of $\varphi(B)$ or $B = X$. Since $B \subseteq \varphi(B)$, it suffices to show that if $B = \varphi(B)$, then $B = X$. Suppose $B = \varphi(B)$. To show that $B = X$, it suffices to show that that for each $A \in \mathscr{F}$, we have $A \subseteq B$. Let

$$\mathscr{A} = \{\, A \in \mathscr{F} : A \subseteq B \,\}.$$

Then $\mathscr{A} \subseteq \mathscr{F}$. We wish to show that that $\mathscr{A} = \mathscr{F}$. Since $\mathscr{F}$ is the smallest φ-tower, it suffices to show that $\mathscr{A}$ is a φ-tower. Obviously $\mathscr{A} \subseteq \mathscr{H}$ and $\emptyset \in \mathscr{A}$. Let us to show that for each $A \in \mathscr{A}$, we have $\varphi(A) \in \mathscr{A}$. Let $A \in \mathscr{A}$, so that $A \in \mathscr{F}$ and $A \subseteq B$. Since $\mathscr{F}$ is a φ-tower, $\varphi(A) \in \mathscr{F}$. If $A = B$, then $\varphi(A) = \varphi(B) = B$, so $\varphi(A) \subseteq B$, so $\varphi(A) \in \mathscr{A}$. Suppose A is a proper subset of B. Then by (b), $\varphi(A) \subseteq B$, so $\varphi(A) \in \mathscr{A}$. To show that $\mathscr{A}$ is a φ-tower, it remains to show that for each chain $\mathscr{C} \subseteq \mathscr{A}$, we have $\bigcup \mathscr{C} \in \mathscr{A}$. Consider any chain $\mathscr{C} \subseteq \mathscr{A}$. Then $\bigcup \mathscr{C} \in \mathscr{F}$. Since $\mathscr{C} \subseteq \mathscr{A}$, we have $C \subseteq B$ for each $C \in \mathscr{C}$. Hence $\bigcup \mathscr{C} \subseteq B$. Thus $\bigcup \mathscr{C} \in \mathscr{A}$. This completes the proof that $\mathscr{A}$ is a φ-tower, so (g) is established.

(h) Finally, let us show that $\mathscr{F}$ is well-ordered by set-inclusion. Let $\mathscr{M}$ be a nonempty subset of $\mathscr{F}$. Let

$$\mathscr{V} = \{\, V \in \mathscr{F} : V \subseteq M \text{ for each } M \in \mathscr{M} \,\}.$$

Let $W = \bigcup \mathscr{V}$. Now $W \in \mathscr{F}$, by (e), and $W \subseteq M$ for each $M \in \mathscr{M}$. Hence $W \in \mathscr{V}$. Thus $\mathscr{V}$ has a largest element, namely W. We claim that W is the least element of $\mathscr{M}$. To show this, it suffices to show that $W \in \mathscr{M}$, because $W \subseteq M$ for each $M \in \mathscr{M}$. Suppose $W \notin \mathscr{M}$. Then for each $M \in \mathscr{M}$, W is a proper subset of M, so by (b), $\varphi(W) \subseteq M$. Hence $\varphi(W) \in \mathscr{V}$. Let $M_0 \in \mathscr{M}$. Then $M_0 \subseteq X$, so since W is a proper subset of M_0, W is a proper subset of X, so by (g), W is a proper subset of $\varphi(W)$. But then $\varphi(W)$ is an element of $\mathscr{V}$ that is larger than W, so W is not the largest element of $\mathscr{V}$. This is contradictory. Therefore W must belong to $\mathscr{M}$ after all. This completes the proof of (h). ■

18.9 Theorem. *Let $\mathscr{H}$, φ, $\mathscr{F}$, and X be as in Theorem 18.8. Suppose in addition that for each $A \in \mathscr{H}$, the set $\varphi(A) \setminus A$ has at most one element. Then*:

