APPENDIX A

Logic and Proof

This Appendix summarizes the basic facts about logic and proof that are needed to read this book. For a complete discussion of these topics see Galovich [9], Lucas [11], Smith-Eggen-St. Andre [12], or Solow [13].

LOGIC

A **statement** is a declarative sentence that is either true or false. For instance, each of these sentences is a statement:

> π is a real number.
>
> Every triangle is isosceles.
>
> 103 bald eagles were born in the United States last year.

Note that the last sentence *is* a statement even though we may not be able to verify its truth or falsity. Neither of the following sentences is a statement:

> What time is it? Wow!

Compound Statements

We frequently deal with **compound statements** that are formed from other statements by using the connectives "and" and "or." The truth of the compound statement will depend on the truth of its components. If P and Q are statements, then

"*P* and *Q*" is a true statement when *both* *P* and *Q* are true, and false otherwise.

For example,

$$\pi \text{ is a real number and } 9 < 10$$

is a true statement because both of its components are true. But

$$\pi \text{ is a real number and } 7 - 5 = 18$$

is a false statement since one of its components is false.

In ordinary English the word "or" is most often used in exclusive sense, meaning "one or the other but not both," as in

He is at least 21 years old or he is younger than 21.

But "or" can also be used in an inclusive sense, meaning "one or the other, or possibly both," as in the sentence

They will win the first game or they will win the second.

Thus the inclusive "or" has the same meaning as "and/or" in everyday language. In mathematics, *"or" is always used in the inclusive sense,* which allows the possibility that both components might be true but does not require it. Consequently, if P and Q are statements, then

"*P* or *Q*" is a true statement when at least one of *P* or *Q* is true and false when both *P* and *Q* are false.

For example, both

$$7 > 5 \quad \text{or} \quad 3 + 8 = 11$$

and

$$7 > 5 \quad \text{or} \quad 3 + 8 = 23$$

are true statements because at least one component is true in each case, but

$$4 < 2 \quad \text{or} \quad 5 + 3 = 12$$

is false since both components are false.

Negation

The **negation** of a statement P is the statement "it is not the case that P," which we can conveniently abbreviate as "not-P." Thus the negation of

7 is a positive integer

is the statement "it is not the case that 7 is a positive integer," which we would normally write in the less awkward form "7 is not a positive integer." If P is a statement, then

The negation of *P* is true exactly when *P* is false, and the negation of *P* is false exactly when *P* is true.

The negation of the statement "P and Q" is the statement "it is not the case that P and Q." Now "P and Q" is true exactly when both P and Q are true, so to say that this is not the case means that at least one of P or Q is false. But this occurs exactly when at least one of not-P or not-Q is true. Thus

The negation of the statement "P and Q" is the statement "not-P *or* not-Q."

For example, the negation of

f is continuous and f is differentiable at $x = 5$

is the statement

f is not continuous or f is not differentiable at $x = 5$.

The negation of the statement "P or Q" is the statement "it is not the case that P or Q." Now "P or Q" is true exactly when at least one of P or Q is true. To say that this is not the case means that both P and Q are false. But P and Q are both false exactly when not-P and not-Q are both true. Hence,

The negation of the statement "P or Q" is the statement "not-P *and* not-Q."

For instance, the negation of

119 is prime or $\sqrt{3}$ is a rational number

is the statement

119 is not prime and $\sqrt{3}$ is not a rational number.

Quantifiers

Many mathematical statements involve quantifiers. The **universal quantifier** states that a property is true *for all* the items under discussion. There are several grammatical variations of the universal quantifier, such as

For all real numbers c, $c^2 - 1$.
Every integer is a real number.
All integers are rational numbers.
For each real number a, the number $a^2 + 1$ is positive.

The **existential quantifier** asserts that *there exists* at least one object with certain properties. For example, There exist positive rational numbers.

There exists a number x such that $x^2 - 5x + 6 = 0$.

There is an even prime number.

In mathematics, the word "some" means "at least one" and is, in effect, an existential quantifier. For instance,

Some integers are prime

is equivalent to saying "at least one integer is prime," that is,

There exists a prime integer.

Care must be used when forming the negation of statements involving quantifiers. For example, the negation of

All real numbers are rational

is "it is not the case that all real numbers are rational," which means that there is at least one real number that is irrational (= not rational). So the negation is

There exists an irrational real number.

In particular, the statements "all real numbers are not rational" and "all real numbers are irrational" are *not* negations of "all real numbers are rational." This example illustrates the general principle:

The negation of a statement with a universal quantifier is a statement with an existential quantifier.

