3

Proofs

3.1. Proof Strategies

Mathematicians are skeptical people. They use many methods, including experimentation with examples, trial and error, and guesswork, to try to find answers to mathematical questions, but they are generally not convinced that an answer is correct unless they can prove it. You have probably seen some mathematical proofs before, but you may not have any experience writing them yourself. In this chapter you'll learn more about how proofs are put together, so you can start writing your own proofs.

Proofs are a lot like jigsaw puzzles. There are no rules about how jigsaw puzzles must be solved. The only rule concerns the final product: All the pieces must fit together, and the picture must look right. The same holds for proofs.

Although there are no rules about how jigsaw puzzles must be solved, some techniques for solving them work better than others. For example, you'd never do a jigsaw puzzle by filling in every *other* piece, and then going back and filling in the holes! But you also don't do it by starting at the top and filling in the pieces in order until you reach the bottom. You probably fill in the border first, and then gradually put other chunks of the puzzle together and figure out where they go. Sometimes you try to put pieces in the wrong places, realize that they don't fit, and feel that you're not making any progress. And every once in a while you see, in a satisfying flash, how two big chunks fit together and feel that you've suddenly made a lot of progress. As the pieces of the puzzle fall into place, a picture emerges. You suddenly realize that the patch of blue you've been putting together is a lake, or part of the sky. But it's only when the puzzle is complete that you can see the whole picture.

Similar things could be said about the process of figuring out a proof. And I think one more similarity should be mentioned. When you finish a jigsaw puzzle, you don't take it apart right away, do you? You probably leave it out for a day or two, so you can admire it. You should do the same thing with a proof. You figured out how to fit it together yourself, and once it's all done, isn't it pretty?

In this chapter we will discuss the proof-writing techniques that mathematicians use most often and explain how to use them to begin writing proofs yourself. Understanding these techniques may also help you read and understand proofs written by other people. Unfortunately, the techniques in this chapter do not give a step-by-step procedure for solving every proof problem. When trying to write a proof you may make a few false starts before finding the right way to proceed, and some proofs may require some cleverness or insight. With practice your proof-writing skills should improve, and you'll be able to tackle more and more challenging proofs.

Mathematicians usually state the answer to a mathematical question in the form of a *theorem* that says that if certain assumptions called the *hypotheses* of the theorem are true, then some conclusion must also be true. Often the hypotheses and conclusion contain free variables, and in this case it is understood that these variables can stand for any elements of the universe of discourse. An assignment of particular values to these variables is called an *instance* of the theorem, and in order for the theorem to be correct it must be the case that for every instance of the theorem that makes the hypotheses come out true, the conclusion is also true. If there is even one instance in which the hypotheses are true but the conclusion is false, then the theorem is incorrect. Such an instance is called a *counterexample* to the theorem.

Example 3.1.1. Consider the following theorem:

Theorem. *Suppose* $x > 3$ *and* $y < 2$. *Then* $x^2 - 2y > 5$.

This theorem is correct. (You are asked to prove it in exercise 14.) The hypotheses of the theorem are $x > 3$ and $y < 2$, and the conclusion is $x^2 - 2y > 5$. As an instance of the theorem, we could plug in 5 for x and 1 for y. Clearly with these values of the variables the hypotheses $x > 3$ and $y < 2$ are both true, so the theorem tells us that the conclusion $x^2 - 2y > 5$ must also be true. In fact, plugging in the values of x and y we find that $x^2 - 2y = 25 - 2 = 23$, and certainly $23 > 5$. Note that this calculation does not constitute a proof of the theorem. We have only checked one instance of the theorem, and a proof would have to show that *all* instances are correct.

If we drop the second hypothesis, then we get an incorrect theorem:

Incorrect Theorem. *Suppose* $x > 3$. *Then* $x^2 - 2y > 5$.

We can see that this theorem is incorrect by finding a counterexample. For example, suppose we let $x = 4$ and $y = 6$. Then the only remaining hypothesis, $x > 3$, is true, but $x^2 - 2y = 16 - 12 = 4$, so the conclusion $x^2 - 2y > 5$ is false.