- **(a)** *For each $a \in X$, let $\mathscr{V}_a = \{\, V \in \mathscr{F} : a \notin V \,\}$ and let $X_a = \bigcup \mathscr{V}_a$. Then for each $a \in X$, X_a is the largest element of $\mathscr{V}_a$, $\varphi(X_a) = X_a \cup \{\, a \,\}$, and $\varphi(X_a)$ is the smallest element of $\mathscr{F} \setminus \mathscr{V}_a$.*
- **(b)** *The map $a \mapsto X_a$ is one-to-one.*
- **(c)** *Define a relation $\leq$ on X by $a \leq b$ iff $X_a \subseteq X_b$. Then $\leq$ is a well-ordering of X;*
- **(d)** *$\mathscr{F} = \{\, X_a : a \in X \,\} \cup \{\, X \,\}$.*
- **(e)** *For each $a \in X$, we have $X_a = \{\, x \in X : x < a \,\}$, where of course $x < a$ means $x \leq a$ and $x \neq a$.*

Proof. (a) Let $a \in X$. Then $X_a \in \mathscr{F}$, by Theorem 18.8(e). Now $a \notin X_a$ and for each $V \in \mathscr{V}_a$, $V \subseteq X_a$. Thus X_a is the largest element of $\mathscr{V}_a$. Since $a \notin X_a$, we have $X_a \neq X$, so by Theorem 18.8(g), X_a is a

proper subset of $\varphi(X_a)$, so $\varphi(X_a) \notin \mathscr{V}_a$, so $\varphi(X_a) \in \mathscr{F} \setminus \mathscr{V}_a$. Now $\varphi(X_a) \setminus X_a$ has at most one element. Hence $\varphi(X_a) \setminus X_a = \{ x \}$ for some x. But x must be equal to a, for otherwise we would have $a \notin \varphi(X_a)$, so that $\varphi(X_a) \in \mathscr{V}_a$, which is contradictory. Thus $\varphi(X_a) = X_a \cup \{ a \}$. For each $W \in \mathscr{F} \setminus \mathscr{V}_a$, we have $a \in W$, so $W \not\subseteq X_a$, so by Theorem 18.8(d), $X_a \subseteq W$, so $X_a \cup \{ a \} \subseteq W$, or in other words, $\varphi(X_a) \subseteq W$. Thus $\varphi(X_a)$ is the smallest element of $\mathscr{F} \setminus \mathscr{V}_a$.

(b) For all $a, b \in X$, if $X_a = X_b$, then $\{ a \} = \varphi(X_a) \setminus X_a = \varphi(X_b) \setminus X_b = \{ b \}$, so that $a = b$. Thus the map $a \mapsto X_a$ is one-to-one.

(c) For all $a, b \in X$, if $a \leq b$ and $b \leq a$, then $X_a \subseteq X_b$ and $X_b \subseteq X_a$ by the definition of $\leq$, so $X_a = X_b$, so $a = b$. Thus $\leq$ is antisymmetric. For each $a \in X$, we have $X_a \subseteq X_a$, so $a \leq a$. Hence $\leq$ is reflexive. For all $a, b, c \in X$, if $a \leq b$ and $b \leq c$, then $X_a \subseteq X_b$ and $X_b \subseteq X_c$, so $X_a \subseteq X_c$, so $a \leq c$. Thus $\leq$ is transitive. Now let T be a nonempty subset of X. Let $\mathscr{T} = \{ X_a : a \in T \}$. Then $\mathscr{T}$ is a nonempty subset of $\mathscr{F}$. By Theorem 18.8(h), $\mathscr{T}$ has a least element with respect to set inclusion. In other words, there exists $A \in \mathscr{T}$ such that for each $B \in \mathscr{T}$, we have $A \subseteq B$. Since $A \in \mathscr{T}$, we have $A = X_a$ for some $a \in T$. Let $b \in T$. Then $X_b \in \mathscr{T}$, so $X_a \subseteq X_b$, so $a \leq b$. Thus a is the least element of T with respect to $\leq$. In particular, T has a least element with respect to $\leq$. This holds for each nonempty set $T \subseteq X$. Therefore $\leq$ is a well-ordering of X. This completes the proof of (c).