The negation of the statement

There exists a positive integer

is "it is not the case that there is a positive integer," which means that "every integer is nonpositive" or, equivalently, "no integer is positive." Thus

The negation of a statement with an existential quantifier is a statement with a universal quantifier.

Conditional and Biconditional Statements

In mathematical proofs we deal primarily with **conditional statements** of the form

If P, then Q

which is written symbolically as $P \Rightarrow Q$. The statement P is called the

hypothesis or **premise,** and Q is called the **conclusion.** Here are some examples:

If c and d are integers, then cd is an integer.
If f is continuous at $x = 3$, then f is differentiable there.
$a \neq 0 \Rightarrow a^2 > 0$.

There are several grammatical variations, all of which mean the same thing as "if P, then Q":

P implies Q.
P is sufficient for Q.
Q provided that P.
Q whenever P.

In ordinary usage the statement "if P, then Q" means that the truth of P guarantees the truth of Q. Consequently,

"$P \Rightarrow Q$" is a true statement when both P and Q are true and false when P is true and Q is false.

Although the situation rarely occurs, we must sometimes deal with the statement "$P \Rightarrow Q$" when P is false. For example, consider this campaign promise: "If I am elected, then taxes will be reduced." If the candidate is elected (P is true), the truth or falsity of this statement depends on whether or not taxes are reduced. But what if the candidate is *not* elected (P is false)? Regardless of what happens to taxes, you can't fairly call the campaign promise a lie. Consequently, it is customary in symbolic logic to adopt this rule:

When P is false, the statement "$P \Rightarrow Q$" is true.

The **contrapositive** of the conditional statement "$P \Rightarrow Q$" is the statement "not-$Q \Rightarrow$ not-P." For instance, the contrapositive of this statement about integers

If c is a multiple of 6, then c is even

is the statement

If c is not even, then c is not a multiple of 6.

Notice that both the original statement and its contrapositive are true. Two statements are said to be **equivalent** if one is true exactly when the other is. We claim that

The conditional statement "$P \Rightarrow Q$" is equivalent to its contrapositive "not-$Q \Rightarrow$ not-P."

To prove this equivalence, suppose $P \Rightarrow Q$ is true and consider the statement not-$Q \Rightarrow$ not-P. Suppose not-Q is true. Then Q is false. Now if P were true, then Q would necessarily be true, which is not the case. So P must be false, and, hence, not-P is true. Thus not-$Q \Rightarrow$ not-P is true. A similar argument shows that when not-$Q \Rightarrow$ not-P is true, then $P \Rightarrow Q$ is also true.

The **converse** of the conditional statement "$P \Rightarrow Q$" is the statement "$Q \Rightarrow P$." For example, the converse of the statement

If b is a positive real number, then b^2 is positive

is the statement

If b^2 is positive, then b is a positive real number.

This last statement is false since, for example, $(-3)^2$ is the positive number 9, but -3 is not positive. Thus

The converse of a true statement may be false.

There are some situations in which a conditional statement and its converse are both true. For example,

If the integer k is odd, then the integer $k + 1$ is even

is true, as is its converse

If the integer $k + 1$ is even, then the integer k is odd.

We can state this fact in succinct form by saying that "k is odd *if and only if* $k + 1$ is even." More generally, the statement

P if and only if Q,

which is abbreviated as "P iff Q" or "$P \Leftrightarrow Q$," means

$$P \Rightarrow Q \qquad \textit{and} \qquad Q \Rightarrow P.$$

"P if and only if Q" is called a **biconditional statement.** The rules for compound statements show that "P if and only if Q" is true exactly when both $P \Rightarrow Q$ and $Q \Rightarrow P$ are true. In this case, the truth of P implies the truth of Q and vice-versa, so that P is true exactly when Q is true. In other words, "P if and only if Q" means that P and Q are equivalent statements.

THEOREMS AND PROOF

The formal development of a mathematical topic begins with certain undefined terms and **axioms** (statements about the undefined terms that are assumed to be true). These undefined terms and axioms are used to define new terms and to construct **theorems** (true statements about these objects). The **proof** of a theorem is a complete justification of the truth of the statement.

Most theorems are conditional statements. A theorem that is not stated in conditional form is often equivalent to a conditional statement. For instance, the statement

Every integer greater than 1 is a product of primes

is equivalent to

If n is an integer and $n > 1$, then n is a product of primes.

The first step in proving a theorem that can be phrased in conditional form is to identify the hypothesis P and the conclusion Q. In order to prove the theorem "$P \Rightarrow Q$," one assumes that the hypothesis P is true and then uses it, together with axioms, definitions, and previously proved theorems, to argue that the conclusion Q is necessarily true.