If you find a counterexample to a theorem, then you can be sure that the theorem is incorrect, but the only way to know for sure that a theorem is correct is to prove it. A proof of a theorem is simply a deductive argument whose premises are the hypotheses of the theorem and whose conclusion is the conclusion of the theorem. Of course the argument should be valid, so we can be sure that if the hypotheses of the theorem are true, then the conclusion must be true as well. How you figure out and write up the proof of a theorem will depend mostly on the logical form of the conclusion. Often it will also depend on the logical forms of the hypotheses. The proof-writing techniques we will discuss in this chapter will tell you which proof strategies are most likely to work for various forms of hypotheses and conclusions.

Proof-writing techniques that are based on the logical forms of the hypotheses usually suggest ways of drawing inferences from the hypotheses. When you draw an inference from the hypotheses, you use the assumption that the hypotheses are true to justify the assertion that some other statement is also true. Once you have shown that a statement is true, you can use it later in the proof exactly as if it were a hypothesis. Perhaps the most important rule to keep in mind when drawing such inferences is this: *Never assert anything until you can justify it completely* using the hypotheses or using conclusions reached from them earlier in the proof. Your motto should be: “I shall make no assertion before its time.” Following this rule will prevent you from using circular reasoning or jumping to conclusions and will guarantee that, if the hypotheses are true, then the conclusion must also be true. And this is the primary purpose of any proof: to provide a guarantee that the conclusion is true if the hypotheses are.

To make sure your assertions are adequately justified, you must be skeptical about every inference in your proof. If there is any doubt in your mind about whether the justification you have given for an assertion is adequate, then it isn’t. After all, if your own reasoning doesn’t even convince *you*, how can you expect it to convince anybody else?

Proof-writing techniques based on the logical form of the conclusion are often somewhat different from techniques based on the forms of the hypotheses. They usually suggest ways of transforming the problem into one that is equivalent but easier to solve. The idea of solving a problem by transforming it into an easier problem should be familiar to you. For example, adding the same number to both sides of an equation transforms the equation into an equivalent equation, and the resulting equation is sometimes easier to solve than the original one. Students who have studied calculus may be familiar with techniques of evaluating integrals, such as substitution or integration by parts, that can be used to transform a difficult integration problem into an easier one.

Proofs that are written using these transformation strategies often include steps in which you assume for the sake of argument that some statement is true without providing any justification for that assumption. It may seem at first that such reasoning would violate the rule that assertions must always be justified, but it doesn't, because *assuming* something is not the same as *asserting* it. To assert a statement is to claim that it is true, and such a claim is never acceptable in a proof unless it can be justified. However, the purpose of making an assumption in a proof is not to make a claim about what *is* true, but rather to enable you to find out what *would be* true *if* the assumption were correct. You must always keep in mind that any conclusion you reach that is based on an assumption might turn out to be false if the assumption is incorrect. Whenever you make a statement in a proof, it's important to be sure you know whether it's an assertion or an assumption.

Perhaps an example will help clarify this. Suppose during the course of a proof you decide to assume that some statement, call it P, is true, and you use this assumption to conclude that another statement Q is true. It would be wrong to call this a proof that Q is true, because you can't be sure that your assumption about the truth of P was correct. All you can conclude at this point is that *if* P is true, then you can be sure that Q is true as well. In other words, you know that the statement $P \rightarrow Q$ is true. If the conclusion of the theorem being proven was Q, then the proof is incomplete at best. But if the conclusion was $P \rightarrow Q$, then the proof is complete. This brings us to our first proof strategy.

To prove a conclusion of the form $P \rightarrow Q$:
Assume P is true and then prove Q.

Here's another way of looking at what this proof technique means. Assuming that P is true amounts to the same thing as adding P to your list of hypotheses. Although P might not originally have been one of your hypotheses, once you have assumed it, you can use it exactly the way you would use any other hypothesis. Proving Q means treating Q as your conclusion and forgetting about the original conclusion. So this technique says that if the conclusion of the theorem you are trying to prove has the form $P \rightarrow Q$, then you can *transform the problem* by adding P to your list of hypotheses and changing your conclusion from $P \rightarrow Q$ to Q. This gives you a new, perhaps easier proof problem to work on. If you can solve the new problem, then you will have shown that *if* P is true then Q is also true, thus solving the original problem of proving $P \rightarrow Q$. How you solve this new problem will now be guided by the logical form of the new conclusion Q (which might itself be a complex statement), and perhaps also by the logical form of the new hypothesis P.