(d) By (a), we have $X_a \in \mathscr{F}$ for each $a \in X$. By Theorem 18.8(f), we also have $X \in \mathscr{F}$. Thus $\{ X_a : a \in X \} \cup \{ X \} \subseteq \mathscr{F}$. Let $Y \in \mathscr{F}$. We wish to show that $Y = X_a$ for some $a \in X$ or $Y = X$. Suppose $Y \neq X$. Then Y is a proper subset of X, so by (c), $X \setminus Y$ has a least element with respect to $\leq$, say a. Now $a \notin Y$, so $Y \in \mathscr{V}_a$, so $Y \subseteq X_a$. But for each $b \in X \setminus Y$, we have $a \leq b$, so $X_a \subseteq X_b$, so $b \notin X_a$, so $b \in X \setminus X_a$. Thus $X \setminus Y \subseteq X \setminus X_a$, so $X_a \subseteq Y$. Therefore $Y = X_a$. This completes the proof of (d).

(e) Let $a \in X$ and let $A = \{ x \in X : x < a \}$. We wish to show that $X_a = A$. Let $x \in X_a$. Since $x \notin X_x$, we have $X_a \not\subseteq X_x$. Hence $a \not\leq x$, so $x < a$, since $\leq$ is a total ordering of X, so $x \in A$. Thus $X_a \subseteq A$. Conversely, let $x \in A$. Then $x < a$, so $X_x \subseteq X_a$ but $X_x \neq X_a$. Thus X_x is a proper subset of X_a. Hence, by Theorem 18.8(b), $\varphi(X_x) \subseteq X_a$. But by (b), $\varphi(X_x) = X_x \cup \{ x \}$. Hence $x \in X_a$. Thus $A \subseteq X_a$. We have shown that $X_a \subseteq A$ and $A \subseteq X_a$. Therefore $X_a = A$, as desired. ■

18.10 The Well-Ordering Theorem. (Ernst Zermelo, 1904.) *Let X be any set. Then X can be well-ordered.*

Proof. This is easy now because most of the work has already been done in the proofs of Theorem 18.8 and Theorem 18.9. Let $\mathscr{H} = \mathscr{P}(X)$. Now we use the axiom of choice. Let f be a choice function for the set of nonempty subsets of X. Define $\varphi \colon \mathscr{H} \to \mathscr{H}$ by

$$\varphi(A) = \begin{cases} A \cup \{ f(X \setminus A) \} & \text{if } A \text{ is a proper subset of } X, \\ X & \text{if } A = X, \end{cases}$$

for all $A \subseteq X$. Then for each $A \in \mathscr{H}$, we have $A \subseteq \varphi(A)$ and $\varphi(A) \setminus A$ has at most one element. Let $\mathscr{F}$ be the smallest φ-tower, as given by Theorem 18.8. By Theorem 18.8(f), $\mathscr{F}$ has a largest element, namely $\Xi = \bigcup \mathscr{F}$. Now $\Xi \subseteq \varphi(\Xi) \in \mathscr{F}$, so since Ξ is the largest element of $\mathscr{F}$, $\varphi(\Xi) = \Xi$. But then, by the definition of φ, Ξ must be equal to X. In other words, $X = \bigcup \mathscr{F}$. Hence, by Theorem 18.9(c), X can be well-ordered. ■

18.11 Remark. The proofs of Theorem 18.8 and Theorem 18.9 do not use the axiom of choice, so even if we don't assume that the axiom of choice holds in general, the proof of Theorem 18.10 shows that for each set X, if there is a choice function for the set of nonempty subsets of X, then X can be well-ordered. Conversely, if $(X, \leq)$ is a well-ordered set, then for each nonempty set $A \subseteq X$, we can let $f(A)$ be the least element of A and then f will be a choice function for the set of nonempty subsets of X. In summary, even if we don't assume the axiom of choice, we can say that for each set X, X can be well-ordered if and only if there is a choice function for the set of nonempty subsets of X.