Methods of Proof

Some common proof techniques are described below. While such summaries are helpful, there are no hard and fast rules that give a precise procedure for proving every possible mathematical statement. The methods of proof to be discussed here are in the nature of maps to guide you in analyzing and constructing proofs. A map may not reveal all the difficulties of the terrain, but it usually makes the route clearer and the journey easier.

DIRECT METHOD This method of proof depends on the basic rule of logic called *modus ponens:* If R is a true statement and "$R \Rightarrow S$" is a true conditional statement, then S is a true statement. To prove the theorem "$P \Rightarrow Q$" by the direct method, you find a series of statements $P_1, P_2, \ldots, P_n$ and then verify that each of the implications $P \Rightarrow P_1, P_1 \Rightarrow P_2, P_2 \Rightarrow P_3, \ldots, P_{n-1} \Rightarrow P_n$, and $P_n \Rightarrow Q$ is true. Then the assumption that P is true and repeated use of *modus ponens* show that Q is true.

The direct method is the most widely used method of proof. In actual practice, it may be quite difficult to figure out the various intermediate statements that allow you to proceed from P to Q. In order to find them, most mathematicians use a thought process that is sometimes called the **forward-backward technique.** You begin by working forward and asking yourself, What do I know about the hypothesis P? What facts does it imply? What statements follow from these facts? And so on. At this point you may have a list of statements implied by P whose connection with the conclusion Q, if any, is not yet clear.

Now work backward from Q by asking, What facts would guarantee that Q is true? What statements would imply these facts? And so on. You now have a list of statements that imply Q. Compare it with the first list. If you are fortunate some statement will be on both lists, or more likely, there will be a statement S on the first list and a statement T on the second, and you may be able to show that $S \Rightarrow T$. Then you have $P \Rightarrow S$ and $S \Rightarrow T$ and $T \Rightarrow Q$, so that $P \Rightarrow Q$.

When you have used the forward-backward technique successfully to find a proof that $P \Rightarrow Q$, you should write the proof in finished form. This finished form may look quite different from the thought processes that led you to the proof. Your thought process jumped forward and backward, but the finished proof normally should begin with P and proceed in step-by-step logical order from P to S to T to Q. The finished proof should contain only those facts that are needed in the proof. Many statements that arise in the forward-backward process turn out to be irrelevant to the final argument, and they should *not* be included in the finished proof. As illustrated in most of the proofs in this book, the finished proof is usually written as a narrative rather than a series of conditional statements.

CONTRAPOSITIVE METHOD Since every conditional statement is equivalent to its contrapositive, you may prove "not-$Q \Rightarrow$ not-P" in order to conclude that "$P \Rightarrow Q$" is true. For example, instead of proving that for a certain function f,

$$\text{If } a \neq b, \text{ then } f(a) \neq f(b)$$

you can prove the contrapositive

$$\text{If } f(a) = f(b), \text{ then } a = b.$$

PROOF BY CONTRADICTION Suppose that you assume the truth of a statement R and that you make a valid argument that $R \Rightarrow S$ (that is, $R \Rightarrow S$ is a true statement). If the statement S is in fact a *false* statement, there is only one possible conclusion: The original statement R must have been false, because a true premise R and a true statement $R \Rightarrow S$ lead to the truth of S by *modus ponens*.

In order to use this fact to prove the theorem "$P \Rightarrow Q$," assume as usual that P is a true statement. Then apply the argument in the preceding paragraph with R = not-Q. In other words, assume that *not-Q* is true and find an argument (presumably using P and previously proved results) that shows not-$Q \Rightarrow S$, where S is a statement known to be false. Conclude that not-Q must be false. But not-Q is false exactly when Q is true. Therefore, Q is true, and we have proved that $P \Rightarrow Q$. Once again, the hard part will usually be finding the statement S and proving that not-Q implies S.

EXAMPLE Recall that an integer is even if it is a multiple of 2 and that an integer that is not even is said to be odd. We shall use proof by contradiction to prove this statement

If m^2 is even, then m is even.

Here P is the statement "m^2 is even" and Q is the statement "m is even." We assume "m is not even" or equivalently "m is odd" (statement not-Q). But every odd integer is 1 more than some even integer. Since every even integer is a multiple of 2, we must have $m = 2k + 1$ for some integer k. Then the basic laws of arithmetic show that

$$m^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

This last statement says that m^2 is 1 more than a multiple of 2, that is, m^2 is odd. But we are given that m^2 is even (statement P), and, hence, "m^2 is both odd and even" (statement S). This statement is false since no integer is both odd and even. Therefore, our original assumption (not-Q) has led to a contradiction (the false statement S). Consequently, not-Q must be false, and, hence, the statement "m is even" (statement Q) is true.

