Chapter 1

Language, Logic, and Proof

1.1. Language and logic

Like all scientific subjects, mathematics requires evidence in order to justify claims. While the lab sciences often use experimental data to justify their claims, in mathematics, logical reasoning is the standard of truth.

Mathematics is concerned with formal *statements* about mathematical objects, such as integers or functions, and whether these statements are true or false. The *language* of mathematics must therefore be precise and unambiguous—it has a vocabulary and a grammar. Logical arguments called *proofs* are used to deduce statements from basic assumptions; i.e., given a mathematical statement, we want to determine whether it is true or false and prove that our assertion is correct. For example, you may have learned in a previous course that there exist infinitely many prime numbers. Just a few definitions and proof techniques will enable us to prove this statement, which we do in Section 2.3.

The language and tools of mathematics are used by other scientists, particularly physicists and computer scientists, as well. For example, a computer scientist may wish to determine the "computational complexity" (or "hardness") of an algorithm, or even to prove that an algorithm "works" at all.

We will begin with mathematical *language*, the logical connectives and quantifiers, and then we will study the fundamental techniques of *proof.* Once armed with these tools, we are ready to study the concepts most often needed in mathematics and computer science, such as sets, functions, and relations. We then consider a variety of mathematical topics designed to prepare you for future proof-based math courses.

Definition 1.1.1. A *proposition* is a sentence (i.e., it has both a subject and a verb) which has exactly one truth value; i.e., it is either true or false, but not both.

Example 1.1.2. Consider the following examples of propositions.

(1) $2 + 3 = 6$.

Here, the verb is *equals*, which is represented notationally. (Remember we said that our mathematical language has a grammar!) Clearly this proposition is false.

(2) The 10^{46}th digit of π is 7.

At the time this book was written, the 10^{46}th digit of π was unknown. Consequently, this proposition is a bit unusual—it is certainly true or false, but not both, but which truth value it has is unknown.

(3) Every prime number is odd.

Is this proposition true or false? To answer this, you first need to know what the words *prime* and *odd* mean. (If necessary, consult Definitions 2.1.7 and 1.2.1.) ♢

We will often represent propositions with capital letters, such as P, Q, or R. Next we consider some nonexamples of propositions.

Example 1.1.3.

(1) $2 + 3$.

What is the problem here? Refer to Example 1.1.2(1).

(2) $n + 1 > 3$.

What is the problem here? It is impossible to determine a truth value. However, the situation is very different from that of Example 1.1.2(2). Here we cannot determine a truth value because the truth value depends on the value assigned to n. For example, the statement is true if $n = 4$ and false if $n = 1$. The statement "$n + 1 > 3$" *is* a sentence, though; such a statement is called a *predicate*. We can denote the predicate "$n + 1 > 3$" by the notation $P(n)$ to emphasize that n is a *free variable*, i.e., a variable that we need to "substitute for" in order to obtain a proposition.

There is another, more subtle issue, here as well. Given the predicate $P(n)$, we should really ask ourselves what we are *allowed* to substitute for n; i.e., what is the *universe*, or possible range of values, for n? So, we can see that we will either need to make the universe for a given predicate explicit or be able to deduce it from the context (here, there was no context given). ♢

So, we have two types of mathematical statements, propositions and predicates. We can build more complicated statements using *logical connectives.*

1.1.1. Basic connectives. Suppose that P and Q are statement letters (i.e., letters that represent propositions or predicates). We define the logical connectives *conjunction*, *disjunction*, and *negation* as follows.

The *conjunction* of P and Q is the statement "P and Q", which is denoted by $P \wedge Q$; the statements P and Q are called the *conjuncts* of the statement $P \wedge Q$. The intended meaning of the statement $P \wedge Q$ is clear; the statement $P \wedge Q$ will be true when P is true and Q is true, and false otherwise. We can represent this definition by the *truth table* in Table 1.1.

Note that when we build a truth table for a compound statement involving two (or more) statement letters (say, P and Q), we must consider all the possible truth values for each statement letter. Here there are two possible truth values for

Table 1.1. Truth table for $\wedge$.

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

P (true, false), and similarly for Q, so there are $2 \cdot 2$, or 4, possible truth values for the statement $P \wedge Q$. (This method of counting is called the *multiplication principle*, which we discuss in Section 8.2.)

Next, we consider disjunction. The *disjunction* of P and Q is the statement "P or Q", which is denoted by $P \vee Q$; here, the statements P and Q are called the *disjuncts* of the statement $P \vee Q$. We must decide on the intended meaning of this connective, since it can be interpreted in one of two ways.

In the English language, the word "or" is often an *exclusive* "or". For example, at a restaurant you may be asked to choose to have soup or salad with your entree. It is understood that you should choose one or the other, but not both (unless you pay extra!).

In mathematics, however, the common usage of the word "or" is in the *inclusive* sense. For example, consider the following well-known mathematical statement:

$$\text{if } a \text{ and } b \text{ are integers with } ab = 0, \text{ then } a = 0 \text{ or } b = 0.$$

Here, we know that we should interpret this statement as "if a and b are integers with $ab = 0$, then $a = 0$ *or* $b = 0$ *or* possibly *both* $a = 0$ and $b = 0$".

To repeat, *in mathematics, the usage of the word "or" is always inclusive, unless explicitly stated otherwise.* The truth table for disjunction is given in Table 1.2.

Table 1.2. Truth table for $\vee$.

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

Finally, we consider negation. The *negation* of P is the statement "not P", which is denoted by $\neg P$ and interpreted just as you suspect, in Table 1.3.

Table 1.3. Truth table for $\neg$.

P	$\neg P$
T	F
F	T

Before introducing our last two basic connectives, let's consider some examples. Just as we can make more complicated statements by forming the negation of a statement, or the conjunction or disjunction of two statements, we can form other compound statements by combining connectives.

Example 1.1.4. Determine whether the following statements are true or false.

(1) $2 + 3 = 5$ and $\neg(1 + 1 = 2)$.
Since $\neg(1 + 1 = 2)$ is false, this conjunction is false.

(2) $2 + 3 = 5$ or $\neg(1 + 1 = 2)$.
This disjunction is true since $2 + 3 = 5$ is true. ♢

Example 1.1.5. Find the truth tables for the statements

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

Before we begin, notice that we have already made an assumption about the connective $\neg$, namely, that it always modifies as little as possible, unless we explicitly indicate otherwise. Thus, we should interpret the statement $\neg P \wedge \neg Q$ as $(\neg P) \wedge (\neg Q)$. In addition, the parentheses in $\neg(P \wedge Q)$ are necessary, since $\neg P \wedge Q$ would be interpreted as $(\neg P) \wedge Q$, by our previous rule. In general, therefore, just as parentheses are used in arithmetical expressions to indicate the order in which the arithmetical operations should be evaluated, parentheses are used in compound logical statements to indicate the order in which the logical connectives should be evaluated. The requested truth tables are in Table 1.4.

Table 1.4. Truth table for $\neg(P \wedge Q)$, $\neg P \wedge \neg Q$, $\neg P \vee \neg Q$.

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

♢

We see from this example that not only does the order of connectives matter, but also the sixth and eighth columns in Table 1.4 show that the statements $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ have the same logical meaning.