Some Other Applications of the "And So On" Theorem.

We have already defined what it means for a set of sets to be a chain. In the next definition, we extend this concept to subsets of an arbitrary partially ordered set. We also introduce the concept of a maximal chain in a partially ordered set.

18.12 Definitions. Let $(S, \leq)$ be a partially ordered set.

(a) To say that C *is a chain in* $(S, \leq)$ means that C is a totally ordered subset of X, or in other words that $C \subseteq S$ and for all $x, y \in C$, we have $x \leq y$ or $y \leq x$.

(b) To say that C *is a maximal chain in* $(S, \leq)$ means that C is a chain in $(S, \leq)$ and for each chain C' in $(S, \leq)$, if $C \subseteq C'$, then $C = C'$.

18.13 Example. Let $(S, \leq)$ be a partially ordered set.

(a) The empty set $\emptyset$ is a chain in $(S, \leq)$.

(b) For each $x \in S$, $\{ x \}$ is a chain in $(S, \leq)$.

(c) Let $x, y \in S$. Then $\{ x, y \}$ is a chain in $(S, \leq)$ iff $x \leq y$ or $y \leq x$.

Of course these are rather trivial examples but they may help you to solve an exercise that is coming soon.

18.14 Remark. We now have two related definitions for the term "chain." Usually the context will make it clear which is meant. But if we need to be more explicit for clarity, we may use the term "chain of sets" for the kind of chain introduced in Definition 18.6. This will be important for the proof of the next result, in which we shall need to consider "chains of chains."

18.15 Hausdorff's Maximality Principle. (Felix Hausdorff, 1909, 1914.) *Let $(S, \leq)$ be a partially ordered set. Then there exists a maximal chain in $(S, \leq)$.*

Proof. Let $\mathscr{H}$ be the set of all chains in $(S, \leq)$. Define $g \colon \mathscr{H} \to \mathscr{P}(S)$ by

$$g(C) = \{ y \in S \setminus C : C \cup \{ y \} \text{ is a chain in } (S, \leq) \}.$$

Let f be a choice function for the set of nonempty subsets of S. Define φ on $\mathscr{H}$ by

$$\varphi(C) = \begin{cases} C \cup f(g(C)) & \text{if } g(C) \neq \emptyset, \\ C & \text{if } g(C) = \emptyset. \end{cases}$$