Note that this technique doesn't tell you how to do the whole proof, it just gives you one step, leaving you with a new problem to solve in order to finish the proof. Proofs are usually not written all at once, but are created gradually by applying several proof techniques one after another. Often the use of these techniques will lead you to transform the problem several times. In discussing this process it will be helpful to have some way to keep track of the results of this sequence of transformations. We therefore introduce the following terminology. We will refer to the statements that are known or assumed to be true at some point in the course of figuring out a proof as *givens*, and the statement that remains to be proven at that point as the *goal*. When you are starting to figure out a proof, the givens will be just the hypotheses of the theorem you are proving, but they may later include other statements that have been inferred from the hypotheses or added as new assumptions as the result of some transformation of the problem. The goal will initially be the conclusion of the theorem, but it may be changed several times in the course of figuring out a proof.

To keep in mind that all of our proof strategies apply not only to the original proof problem but also to the results of any transformation of the problem, we will talk from now on only about givens and goals, rather than hypotheses and conclusions, when discussing proof-writing strategies. For example, the strategy stated earlier should really be called a strategy for proving a *goal* of the form $P \rightarrow Q$, rather than a conclusion of this form. Even if the conclusion of the theorem you are proving is not a conditional statement, if you transform the problem in such a way that a conditional statement becomes the goal, then you can apply this strategy as the next step in figuring out the proof.

Example 3.1.2. Suppose a and b are real numbers. Prove that if $0 < a < b$ then $a^2 < b^2$.

Scratch work

We are given as a hypothesis that a and b are real numbers. Our conclusion has the form $P \rightarrow Q$, where P is the statement $0 < a < b$ and Q is the statement

$a^2 < b^2$. Thus we start with these statements as given and goal:

Givens	*Goal*
a and b are real numbers	$(0 < a < b) \rightarrow (a^2 < b^2)$

According to our proof technique we should assume that $0 < a < b$ and try to use this assumption to prove that $a^2 < b^2$. In other words, we transform the problem by adding $0 < a < b$ to the list of givens and making $a^2 < b^2$ our goal:

Givens	*Goal*
a and b are real numbers	$a^2 < b^2$
$0 < a < b$	

Comparing the inequalities $a < b$ and $a^2 < b^2$ suggests that multiplying both sides of the given inequality $a < b$ by either a or b might get us closer to our goal. Because we are given that a and b are positive, we won't need to reverse the direction of the inequality if we do this. Multiplying $a < b$ by a gives us $a^2 < ab$, and multiplying it by b gives us $ab < b^2$. Thus $a^2 < ab < b^2$, so $a^2 < b^2$.

Solution

Theorem. *Suppose a and b are real numbers. If* $0 < a < b$ *then* $a^2 < b^2$.

Proof. Suppose $0 < a < b$. Multiplying the inequality $a < b$ by the positive number a we can conclude that $a^2 < ab$, and similarly multiplying by b we get $ab < b^2$. Therefore $a^2 < ab < b^2$, so $a^2 < b^2$, as required. Thus, if $0 < a < b$ then $a^2 < b^2$. □

As you can see from the preceding example, there's a difference between the reasoning you use when you are figuring out a proof and the steps you write down when you write the final version of the proof. In particular, although we will often talk about givens and goals when trying to figure out a proof, the final write-up will rarely refer to them. Throughout this chapter, and sometimes in later chapters as well, we will precede our proofs with the scratch work used to figure out the proof, but this is just to help you understand how proofs are constructed. When mathematicians write proofs, they usually just write the steps needed to justify their conclusions with no explanation of how they thought of them. Some of these steps will be sentences indicating that the problem has been transformed (usually according to some proof strategy based on the logical form of the goal); some steps will be assertions that are justified by inferences from the givens (often using some proof strategy based on the logical form of a given). However, there will usually be no explanation of how the mathematician thought of these transformations and inferences. For example, the proof in Example 3.1.2 starts with the sentence "Suppose $0 < a < b$," indicating that the problem has been transformed according to our strategy, and then proceeds with a sequence of inferences leading to the conclusion that $a^2 < b^2$. No other explanations were necessary to justify the final conclusion, in the last sentence, that if $0 < a < b$ then $a^2 < b^2$.