Definition 1.1.6. Two statements involving the same statement letters are *logically equivalent* if they have the same truth table.

In Example 1.1.5, we see that the statements $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ are logically equivalent. On the other hand, the statements $\neg(P \wedge Q)$ and $\neg P \wedge \neg Q$ are not logically equivalent because when P is true and Q is false, $\neg(P \wedge Q)$ is true, while $\neg P \wedge \neg Q$ is false. The statement that $\neg(P \wedge Q)$ is logically equivalent to $\neg P \vee \neg Q$ is one of *DeMorgan's Laws*.

Proposition 1.1.7 (DeMorgan's Laws)**.** *Let P and Q be statements.*

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

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

Proof. We proved (1) using the truth table in Table 1.4. The proof of (2) is Exercise 1.1.2d. □

We consider two more examples before introducing our final two logical connectives.

Example 1.1.8. Assume that x is a fixed real number. What is the negation of the statement $1 < x < 2$?

We must first recall that the statement $1 < x < 2$ is an abbreviation of the compound statement

$$1 < x \text{ and } x < 2.$$

The negation of this statement is

$$\text{it is not the case that } 1 < x \text{ and } x < 2,$$

or, in notation form, $\neg[(1 < x) \wedge (x < 2)]$.

While our answer is technically correct, sometimes we find that expressing a statement "negatively", as a negation, is not useful. Often, a more useful way to express the negated statement is to express it "positively", using Proposition 1.1.7 to find a logically equivalent statement. Using DeMorgan's Laws, the negation of the statement $1 < x < 2$ is logically equivalent to the statement $\neg(1 < x) \vee \neg(x < 2)$. Simplifying further, we see that the negation of the statement $1 < x < 2$ is logically equivalent to the statement

$$x \leq 1 \text{ or } x \geq 2.$$

Here we are using what is called the *Trichotomy Axiom* of real numbers: given fixed real numbers a and b, exactly one of the statements $a < b$, $a = b$, $b < a$ is true. ◊

When we use DeMorgan's Laws to express the negation of a conjunction or disjunction "positively", we shall say that we have found a *useful denial* of that statement.

Example 1.1.9. Assume that n is a fixed positive integer. Find a useful denial of the statement

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

Using DeMorgan's Laws, we see that

$$\neg[(n = 2) \vee n \text{ is odd}]$$

is logically equivalent to

$$n \neq 2 \wedge n \text{ is even},$$

where we are using the fact that every integer is either even or odd, but not both. Thus, a useful denial of the given statement is, in natural English,

$$n \text{ is an even positive integer other than 2.}$$ ◊

We now present the final two logical connectives. As before, we let P and Q denote fixed statements.

The *implication* or *conditional* statement $P \Rightarrow Q$ is the statement "if P, then Q", or "P implies Q". The intended mathematical meaning of this connective, however, may surprise you. When should the statement $P \Rightarrow Q$ be true? Certainly the English usage of the phrase "if ..., then" conjures up the mental phrase "if P is true, then Q must also be true". However, mathematicians also consider the statement $P \Rightarrow Q$ to be true when P is false, regardless of the truth value of Q. One way to think about this is to think about when $P \Rightarrow Q$ "should" be false, namely, only when P is true and Q is false. As with the other connectives, we summarize this information in a truth table (see Table 1.5).

Table 1.5. Truth table for $\Rightarrow$.

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

In the statement $P \Rightarrow Q$, P is called the *hypothesis*, or *antecedent*, and Q is called the *conclusion* or *consequent.*

There are several other English phrases that are always interpreted to mean $P \Rightarrow Q$, or P implies Q, which are given in Table 1.6. It is important to note, therefore, that the words *if, only if, necessary, sufficient* (as well as *and* and *or*) have particular mathematical meanings, and so we must take care to use and interpret these words correctly.

Table 1.6. Alternative expressions for $P \Rightarrow Q$.

If P, then Q	Q when P
P only if Q	Q if P
P is sufficient for Q	Q is necessary for P

For our final logical connective (here, again, P and Q are fixed statements), the *biconditional* statement $P \Leftrightarrow Q$ is an abbreviation for the compound statement $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$; the truth table is given in Table 1.7.

Table 1.7. Truth table for $\Leftrightarrow$.

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

As with the conditional, there are several English phrases which can denote the biconditional (see Table 1.8). In particular, note that we interpret the $\Leftarrow$ of $P \Leftrightarrow Q$ as *if*, while we interpret the $\Rightarrow$ as *only if.*

Table 1.8. Alternative expressions for $P \Leftrightarrow Q$.

P if and only if Q
P iff Q
P is equivalent to Q
P exactly when Q
P is necessary and sufficient for Q

Example 1.1.10. Determine whether the following statements are true or false.

(1) If $7+6=14$, then $5+5=10$.

Since $7+6=14$ is false, we see that this implication is true.

(2) p is odd is necessary for p to be prime. (Here, think of p as a fixed positive integer.)

In general, we will find it easier to interpret this statement if we rephrase it as an "if ..., then" statement using Table 1.6. In this form, the statement becomes

if p is prime, then p is odd.

Note again that we are relying on knowing the definitions of "prime" and "odd" (see Definitions 2.1.7 and 1.2.1). Here we can see that the truth value of the implication will depend on which positive integer p is.

If $p=2$, then the hypothesis "p is prime" is true, but the conclusion "p is odd" is false. In this case, the implication is false.

If $p=3$, then the hypothesis "p is prime" is true and also the conclusion "p is odd" is true. In this case, the implication is true. Here we can also see that mathematical implication has nothing to do with "causality". The fact that 3 is odd is not "caused" by the fact that 3 is prime.

If $p=4$ or $p=9$, then the hypothesis "p is prime" is false. Thus, in these cases, the implication is true.

We invite you to determine exactly for which positive integers p the given statement is true.

(3) $|x|=1$ iff $x=1$ or $x=-1$. (Here, think of x as a fixed real number.)

This biconditional is a true statement. When x is a fixed real number, regardless of its value, the two statements $|x|=1$ and $(x=1)\vee(x=-1)$ have the same truth value (see Proposition 1.1.11(3) and Definition 2.1.11). ◊

We will find it useful to have more than one way of thinking of certain statements.

Proposition 1.1.11. *Let P and Q be statements.*

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

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

(3) $P \Leftrightarrow Q$ *is true exactly when P and Q have the same truth value.*

Proof. See Exercise 1.1.2e, Exercise 1.1.2f, and Table 1.7. Use truth tables. □

Proposition 1.1.11(2) indicates how to find a useful denial of an implication.

Example 1.1.12. Find a useful denial of the statement

n is prime only if $n=2$ or n is odd.

(Assume that n is a fixed positive integer.)

As before, we should first rewrite the statement as an "if ..., then" statement; i.e.,

n is prime $\Rightarrow$ ($n=2$ or n is odd).

By Proposition 1.1.11(2) and Example 1.1.9, a useful denial of the given statement is, in natural English,

n is prime, and n is an even positive integer other than 2. ♢

1.1.2. Statements related to $P \Rightarrow Q$.

We consider now two statements related to the implication $P \Rightarrow Q$.