In the preceding example various statements were labeled by letters so that you could easily relate the example to the general discussion. This is not usually done in proofs by contradiction, and such proofs may not be given in as much detail as in this example.

The choice of a method of proof is partly a matter of taste and partly a question of efficiency. Although any of those listed above may be used, one method may lead to a much shorter or easier-to-follow proof than another, depending on the circumstances. In addition there are methods of proof that can be applied only to certain types of statements.

PROOF BY INDUCTION This method is discussed in detail in Appendix C.

CONSTRUCTION METHOD This method is appropriate for theorems that include a statement of the type "There exists a such-and-such with property so-and-so." For instance,

There is an integer d such that $d^2 - 4d - 5 = 0$.

If r and s are distinct rational numbers, then there is a rational number between r and s.

> If r is a positive real number, then there is a positive integer m such that $\frac{1}{m} < r$.

To prove such a statement, you must construct (find, build, guess, etc.) an object with the desired property. When you are reading the proof of such a statement, you need only verify that the object presented in the proof does in fact have the stated property. An existence proof may amount to nothing more than presenting an example (for instance, the integer 2 provides a proof of "there exists a positive integer"). But more often a nontrivial argument will be needed to produce the required object.

> **Warning** Although an example is sufficient to prove an existence statement, examples can never *prove* a statement that directly or indirectly involves a universal quantifier. For instance, even if you have a million examples for which this statement is true:
>
> If c is an integer, then $c^2 - c + 11$ is prime,
>
> you will not have proved it. For the statement says, in effect, that for *every* integer c, a certain other integer is prime. This is *not* the case when $c = 12$ since $12^2 - 12 + 11 = 143 = 13 \cdot 11$. So the statement is false. This example demonstrates that
>
> **A counterexample is sufficient to *disprove* a statement.**

The moral of the story is that when you are uncertain if a statement is true, try to find some examples where it holds or fails. If you find just one example where it fails, you have disproved the statement. If you can find only examples where the statement holds, you haven't proved it, but you do have encouraging evidence that it may be true.

Proofs of Multiconditional Statements

In order to prove the biconditional statement "P if and only if Q," you must prove *both* "$P \Rightarrow Q$" *and* "$Q \Rightarrow P$." Proving one of these statements and failing to prove the other is a common student mistake. For example, the proof of

> A triangle with sides a, b, c is a right triangle with hypotenuse c if and only if $c^2 = a^2 + b^2$

consists of two separate parts. *First* you must assume that you have a right triangle with sides a, b and hypotenuse c and prove that $c^2 = a^2 + b^2$. Then you must give a *second* argument: Assume that the sides of a triangle satisfy $c^2 = a^2 + b^2$ and prove that this is a right triangle with hypotenuse c.

A statement of the form

The following conditions are equivalent: P, Q, R, S, T

is called a **multiconditional statement** and means that any one of the statements P, Q, R, S, or T implies every other one. Thus a multiconditional statement is just shorthand for a list of biconditional statements; $P \Leftrightarrow Q$ and $P \Leftrightarrow R$ and $P \Leftrightarrow S$ and $P \Leftrightarrow T$ and $Q \Leftrightarrow R$ and $Q \Leftrightarrow S$, etc. To prove this multiconditional statement you need only prove

$$P \Rightarrow Q \text{ and } Q \Rightarrow R \text{ and } R \Rightarrow S \text{ and } S \Rightarrow T \text{ and } T \Rightarrow P.$$

All the other required implications then follow immediately; for instance, from $T \Rightarrow P$ and $P \Rightarrow Q$, we know that $T \Rightarrow Q$, and similarly in the other cases.

EXAMPLE In order to prove this theorem about integers:

The following conditions on a positive integer p are equivalent:

(1) *p is prime.*

(2) *If p is a factor of ab, then p is a factor of a or p is a factor of b.*

(3) *If $p = rs$, then $r = \pm 1$ or $s = \pm 1$.*

you must make *three* separate arguments. First, assume (1) and prove (2), so that (1) $\Rightarrow$ (2) is true. Second, you assume (2) and prove (3), so that (2) $\Rightarrow$ (3) is true. Finally, you must assume (3) and prove (1), so that (3) $\Rightarrow$ (1) is true. *Be careful:* At each stage you assume only one of the three statements and use it to prove another; the third statement does not play a role in that part of the argument.