Clearly for each $C \in \mathscr{H}$, $\varphi(C)$ is a chain in $(S, \leq)$, so $\varphi(C) \in \mathscr{H}$. Thus $\varphi \colon \mathscr{H} \to \mathscr{H}$. We claim that $\mathscr{H}$ is a φ-tower. Notice that $\emptyset \in \mathscr{H}$. It is clear that for each $C \in \mathscr{H}$, $C \subseteq \varphi(C)$ and $\varphi(C) \setminus C$ has at most one element. To complete the proof of the claim, it remains to show that for each chain of sets $\mathscr{C} \subseteq \mathscr{H}$, we have $\bigcup \mathscr{C} \in \mathscr{H}$. Let $\mathscr{C} \subseteq \mathscr{H}$ such that $\mathscr{C}$ is a chain of sets. Let $x, y \in \bigcup \mathscr{C}$. Then $x \in C$ and $y \in D$ for some $C, D \in \mathscr{C}$. Since $\mathscr{C}$ is a chain of sets, either $C \subseteq D$ or $D \subseteq C$. If $C \subseteq D$, then $x, y \in D$, so since D is a chain in $(S, \leq)$, either $x \leq y$ or $y \leq x$. Similarly, if $D \subseteq C$, then $x, y \in C$, so since C is a chain in $(S, \leq)$, either $x \leq y$ or $y \leq x$. Thus in either case, $x \leq y$ or $y \leq x$. It follows that $\bigcup \mathscr{C}$ is a chain in $(S, \leq)$. This completes the proof of the claim that $\mathscr{H}$ is a φ-tower. By Theorem 18.8, there is a smallest φ-tower, say $\mathscr{F}$, and $\mathscr{F}$ is a chain. Let $C = \bigcup \mathscr{F}$. Then by the claim, C is a chain in $(S, \leq)$. We shall show that C is a maximal chain in $(S, \leq)$. Let C' be a chain in $(S, \leq)$ such that $C \subseteq C'$. We wish to show that $C = C'$, or in other words that $C' \setminus C = \emptyset$. Now $C' \setminus C \subseteq g(C)$ by the definition of $g(C)$, so it suffices to show that $g(C) = \emptyset$, or equivalently, that $\varphi(C) = C$. We have $C \subseteq \varphi(C)$ by the definition of $\varphi(C)$. But $\varphi(C) \in \mathscr{F}$, so $\varphi(C) \subseteq \bigcup \mathscr{F} = C$. Thus $\varphi(C) = C$, so we are done. ■

18.16 Remark. Of course the proof of Theorem 18.15 used the axiom of choice. As we shall see soon, Theorem 18.15 holds for each partially ordered set $(S, \leq)$ if and only if the axiom of choice holds.

18.17 Remark. In the proof of Theorem 18.15, we showed that in any partially ordered set, the union of each chain of chains is a chain. Now the union of an arbitrary collection of chains in a partially ordered set need not be a chain. If each such union is a chain, then the partially ordered set must itself be a chain, as the next exercise reveals.

Exercise 2. Let $(S, \leq)$ be a partially ordered set in which the union of each set of chains is a chain. Prove that $(S, \leq)$ is totally ordered.

18.18 Definition. Let $(S, \leq)$ be partially ordered set and let $A \subseteq S$. To say that x *is a maximal element of* A means that $x \in A$ and for each $y \in A$, if $x \leq y$, then $x = y$.

18.19 Example. Let $X = \{1, 2, 3\}$, let $S = \mathscr{P}(X)$, and let $\leq$ be the relation on S defined by $x \leq y$ iff $x \subseteq y$. As we know, $\leq$ is a partial order relation on S. Let A be the set of proper subsets of X. In other words, let $A = S \setminus \{X\}$. Let $x \in A$. When is x a maximal element in $(S, \leq)$? A moment's thought reveals that this is the case iff x has exactly two elements. Thus A has three maximal elements, namely $\{1, 2\}$, $\{1, 3\}$, and $\{2, 3\}$. But note that A has no greatest element.

18.20 Remark. Of course minimal elements can be defined analogously. (I'll leave the formulution of the definition to you.) If X and $(S, \leq)$ are as in Example 18.19 and B is the set of nonempty subsets of X, then B has no least element but B has three minimal elements, namely $\{1\}$, $\{2\}$, and $\{3\}$.

18.21 Example. Let $(S, \leq)$ be a partially ordered set. Let Γ be the set of chains in S. Since Γ is a set of sets, we may partially order Γ by set inclusion. Then a maximal chain in $(S, \leq)$ in the sense of Definition 18.12(b) is the same thing as a maximal element of Γ.

18.22 Remark. The next result is a variation on Hausdorff's maximality principle that has become the most widely used principle of this type, mainly because of its very general and flexible formulation.

18.23 Zorn's Lemma. (Max Zorn, 1935.) *Let $(S, \leq)$ be a partially ordered set in which each chain has an upper bound. Then $(S, \leq)$ has a maximal element.*

Exercise 3. Prove Theorem 18.23. (Hint: By Hausdorff's maximality principle, there exists a maximal chain in $(S, \leq)$, say C. By assumption, C has an upper bound.)