Definition 1.1.13. Let P and Q be statements.

(1) The *converse* of $P \Rightarrow Q$ is the statement $Q \Rightarrow P$.

(2) The *contrapositive* of $P \Rightarrow Q$ is the statement $(\neg Q) \Rightarrow (\neg P)$.

We illustrate these ideas using a familiar implication from calculus.

Example 1.1.14. Let f be a fixed real-valued function defined on some collection of real numbers (i.e., the type of function one considers in calculus), and let a be a fixed real number. Consider the conditional statement

$$\text{if } f \text{ is differentiable at } a, \text{ then } f \text{ is continuous at } a. \tag{1.1}$$

The converse of this statement is

$$\text{if } f \text{ is continuous at } a, \text{ then } f \text{ is differentiable at } a. \tag{1.2}$$

The contrapositive is

$$\text{if } f \text{ is not continuous at } a, \text{ then } f \text{ is not differentiable at } a. \tag{1.3}$$ ♢

It is important to know the difference between the converse and the contrapositive of an implication, as the truth table in Table 1.9 shows.

Table 1.9. Truth table for $P \Rightarrow Q$, $Q \Rightarrow P$, $(\neg Q) \Rightarrow (\neg P)$.

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

Table 1.9 shows that the statement $P \Rightarrow Q$ and its contrapositive $(\neg Q) \Rightarrow (\neg P)$ are logically equivalent. We also see that the implication $P \Rightarrow Q$ is not logically equivalent to its converse $Q \Rightarrow P$, since when $P \Rightarrow Q$ is true, $Q \Rightarrow P$ may be true or false, depending on the truth values of P and Q. We have thus proved the following proposition.

Proposition 1.1.15. *Let P and Q be statements.*

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

(2) *$P \Rightarrow Q$ is not logically equivalent to $Q \Rightarrow P$.*

Consider Example 1.1.14 again. We learn in calculus that statement (1.1) is a true statement, regardless of which fixed function f and real number a we consider. Hence, the contrapositive statement (1.3) is also true, regardless of which fixed function f and real number a we consider. We also learn in calculus that the truth or falsity of the converse of (1.1), statement (1.2), depends on *which* fixed function f and real number a we consider. To prove that statement (1.2) does not hold *for all* functions f and *for all* real numbers a, we must demonstrate a particular function f and a particular real number a such that f is continuous at a but not differentiable at a (see Exercise 1.1.6). We discuss the quantifier "for all", and how it is negated, in Subsection 1.1.3.

1.1.3. Quantifiers.

Recall that the statement "$n+1>3$" on its own is not a *proposition* because it doesn't have a truth value. Instead, it is a *predicate* because it becomes a proposition when the "free variable" n is replaced by a particular value from the universe in question.

Let $P(n)$ denote the predicate "$n+1>3$" (the notation makes explicit the fact that n is a free variable). As an example, we'll also assume that the universe over which n can range is $\mathbb{N}=\{1,2,3,\dots\}$, the set of all natural numbers (also called the set of positive integers). Then $P(2)$ is the proposition "$2+1>3$", which is false, and $P(7)$ is the proposition "$7+1>3$", which is true.

Another way to turn a predicate into a statement with a truth value is to modify it with a *quantifier.*

Definition 1.1.16. Let $\mathcal{U}$ be the universe under consideration and $P(x)$ be a predicate whose only free variable is x. Then the statements

$$\begin{array}{rl} \text{"for all } x,\ P(x)\text{"} & \qquad \text{notation: } (\forall x)P(x), \\ \text{"there exists } x \text{ such that } P(x)\text{"} & \qquad \text{notation: } (\exists x)P(x) \end{array}$$

are statements that have truth values.

The symbol $\forall$ is called the *universal quantifier.* The statement $(\forall x)P(x)$ is true exactly when each individual element a in the universe $\mathcal{U}$ has the property that $P(a)$ true.

The symbol $\exists$ is called the *existential quantifier.* The statement $(\exists x)P(x)$ is true exactly when the universe $\mathcal{U}$ contains at least one element a with $P(a)$ true.

We can make the universe $\mathcal{U}$ explicit by writing $(\forall x\in\mathcal{U})P(x)$ instead of $(\forall x)P(x)$, and similarly by writing $(\exists x\in\mathcal{U})P(x)$ instead of $(\exists x)P(x)$. We read the notation $(\forall x\in\mathcal{U})$ as "for all x in $\mathcal{U}$" and $(\exists x\in U)$ as "there exists x in $\mathcal{U}$". The symbol $\in$ is used in order to denote an element of a set; for example, the statement $3\in\mathbb{N}$ says that 3 is a natural number, while the statement $\frac{1}{2}\notin\mathbb{N}$ says that $\frac{1}{2}$ is not a natural number. We discuss this concept in more depth in Chapter 4.

Example 1.1.17. Determine whether the following statements are true or false.

(1) There exists a natural number n such that $n+1>3$.
 The statement $(\exists n\in\mathbb{N})(n+1>3)$ is true because $7\in\mathbb{N}$ and $7+1>3$ is true.

(2) For all real numbers x, $x^2\geq 0$.
 We'll use $\mathbb{R}$ to denote the set of all real numbers. You've probably learned in a previous math course that the statement $(\forall x\in\mathbb{R})(x^2\geq 0)$ is true; i.e., the square of a real number is never negative. (See Exercise 2.1.6, which requests a proof of this statement.)

(3) For all natural numbers n, $n+1>3$.

The statement $(\forall n \in \mathbb{N})(n+1>3)$ is false because 2 is a natural number, but $2+1>3$ is false. Here, the natural number 2 is called a *counterexample* to the statement $(\forall n \in \mathbb{N})(n+1>3)$; this means that it is an example that shows that the universal statement $(\forall n \in \mathbb{N})(n+1>3)$ is false.

(4) $(\forall x \in \mathbb{R})(x^3+52x^2+79x+1000 \geq 0)$

Here we need to think a bit before proceeding. We learn in calculus that the power function x^3 "grows faster" than the power function x^2 when x is large. Thus, when x is large negative, we expect that the polynomial $x^3+52x^2+79x+1000$ should be negative; i.e., we conjecture that we should be able to find a counterexample that shows the given statement is false. If we try $x=-2$, then we compute

$$(-2)^3+52\cdot(-2)^2+79(-2)+1000=1042,$$

which tells us nothing since $1042 \geq 0$. In other words, -2 is not the counterexample we seek. However, it is important to note that *this computation does not show that the given statement is true.* We try another value of x, such as $x=-100$. We compute

$$(-100)^3+52\cdot(-100)^2+79(-100)+1000=-486900<0.$$

Thus we have successfully found a counterexample that shows that the statement $(\forall x \in \mathbb{R})(x^3+52x^2+79x+1000 \geq 0)$ is false. ♢

Note that Definition 1.1.16 states that in order to determine the truth value of a statement $(\forall x)P(x)$ or $(\exists x)P(x)$, the universe over which x can range must be known. A quick example illustrates why. The statement $(\exists x \in \mathbb{N})(2x=3)$ is false because the equation $2x=3$ has no solution in the natural numbers. However, the statement $(\exists x \in \mathbb{R})(2x=3)$ is true because $\frac{3}{2}$ is a real number and $2\cdot\frac{3}{2}=3$.

For convenience, we collect in Table 1.10 the definitions and notation for the various number universes $\mathcal{U}$ we will consider in this text, namely, the natural numbers, the integers, the rational numbers, and the real numbers. Note that in some texts, 0 is considered to be a natural number, so it is important to check the definition in whatever source you are using. Note also that because every rational number has infinitely many representations (for example, $\frac{1}{2}=\frac{3}{6}=\frac{-2}{-4}=\cdots$), our definition of $\mathbb{Q}$ is informal. Defining $\mathbb{Q}$ more carefully, including checking that the arithmetic operations are "well-defined", is often addressed in an abstract algebra course (see also Exercise 7.2.9). Similarly, our definition of what it means to be a real number is informal only. Formally defining the concept of a real number is often addressed in courses such as real analysis or set theory; see Chapter 9.

Table 1.10. Number universes.

natural numbers $\mathbb{N}$:	$\mathbb{N}=\{1,2,3,\ldots\}$
integers $\mathbb{Z}$:	$\mathbb{Z}=\{\ldots,-3,-2,-1,0,1,2,3,\ldots\}$
rational numbers $\mathbb{Q}$:	$x \in \mathbb{Q}$ if there exist a, $b \in \mathbb{Z}$, $b \neq 0$, such that $x=\frac{a}{b}$
real numbers $\mathbb{R}$:	*informally,* $x \in \mathbb{R}$ if x has a decimal expansion

Sometimes we will denote the set of positive integers by $\mathbb{Z}^+$. Similarly, $\mathbb{Q}^+$ denotes the set of positive rational numbers, etc.

Next, we need to determine how the quantifiers interact with negation. Here, the usual English usage of these phrases gives us exactly the right idea. The negation of the statement "all members of this class have brown hair" is "at least one member of this class doesn't have brown hair". Here we see that the universal quantifer (all members of this class) became an existential quantifier (at least one member of this class), and the statement "has brown hair" was negated to become "doesn't have brown hair". Similarly, the negation of the statement "there is a member of this class who is left-handed" is "every member of this class is right-handed".

Proposition 1.1.18. *Let $P(x)$ be a predicate and let $\mathcal{U}$ be the intended universe. Then:*

(1) $\neg(\forall x)P(x)$ *is logically equivalent to* $(\exists x)(\neg P(x))$*; i.e.,* $\neg(\forall x \in \mathcal{U})P(x)$ *is logically equivalent to* $(\exists x \in \mathcal{U})(\neg P(x))$.

(2) $\neg(\exists x)P(x)$ *is logically equivalent to* $(\forall x)(\neg P(x))$*; i.e.,* $\neg(\exists x \in \mathcal{U})P(x)$ *is logically equivalent to* $(\forall x \in \mathcal{U})(\neg P(x))$.

Proof. See Exercise 1.1.8. Use Definition 1.1.16. □

Proposition 1.1.18 tells us how to find a useful denial of a quantified statement.

Example 1.1.19. Find a useful denial of the statement

for all real numbers x, if $x > 2$, then $x^2 > 4$.

Remember that finding a useful denial of a statement means to express the negation of the statement positively. At first, you may find this type of exercise easier if you first express the statement using a mixture of English and mathematical notation, and then proceed one step at a time. The statement

$$\neg(\forall x \in \mathbb{R})[x > 2 \Rightarrow x^2 > 4] \qquad \text{is equivalent to}$$
$$(\exists x \in \mathbb{R})[\neg(x > 2 \Rightarrow x^2 > 4)], \qquad \text{by Proposition 1.1.18(1),}$$

which is equivalent to

$$(\exists x \in \mathbb{R})[x > 2 \wedge x^2 \leq 4] \qquad \text{by Proposition 1.1.11(2).}$$

Thus, a useful denial of the statement

for all real numbers x, if $x > 2$, then $x^2 > 4$

is

there exists a real number x such that $x > 2$ and $x^2 \leq 4$. ♢

Notice in the example above that we did not allow ourselves to be distracted by the truth or falsity of the statements.

We conclude this subsection with a final comment about statements such as $(\forall x \in \mathcal{U})P(x)$, which explicitly indicate the universe $\mathcal{U}$ under consideration. The notation $(\forall x \in \mathcal{U})$ is called a *modified quantifier*, since we have modified the universal quantifier $(\forall x)$. The notation

$$(\forall x \in \mathcal{U})P(x)$$

is actually an abbreviation for the statement

$$(\forall x)(x \in \mathcal{U} \Rightarrow P(x)).$$

Similarly, the notation

$$(\exists x \in \mathcal{U})P(x)$$

is an abbreviation for

$$(\exists x)(x \in \mathcal{U} \wedge P(x)).$$

See Exercise 1.1.8b.

Quantifiers that are modified in other ways, such as the modification seen in the statement $(\forall x > 2)(x^2 > 4)$, follow the same rules. For example,

$$(\forall x > 2)(x^2 > 4)$$

is an abbreviation for

$$(\forall x)(x > 2 \Rightarrow x^2 > 4),$$

and

$$(\exists x < 2)(x^2 > 4)$$

is an abbreviation for

$$(\exists x)(x < 2 \wedge x^2 > 4).$$

1.1.4. A warning: hidden and implied quantifiers. From the beginning of this chapter, we have emphasized the language of mathematics. In order for us to understand and be understood, we must use that language (including its notation) precisely to say exactly what we mean, no more and no less. However, there are several situations in mathematical practice where the mathematical language may imply more than it says explicitly.

One important example of this is illustrated by the following statement. The universe here is the set $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ of integers.

(1.4) If n is odd, then $n + 1$ is even.

We have emphasized already that this statement is not a proposition (i.e., it doesn't have a truth value) but rather a predicate. However, the custom in mathematics is to treat an isolated implication such as this one as a *universal* statement, even though the universal quantifier $\forall$ is not explicitly mentioned. This is because n is to be treated as a fixed, but *arbitrary*, integer. Thus, the statement "if n is odd, then $n + 1$ is even" is often interpreted as

$$(\forall n \in \mathbb{Z})[\text{if } n \text{ is odd, then } n + 1 \text{ is even}]. \tag{1.5}$$

Recognizing the hidden quantifiers is also important when one needs to negate a statement. If an author had intended for statement (1.4) to be interpreted as statement (1.5) (and one should be able to tell this from the context), then one needs to make the quantifiers explicit first in order to find the correct negation:

$$(\exists n \in \mathbb{Z})[n \text{ and } n + 1 \text{ are both odd}].$$

Again, do not be distracted by the truth or falsity of these statements.

So, to repeat, *an implication involving one or more free variables is often treated as a universally quantified statement.*

In addition, quantifiers may "hide" in other ways, such as in the definition of mathematical terms like "even". For example, the statement that "12 is an even integer" means that 12 is divisible by 2, which itself means that there is an integer k such that $2k = 12$ (here, $k = 6$). The phrase "12 is even" *hides* an existential quantifier, which is important to recognize.