18.24 Remark. We've used the axiom of choice to prove Hausdorff's maximality principle and we've used Hausdorff's maximality principle to prove Zorn's lemma. Next you are asked to use Zorn's lemma to prove the axiom of choice. Thus Hausdorff's maximality principle and Zorn's lemma are each actually equivalent to the axiom of choice, just as Zermelo's well-ordering theorem is.

Exercise 4. Assume that Zorn's lemma holds in general. Prove that the axiom of choice holds. (Here is an outline of the proof. Let $(X_i)_{i \in I}$ be a family of nonempty sets. We wish to show that there is a choice function for this family. Let

$$\Phi = \{ f : f \text{ is a choice function for } (X_i)_{i \in J} \text{ for some } J \subseteq I \}.$$

For the purposes of this proof, let us adhere to the convention that a function f is the same thing as the set $\{(i, f(i)) : i \in \mathrm{Dom}(f)\}$ which is its graph, as we did in Section 12. Then Φ is a set of sets, so let us partially order it by set inclusion. Check that for each chain C in Φ, we have $\bigcup C \in \Phi$ and that $\bigcup C$ is an upper bound for C in Φ. Thus each chain in Φ has an upper bound. Hence, by Zorn's lemma, Φ has a maximal element, say f. Observe that then $\mathrm{Dom}(f)$ must be equal to I, for otherwise we could pick $i \in I \setminus \mathrm{Dom}(f)$ and extend f to an element g of Φ with $\mathrm{Dom}(g) = \mathrm{Dom}(f) \cup \{i\}$, contrary to the supposed maximality of f.)

18.25 Remark. Exercise 4 is a very typical application of Zorn's lemma.

Exercise 5. Deduce Zorn's lemma, Theorem 18.23, directly from Theorem 18.8, without using Hausdorff's maximality principle. (Hint: Let $(S, \leq)$ be a partially ordered set in which each chain has an upper bound. Let $\mathscr{H} = \{A \subseteq S : A \text{ is a chain in } (S, \leq)\}$. For each $A \in \mathscr{H}$, let

$$U_A = \{u \in S : x < u \text{ for each } x \in A\},$$

let f be a choice function for the set of nonempty subsets of S, define $\varphi \colon \mathscr{H} \to \mathscr{H}$ by

$$\varphi(A) = \begin{cases} A \cup f(U_A) & \text{if } U_A \neq \emptyset, \\ A & \text{if } U_A = \emptyset, \end{cases}$$

show that $\mathscr{H}$ is a φ-tower, let $\mathscr{F}$ be the smallest φ-tower (see Theorem 18.8), let $C = \bigcup \mathscr{F}$, verify that C is a chain in $(S, \leq)$, let v be an upper bound for C in $(S, \leq)$, and verify that v is a maximal element of S.)

18.26 Remark. It is not hard to see that collection $\boldsymbol{\omega}$ of all whole numbers is a set iff the axiom of infinity holds. Let us assume that it does, as is customary in set theory. Then the whole numbers are the initial part of a much larger collection of objects which are called *ordinal numbers*. The whole numbers are the finite ordinal numbers. Notice that for each whole number n, we have

$$n+1 = \{\,0,1,2,\ldots,n-1,n\,\} = \{\,0,1,2,\ldots,n-1\,\} \cup \{\,n\,\} = n \cup \{\,n\,\}.$$