Another example of hidden quantifiers occurs in the statement that "$\sqrt{2}$ is irrational", i.e., that "$\sqrt{2}$ is not a rational number". The statement "$\sqrt{2}$ *is* rational" means that there exist positive integers p and q such that $\sqrt{2} = \frac{p}{q}$. We can therefore express "$\sqrt{2}$ is irrational" using notation as

$$\neg(\exists p \in \mathbb{Z}^+)(\exists q \in \mathbb{Z}^+)\left[\sqrt{2} = \frac{p}{q}\right]$$

or

$$(\forall p \in \mathbb{Z}^+)(\forall q \in \mathbb{Z}^+)\left[\sqrt{2} \neq \frac{p}{q}\right].$$

Exercises 1.1

1. Let P, Q, and R be statements. Determine whether or not the two expressions in each pair are logically equivalent. In each case, demonstrate that your answer is correct.
   (a) $(P \wedge Q) \wedge R, \quad P \wedge (Q \wedge R)$.
   (b) $(P \vee Q) \vee R, \quad P \vee (Q \vee R)$.
   (c) $(P \wedge Q) \vee R, \quad P \wedge (Q \vee R)$.
   (d) $(P \vee Q) \wedge R, \quad P \vee (Q \wedge R)$.

2. Let P, Q, and R be statements. Show that the following statements are logically equivalent.
   (a) $\neg(\neg P)$ and P.
   (b) $(P \vee Q) \wedge R$ and $(P \wedge R) \vee (Q \wedge R)$.
   (c) $(P \wedge Q) \vee R$ and $(P \vee R) \wedge (Q \vee R)$.
   (d) $\neg(P \vee Q)$ and $(\neg P) \wedge (\neg Q)$.
   (e) $P \Rightarrow Q$ and $(\neg P) \vee Q$.
   (f) $\neg(P \Rightarrow Q)$ and $P \wedge (\neg Q)$.

3. Let P, Q, and R be statements. Determine whether or not the two expressions in each pair are logically equivalent. In each case, demonstrate that your answer is correct.
   (a) $(P \Rightarrow Q) \Rightarrow R, \quad P \Rightarrow (Q \Rightarrow R)$.
   (b) $(P \vee Q) \Rightarrow R, \quad (P \Rightarrow R) \vee (Q \Rightarrow R)$.
   (c) $(P \wedge Q) \Rightarrow R, \quad (P \Rightarrow R) \wedge (Q \Rightarrow R)$.
   (d) $P \Rightarrow (Q \vee R), \quad (P \Rightarrow Q) \vee (P \Rightarrow R)$.
   (e) $P \Rightarrow (Q \wedge R), \quad (P \Rightarrow Q) \wedge (P \Rightarrow R)$.

4. Propositions which are "always true" (respectively, "always false") are called tautologies (respectively, contradictions). More precisely:

Definition 1.1.20. A *tautology* is a proposition that is true for every possible assignment of truth values to the statement letters that occur in it. A *contradiction* is a proposition that is false for every possible assignment of truth values to the statement letters that occur in it.

Let P and Q be statements. Determine whether each of the following statements is a tautology, a contradiction, or neither.
(a) $P \Leftrightarrow \neg(\neg P)$.
(b) $P \wedge \neg P$.
(c) $P \vee \neg P$.
(d) $(P \wedge Q) \vee (\neg P \wedge \neg Q)$.
(e) $P \Rightarrow (Q \Rightarrow P)$.

5. Let n be a fixed positive integer. Which of the following statements are true, regardless of which positive integer n you consider? Explain *briefly.* (While you are not being asked to provide a proof, try to explain clearly.)
(a) If n is divisible by 6, then n is divisible by 3.
(b) If n is divisible by 3, then n is divisible by 6.
(c) If n is divisible by 6, then n is divisible by 9.
(d) If n is divisible by 9, then n is divisible by 6.
(e) If n is divisible by 6, then n^2 is divisible by 6.
(f) If n^2 is divisible by 6, then n is divisible by 6.
(g) If n^2 is divisible by 9, then n is divisible by 9.
(h) If n is divisible by 2 and n is divisible by 3, then n is divisible by 6.
(i) If n is divisible by 2 and n is divisible by 6, then n is divisible by 12.

6. Give an example which shows that statement (1.2) does not hold for all functions f and for all real numbers a; i.e., give a specific example of a function f defined on the real numbers, and a specific real number a, such that f is continuous at a but not differentiable at a.

7. For each of the following statements, give an example of a mathematical universe in which the statement is true and an example of a universe in which the statement is false. Explain why your answers are correct.
(a) $(\forall x)[0 < x^2 < 2 \Rightarrow x = 1]$.
(b) $(\forall x)[0 < x^2 < 2 \Rightarrow (x = 1 \vee x = -1)]$.

8. Let $P(x)$ be a predicate whose only free variable is x and let $\mathcal{U}$ be the intended universe.
(a) Use Definition 1.1.16 to explain why the following statements are logically equivalent (i.e., have the same truth value).
(i) $\neg(\forall x)P(x)$ and $(\exists x)(\neg P(x))$.
(ii) $\neg(\exists x)P(x)$ and $(\forall x)(\neg P(x))$.
(b) Use Proposition 1.1.11, Proposition 1.1.18, and the definitions of the modified quantifiers on page 12 to show that the following statements are logically equivalent.
(i) $\neg(\forall x \in \mathcal{U})P(x)$ and $(\exists x \in \mathcal{U})(\neg P(x))$.
(ii) $\neg(\exists x \in \mathcal{U})P(x)$ and $(\forall x \in \mathcal{U})(\neg P(x))$.

9. Let $\mathcal{U}$ be the universe under consideration, and let $P(x)$ and $Q(x)$ be predicates with free variable x. Find a *useful denial* (i.e., a statement equivalent to the negation) of each statement.

(a) $(\forall x \in \mathcal{U})(P(x) \Rightarrow Q(x))$.
(b) $(\forall x \in \mathcal{U})(Q(x) \vee P(x))$.
(c) $(\exists x \in \mathcal{U})(Q(x) \wedge P(x))$.
(d) $(\exists x \in \mathcal{U})(Q(x) \wedge P(x))$. (Use an implication in your answer.)

10. Express each statement symbolically, including a quantification of all variables which makes the universe explicit. Negate the symbolic statement, and express the negation in natural language as a useful denial.
(a) The inequality $x^2 - 4x + 3 < 0$ has a real solution.
(b) The curves $y = 1 - x^2$ and $y = 3x - 2$ intersect.
(c) Every positive real number has a real square root. (Do not use the symbol $\sqrt{\ }$ in your solution.)

11. Which of the following statements are true? Explain *briefly*. (While you are not being asked to provide a proof, try to explain clearly.)
(a) There exists an integer n such that $4n + 5 = 7n + 3$.
(b) There exists a real number x such that $x^2 + 8x + 12 \geq 0$.
(c) For all real numbers x, $x^2 + 8x + 12 \geq 0$.
(d) For all real numbers x, $x^2 + 8x + 17 \geq 0$.

12. Which of the following statements are true? Explain *briefly*. (While you are not being asked to provide a proof, try to explain clearly.)
(a) For all real numbers x, $x^2 - 2x - 3 = 0$ only if $x = 3$.
(b) For all real numbers x, $x^2 - 2x - 3 = 0$ if $x = 3$.

13. Find the converse and contrapositive of each statement. Here, $\mathbf{v_1}, \mathbf{v_2}, \mathbf{0}$ are fixed vectors in a real vector space (you don't need to know what this means!), x_1, x_2 are fixed real numbers, and f is a fixed function.
(a) $(x_1\mathbf{v_1} + x_2\mathbf{v_2} = \mathbf{0}) \Rightarrow (x_1 = 0 \wedge x_2 = 0)$.
(b) $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

14. Find a *useful denial* (i.e., a statement logically equivalent to the negation) of each statement. Here, $\mathbf{v_1}, \mathbf{v_2}, \mathbf{0}$ are fixed vectors in a real vector space (you don't need to know what this means!) and f is a fixed function.
(a) $(\forall x_1)(\forall x_2)[(x_1\mathbf{v_1} + x_2\mathbf{v_2} = \mathbf{0}) \Rightarrow (x_1 = 0 \wedge x_2 = 0)]$.
(b) $(\forall x_1)(\forall x_2)[f(x_1) = f(x_2) \Rightarrow x_1 = x_2]$.
(c) $(\forall y)(\exists x)[y = f(x)]$.

15. Find a *useful denial* (i.e., a statement logically equivalent to the negation) of each statement, and express it in mathematically precise, natural English. Express all conditional statements in the form "if ..., then ...". Do not add implied quantifiers. (Here, a, b, c, n are fixed integers, f is a fixed function, and x_0, L are fixed real numbers.)
(a) n is not a multiple of 4 if n is even.
(b) If f has a relative maximum at x_0 and f is differentiable at x_0, then $f'(x_0) = 0$.
(c) For every integer m, m^2 is odd and $m^3 - 1$ is divisible by 4.
(d) For all integers j and k, if $n = jk$, then $j = 1$ or $k = 1$.
(e) If n is a perfect square, then there exists an integer k such that $n = 3k$ or $n = 3k + 1$.
(f) bc is divisible by a only if b is divisible by a or c is divisible by a.

(g) For all $\varepsilon > 0$ there exists $\delta > 0$ such that for all x, $|f(x) - L| < \varepsilon$ if $0 < |x - x_0| < \delta$.

(h) For every real number M there exists a real number x such that $f(x) > M$.

(i) If n is an odd integer, then there exists an integer k such that $n = 4k + 1$ or $n = 4k + 3$.

16. Write the converse and contrapositive of each conditional statement. Do not add implied quantifiers. Express all conditional statements in the form "if ..., then ...". (Here, n is a fixed integer, x is a fixed real number, S is a fixed set of real numbers, $\{a_n\}$ is a fixed sequence of real numbers, and G is a group. In this exercise, it is not necessary to know the meanings of any mathematical concepts we have not yet defined.)

(a) If $x > 1$ or $x < -1$, then $x^2 > 1$.

(b) n^2 is a multiple of 3 is sufficient for n to be a multiple of 3.

(c) S is closed and bounded is necessary for S to be compact.

(d) $\{a_n\}$ converges if $\{a_n\}$ is bounded and monotone.

(e) $\{a_n\}$ is Cauchy only if $\{a_n\}$ converges.

(f) If n is an odd integer, then there exists an integer k such that $n = 4k + 1$ or $n = 4k + 3$.

(g) If G is abelian, then every subgroup of G is normal.

(h) If n is a perfect square, then there exists an integer k such that $n = 3k$ or $n = 3k + 1$.

1.2. Proof

1.2.1. Logical arguments. So far we have concentrated on the language, notation, and grammar of mathematical statements. Now we move on to our goal of learning to construct clear and correct mathematical proofs.

What is a proof? Informally, we will define a mathematical proof to be a logical argument that establishes the truth of a mathematical statement.

What is a logical argument? We'll first consider the following familiar example from calculus.

Suppose that f is a fixed function defined on a subset of the real numbers and that a is a fixed real number. Suppose you also know:

- If f is differentiable at a, then f is continuous at a.
- f is differentiable at a.

What logical conclusion can you draw? That f is continuous at a. While you probably came to this conclusion without thinking too much about it, technically you constructed a valid logical argument using the "rule of deduction" called *modus ponens*. If we represent the statement "f is differentiable at a" by the statement letter P and the statement "f is continuous at a" by Q, then *modus ponens* says "from P and $P \Rightarrow Q$, deduce Q". We can see that it is reasonable to adopt *modus ponens* as a rule of deduction by looking again at the truth table for $P \Rightarrow Q$ in Table 1.11.

Table 1.11. Truth table for $\Rightarrow$.

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

Modus ponens says that we begin by knowing that $P \Rightarrow Q$ is true and P is true. Only the first line in the truth table corresponds to this situation; in this line, Q is also true. It follows that "Q is true" is a valid conclusion, based on the hypotheses that P is true and $P \Rightarrow Q$ is true. Thus, the form of a logical argument is based on the logic of our connectives and on the logic of our quantifiers.

If we wish to prove a mathematical statement, then we must first determine the logical form of that statement.

1.2.2. Direct proofs, an introduction. We begin by considering statements of the form $P \Rightarrow Q$. To determine how we might prove that a statement with this logical form is true, we again look at the truth table for implication in Table 1.11. We see that the statement $P \Rightarrow Q$ is automatically true when P is false, so there is no need to consider this situation. In other words, we should begin by assuming that P is true. The first line in the truth table Table 1.11 then shows us how to proceed: we should demonstrate that Q is true. This type of logical argument is called a *direct* proof of the statement $P \Rightarrow Q$. It is so fundamental in mathematics that we emphasize it again in Table 1.12.

Table 1.12. Direct proof of $P \Rightarrow Q$.

To prove a statement of the form $P \Rightarrow Q$ is true (directly).
• We begin with "Assume P is true." • We must then demonstrate that Q is true.

Next, we ask how to prove a statement of the form $(\forall x)P(x)$ is true. Recall that there is an underlying universe $\mathcal{U}$ corresponding to the universal quantifier. Definition 1.1.16 tells us that the statement $(\forall x)P(x)$ is true exactly when every element a in the universe $\mathcal{U}$ has the property that $P(a)$ is true. In general, it's not possible to show $P(a)$ is true for each element a in the universe individually. Indeed, when the universe is infinite, there is no way to do this, since a proof must be finite. In a direct proof of $(\forall x)P(x)$, therefore, we demonstrate that if x is an *arbitrary, fixed* element of the universe, then $P(x)$ is true. See Table 1.13.

Definition 1.1.16 also tells us how to prove (directly) that a statement of the form $(\exists x)P(x)$ is true. See Table 1.14.

Let's begin by proving the following:

The sum of an even integer and an odd integer is odd.

Table 1.13. Direct proof of $(\forall x)P(x)$.

To prove a statement of the form $(\forall x)P(x)$ is true (directly).
• We begin with "Let x be an arbitrary (but now *fixed*), element of the universe." • We must then demonstrate that $P(x)$ is true.

Table 1.14. Direct proof of $(\exists x)P(x)$.