The first infinite ordinal number is the set $\boldsymbol{\omega}$ itself, which is also called the first *limit ordinal*. After $\boldsymbol{\omega}$ comes $\boldsymbol{\omega}+1$, which is defined to be the set $\boldsymbol{\omega} \cup \{\,\boldsymbol{\omega}\,\}$. Then come $\boldsymbol{\omega}+2$, $\boldsymbol{\omega}+3$, and so on. After all these comes the second limit ordinal, $\boldsymbol{\omega}+\boldsymbol{\omega} = \boldsymbol{\omega}2$, which we define to be the set

$$\{\,0,1,2,3\ldots,\boldsymbol{\omega},\boldsymbol{\omega}+1,\boldsymbol{\omega}+2,\boldsymbol{\omega}+3,\ldots\,\}.$$

(We remark that $\boldsymbol{\omega}2$ is different from $2\boldsymbol{\omega}$, because $2\boldsymbol{\omega}$ is $2+2+2+\cdots$ and that is just $\boldsymbol{\omega}$.) After $\boldsymbol{\omega}2$ come $\boldsymbol{\omega}2+1$, $\boldsymbol{\omega}2+2$, $\boldsymbol{\omega}2+3,\ldots,\boldsymbol{\omega}3,\ldots,\boldsymbol{\omega}4,\ldots$. The smallest ordinal larger than all these is $\boldsymbol{\omega}^2$. (As a well-ordered set, $\boldsymbol{\omega}^2$ is isomorphic to the cartesian product $\boldsymbol{\omega}\times\boldsymbol{\omega}$ with the lexicographic order, like the ordering of words in a dictionary.) Repeating the process that we used to reach $\boldsymbol{\omega}^2$ denumerably many times brings us to $\boldsymbol{\omega}^3$ (which is isomorphic to $\boldsymbol{\omega}\times\boldsymbol{\omega}\times\boldsymbol{\omega}$ with the lexicographic order) and, repeating this again and again, we pass $\boldsymbol{\omega}^4,\ldots,\boldsymbol{\omega}^5,\ldots,\boldsymbol{\omega}^6,\ldots$. The smallest ordinal larger than all these is $\boldsymbol{\omega}^{\boldsymbol{\omega}}$. Continuing in this fashion, we pass $\boldsymbol{\omega}^{\boldsymbol{\omega}^{\boldsymbol{\omega}}},\ldots,\boldsymbol{\omega}^{\boldsymbol{\omega}^{\boldsymbol{\omega}^{\boldsymbol{\omega}}}},\ldots$. The smallest ordinal greater than all these is denoted by $\boldsymbol{\varepsilon}_0$. It is the smallest ordinal $\boldsymbol{\varepsilon}>1$ such that $\boldsymbol{\varepsilon}^{\boldsymbol{\omega}}=\boldsymbol{\varepsilon}$. And we have barely even begun to describe all the ordinal numbers that there are. Of course, we have not given a precise definition of which sets are ordinal numbers. But with the help of the "and so on" theorem, it is easy to do so. (Warning: There is no set of all ordinal numbers. The collection of all ordinal numbers is too big to be a set.) It turns out that each ordinal number is a suitable set of sets which is well-ordered by inclusion and that each well-ordered set is "isomorphic" to a unique ordinal number. (This means that each well-ordered set looks just like a unique ordinal number, in a sense which can easily be made precise.) It follows that since each set can be well-ordered, each set is equinumerous to some ordinal number. A finite set is equinumerous to only one ordinal number, which can only be the number of elements in the set. If A is an infinite set, then the cardinal number of the set, or the number of elements in the set, is the least ordinal number α such that A is equinumerous to α. For instance, $\boldsymbol{\omega}\times\boldsymbol{\omega}$ is equinumerous to $\boldsymbol{\omega}^2$ but by part of the Hilbert's hotel story, it is also equinumerous to the smaller ordinal number $\boldsymbol{\omega}$ and that is its cardinal number. With this brief sketch of further vistas in set theory, we have come to the end of this book. If you would like to learn more about what we have just sketched, you may consult more advanced textbooks on set theory, such as Keith Devlin, *Joy Of Sets: Fundamentals of Contemporary Set Theory*, second edition, Springer-Verlag, 1993.