To prove a statement of the form $(\exists x)P(x)$ is true (directly).
• We must *find* an element a in the universe such that $P(a)$ is true. • In other words, we must explicitly *say* what a is *and demonstrate* that $P(a)$ is true.

We cannot proceed until we are sure that we know what the words mean. While you certainly know intuitively what the words "even" and "odd" mean, a mathematical proof that a particular undetermined integer is even or odd relies on knowing the precise mathematical definition of these words. Without knowing the logical structure of these definitions, we will not know what must be proved.

Definition 1.2.1. Let $n \in \mathbb{Z}$.

(1) n is *even* if there exists an integer k such that $n = 2k$; i.e.,

$$n \text{ is even if } (\exists k \in \mathbb{Z})[n = 2k].$$

(2) n is *odd* if there exists an integer k such that $n = 2k + 1$; i.e.,

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

We should make two observations about this formal definition right away. First, it is almost universal in mathematics to use the word "if" in a definition when what is actually meant is "if and only if". For example, technically Definition 1.2.1 says only that, for a given integer n, *if* we know that there exists $k \in \mathbb{Z}$ such that $n = 2k$, *then* we can conclude that n is even. Although not explicitly stated in Definition 1.2.1, it is further understood that *if* we know that n is even, *then* there exists $k \in \mathbb{Z}$ such that $n = 2k$. While this completely contradicts our policy of always saying exactly what we mean, it is standard practice in mathematics that definitions have this special status, and so we may as well get used to it now.

Special status of definitions. *Mathematical definitions are always* **if and only if** *statements.*

Next, we should note that we will assume that every integer is either even or odd, but never both. You certainly believe this, but it actually requires a proof. We will make use of this assumption for now and justify it in Exercise 2.2.2 and Chapter 6.

Most importantly, we need to be sure that we recognize the logical structure of the statement to be proved, which we purposely stated first in colloquial English.

As a mathematical statement, “the sum of an even integer and an odd integer is odd” should be interpreted as follows:

> if m is an even integer and n is an odd integer, then $m+n$ is an odd integer.

Remember that we must be careful. There are assumed universal quantifiers here:

$$(\forall m \in \mathbb{Z})(\forall n \in \mathbb{Z})[(m \text{ is even and } n \text{ is odd}) \Rightarrow (m+n \text{ is odd})].$$

We should never expect to simply “write down” a proof of a statement; we will need to search for it. To organize our thoughts for this “scratchwork”, we will use a “Given-Goal” diagram[1] to identify what is given and what is our goal. The universal quantifiers tell us to assume that m and n are arbitrary (and now fixed) integers.

Given	**Goal**
m, n arbitrary integers	if m is even and n is odd, then $m+n$ is odd

Right away, the logical structure of the goal, an implication, tells us what to do next.

The Goal dictates the form of the proof.

Table 1.12 tells us that we should *assume* the hypotheses that m is even and n is odd and then rewrite our goal:

Given	**Goal**
m, n arbitrary integers m is even n is odd	$m+n$ is odd

We must search for a logical way of getting to our *goal* from our *givens*. One useful way to search is with a “backward-forward” method. You should ask yourself the following questions:

What’s my goal? What does it mean?

What’s given? What does it mean?

Our job is to work back and forth between these ideas until we find the logical connections.

Our *Goal* is to show:

$$m+n \text{ is odd.}$$

Since the definition of *odd* is existential, Table 1.14 tells us that our goal is to

find a particular integer a such that $m+n=2a+1$.

[1] The notion of a “Given-Goal” diagram as a way of organizing one’s thoughts regarding what is known, versus what is to be proved, was first used in Daniel J. Velleman’s book *How to Prove It: A Structured Approach* [**15**]. It is also used in Peter J. Eccles’s book *An Introduction to Mathematical Reasoning: Numbers, Sets and Functions* [**8**], where Velleman is credited with the terminology.

We are *Given* that

$$m \text{ is even.}$$

This means that

$$\textit{there exists} \text{ an integer } k \text{ such that } m = 2k.$$

Since such an integer *exists*, we'll *fix* one so that we can work with it; i.e., we can

$$\text{fix } i \in \mathbb{Z} \text{ such that } m = 2i.$$

Similarly, since we know

$$n \text{ is odd,}$$

we can

$$\text{fix } j \in \mathbb{Z} \text{ such that } n = 2j + 1.$$

Since we both have and want information about the integer $m + n$, it makes sense to investigate this quantity. Note that

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

Since $i + j$ is an integer, we've found the integer a we are seeking.

We've convinced ourselves that the statement is true, but part of our job is to formally and effectively communicate a mathematical proof of this statement to others.

Proposition 1.2.2. *For all integers m and n, if m is even and n is odd, then $m + n$ is odd.*

Proof. Let m, $n \in \mathbb{Z}$ be arbitrary, and assume that m is even and n is odd. We show that $m + n$ is odd; i.e., we must find an integer a such that $m + n = 2a + 1$.

Since m is even, by Definition 1.2.1 we can fix $i \in \mathbb{Z}$ such that $m = 2i$. Similarly, since n is odd, by Definition 1.2.1 we can fix $j \in \mathbb{Z}$ such that $n = 2j + 1$. Then

$$\begin{aligned} m + n &= 2i + (2j + 1) \\ &= (2i + 2j) + 1 \\ &= 2(i + j) + 1, \end{aligned}$$

by the associative and distributive properties. Since $i + j$ is an integer, $m + n$ is odd, by Definition 1.2.1.

Hence, the sum of an even integer and an odd integer is odd. □

1.2.3. Some important observations. Despite the apparent simplicity of the statement and proof of Proposition 1.2.2, there are several important lessons that must be emphasized. First, in our scratchwork, we progressed from the statement

$$m \text{ is even}$$

to

$$(\exists k \in \mathbb{Z})(m = 2k)$$

to

$$\text{fix an integer } i \text{ such that } m = 2i.$$

Going from the existential statement $(\exists k \in \mathbb{Z})(m = 2k)$ (which simply asserts that something exists) to fixing a *particular* integer $i \in \mathbb{Z}$ with $m = 2i$ (which fixes a *particular example* of such an object and gives it a name) is called *existential instantiation.*

It's important here to use a new name (*variable*) *that doesn't already have a particular meaning in your proof.* To avoid wordiness in the final proof, we instantiated the existential quantifiers right away, *taking care to use a new variable each time.*

In fact, at the beginning of the final proof, the name (variable) k did not yet have a meaning. Consequently, we could have replaced the line

since m is even, by Definition 1.2.1 we can fix $i \in \mathbb{Z}$ such that $m = 2i$

by

since m is even, by Definition 1.2.1 we can fix $k \in \mathbb{Z}$ such that $m = 2k$.

Or, we could have replaced it by

since m is even, by Definition 1.2.1 we can fix $\ell \in \mathbb{Z}$ such that $m = 2\ell$.

However, once we choose a name to use to instantiate the first quantifier:

since m is even, by Definition 1.2.1 we can fix $i \in \mathbb{Z}$ such that $m = 2i$,

the meaning of the variable i becomes fixed for the rest of the proof, and *it would then be a mistake to say*,

since n is odd, by Definition 1.2.1 we can fix $i \in \mathbb{Z}$ such that $n = 2i + 1$.

Summarizing:

> If we *know* $(\exists x)P(x)$, where $P(x)$ is some predicate involving the free variable x, then we should *fix a particular* x such that $P(x)$ holds, as long as we take care *not* to use a variable whose meaning in the current proof is already fixed.

Next, note how essential the mathematical definitions of "even" and "odd" were in the proof. As we mentioned earlier, you almost certainly "knew" the definitions of these words already, at least in an intuitive sense. In mathematics, however, language must be used precisely and arguments must be rigorous. To prove that an integer is odd (or that something is a widget), we must have a precise mathematical definition of this concept, and the logical form of that definition indicates the structure of that proof.

Summarizing:

> If we wish to prove that something is a *widget* and all we know about widgets is the definition, then we must use the definition to prove it's a widget.
> The logical form of the definition of widget determines the structure of a proof that something is a widget.

It is also important to note the difference between the *search for the proof* (i.e., the scratchwork) and the mathematical proof we produced at the end. In this case, the scratchwork and the proof look pretty similar, but often it can take several approaches before you come up with the right idea for a proof. In fact, this is why reading mathematical proofs can seem difficult; you are reading the polished, finished product, and not the process by which the proof was discovered. Typically, mathematical proofs do not describe the process by which the proof was discovered (i.e., the scratchwork), although there are exceptions to this.

Furthermore, as we've emphasized from the beginning, we want to be sure to use mathematical language and notation correctly in mathematical writing. See the appendix for some suggested guidelines to help you write mathematics effectively. These guidelines review the general comments mentioned here, as well as address other issues.

Finally, it is important to note that we used some basic properties of integers in the proof of Proposition 1.2.2 (such as the associative property of addition and the distributive property). At the beginning of this section on proof, we noted that a proof is a logical argument and illustrated the role that *modus ponens* plays. Students who first learn about proof in mathematics often wonder what mathematical statements need proof, particularly when a statement "seems obvious" to them. Indeed, while our point of view in this course will be that "all" mathematical statements require proof, one cannot prove anything at all without some basic assumptions, which are often called *axioms*.

To give us a starting point, we will consider the statements found in Basic Properties of Integers 1.2.3 on page 23 (and also the *Principle of Mathematical Induction*, to be discussed in Chapter 3) to be our basic assumptions about the integers. We will accept these statements without proof, and you might take a moment to ask yourself whether you think it is reasonable for us to do so. (In fact, we could have taken a smaller list of statements as our basic assumptions about the integers and proved the rest from that smaller list.) All other statements we mention about integers, however, will require proof, unless we explicitly state otherwise. In this way, it should be very clear to you when a statement requires a proof. In general, we will never consider a mathematical statement, no matter how "simple" it may seem, as "obvious".

Basic Properties of Integers 1.2.3.

For all integers a, b, c:

(Closure under + and $\cdot$) $a + b$ and ab are also integers.

(Associative properties) $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$.

(Commutative properties) $a + b = b + a$ and $ab = ba$.

(Distributive property) $a(b + c) = ab + ac$.

(Identities) $0 \neq 1$, $a + 0 = a$, $a \cdot 1 = a$, and $a \cdot 0 = 0$.

(Additive inverses) There is a unique integer $-a = -1 \cdot a$ such that $a + (-a) = 0$.

(Subtraction) $b - a$ is defined to equal $b + (-a)$.

(No divisors of 0) If $ab = 0$, then $a = 0$ or $b = 0$.

(Cancellation) If $ab = ac$ and $a \neq 0$, then $b = c$.

(Transitive property of <) If $a < b$ and $b < c$, then $a < c$.

(Trichotomy) Exactly one of $a < b$ or $a = b$ or $a > b$ holds.

(Order property 1) If $a < b$, then $a + c < b + c$.

(Order property 2) If $c > 0$, then $a < b$ iff $ac < bc$.

(Order property 3) If $c < 0$, then $a < b$ iff $ac > bc$.

Note in particular the cancellation property of integers; there is no division operation in the integers. In order to use the cancellation property to conclude $b = c$ from $ab = ac$, where $a, b, c \in \mathbb{Z}$, we must first explain why $a \neq 0$.

Exercises 1.2

1. Let n be an integer.
   (a) Prove that if n is even, then n^2 is even.
   (b) Prove that if n is odd, then n^2 is odd.
2. Let m and n be integers.
   (a) Prove that if m and n are even, then $m + n$ is even.
   (b) Prove that if m and n are odd, then $m + n$ is even.
3. (a) Prove that for all $m \in \mathbb{Z}$, if m is even, then mn is even.
   (b) Prove that for all $m, n \in \mathbb{Z}$, if m and n are odd, then mn is odd.
4. Use the definition to prove that for all $n \in \mathbb{N}$, $4n + 7$ is odd.

Appendix

Writing Mathematics

Chances are the mathematics course you are currently taking will require far more "writing in English" than any other math course you have previously taken, which may be surprising to you. Whereas in previous courses you may have written solutions to problems by simply writing line after line of formulas, with no English words at all, now you are required to write complete English sentences and paragraphs. This does not mean that no formulas will appear, but rather, formulas should be incorporated *grammatically* into sentences.

In any subject, whether it be history, biology, economics, or mathematics, our job is to *communicate* what we know, and how we know it, to others. Learning to write mathematics well requires a lot of practice and can be difficult at the beginning. The following guidelines[1] for writing mathematics point out some of the issues you'll want to keep in mind.

(1) All proofs (or solutions involving some sort of explanation) should be written in grammatically correct, complete English sentences.

(2) Begin a proof by assuming the relevant hypotheses. End each proof with a sentence that reiterates what has been proved.
  - For example, if you are trying to prove that the product of two odd numbers is odd, then you should *begin* by saying, "Let m and n be odd integers." The last line of the proof might be something like, "Hence, mn is odd, as desired."

(3) Proofs (or solutions involving some sort of explanation) should include enough detail for the reader to understand your reasoning. Do not assume that the reader knows what you are talking about. Assume that your reader has the same mathematical background as you but does not know the proof you are writing.

[1] These guidelines were originally inspired by a "Writing checklist" created by Dr. Annalisa Crannell of Franklin & Marshall College. I have adapted them over time in the various "proof courses" I have taught in my career at Allegheny College.

(4) Be sure that what you have written is mathematically precise. Mean what you write, and write what you mean.

(5) Use proper mathematical notation and terminology.

- All variables must be *explicitly* defined.
  - For example, if you are trying to prove that the product of two odd numbers is odd, then you should *begin* by saying, "Let m and n be odd integers." If you are then tempted to write "$m = 2k+1$", then you should explicitly identify what k is and explain why it exists.
- Mathematical symbols should not be confused with English words. For example, the symbol "=" should be used only in mathematical formulas and computations, not as the verb "is" in a sentence.

(6) Proofs should explicitly make reference to any definitions or theorems used.

(7) Proofs should not contain any scratchwork or work done in the margins, nor any large sections of "crossed out" work.

(8) Proofread all solutions for correctness and clarity. Recopying your solutions is one useful way to accomplish this.