Although this lack of explanation sometimes makes proofs hard to read, it serves the purpose of keeping two distinct objectives separate: *explaining your thought processes* and *justifying your conclusions*. The first is psychology; the second, mathematics. The primary purpose of a proof is to justify the claim that the conclusion follows from the hypotheses, and no explanation of your thought processes can substitute for adequate justification of this claim. Keeping any discussion of thought processes to a minimum in a proof helps to keep this distinction clear. Occasionally, in a very complicated proof, a mathematician may include some discussion of the strategy behind the proof to make the proof easier to read. Usually, however, it is up to readers to figure this out for themselves. Don't worry if you don't immediately understand the strategy behind a proof you are reading. Just try to follow the justifications of the steps, and the strategy will eventually become clear. If it doesn't, a second reading of the proof might help.

To keep the distinction between the proof and the strategy behind the proof clear, in the future when we state a proof strategy we will often describe both the scratch work you might use to figure out the proof and the form that the final write-up of the proof should take. For example, here's a restatement of the proof strategy we discussed earlier, in the form we will be using to present proof strategies from now on.

To prove a goal of the form $P \to Q$:
Assume P is true and then prove Q.

Scratch work

Before using strategy:

Givens	*Goal*
—	$P \to Q$
—	

After using strategy:

Givens	*Goal*
—	Q
—	
P	

Form of final proof:

Suppose P.
[Proof of Q goes here.]
Therefore $P \to Q$.

Note that the suggested form for the final proof tells you how the beginning and end of the proof will go, but more steps will have to be added in the middle. The givens and goal list under the heading "After using strategy" tells you what is known or can be assumed and what needs to be proven in order to fill in this gap in the proof. Many of our proof strategies will tell you how to write either the beginning or the end of your proof, leaving a gap to be filled in with further reasoning.

There is a second method that is sometimes used for proving goals of the form $P \to Q$. Because any conditional statement $P \to Q$ is equivalent to its contrapositive $\neg Q \to \neg P$, you can prove $P \to Q$ by proving $\neg Q \to \neg P$ instead, using the strategy discussed earlier. In other words:

To prove a goal of the form $P \to Q$:
Assume Q is false and prove that P is false.

Scratch work

Before using strategy:

Givens	*Goal*
—	$P \to Q$
—	

After using strategy:

Givens	*Goal*
—	$\neg P$
—	
$\neg Q$	

Form of final proof:

Suppose Q is false.
[Proof of $\neg P$ goes here.]
Therefore $P \to Q$.

Example 3.1.3. Suppose *a, b,* and c are real numbers and $a > b$. Prove that if $ac \leq bc$ then $c \leq 0$.

Scratch work

Givens	*Goal*
a, b, and c are real numbers	$(ac \leq bc) \rightarrow (c \leq 0)$
$a > b$	

The contrapositive of the goal is $\neg(c \leq 0) \rightarrow \neg(ac \leq bc)$, or in other words $(c > 0) \rightarrow (ac > bc)$, so we can prove it by adding $c > 0$ to the list of givens and making $ac > bc$ our new goal:

Givens	*Goal*
a, b, and c are real numbers	$ac > bc$
$a > b$	
$c > 0$	

We can also now write the first and last sentences of the proof. According to the strategy, the final proof should have this form:

> Suppose $c > 0$.
>   [Proof of $ac > bc$ goes here.]
> Therefore, if $ac \leq bc$ then $c \leq 0$.

Using the new given $c > 0$, we see that the goal $ac > bc$ follows immediately from the given $a > b$ by multiplying both sides by the positive number c. Inserting this step between the first and last sentences completes the proof.

Solution

Theorem. *Suppose a, b, and c are real numbers and $a > b$. If $ac \leq bc$ then $c \leq 0$.*

Proof. We will prove the contrapositive. Suppose $c > 0$. Then we can multiply both sides of the given inequality $a > b$ by c and conclude that $ac > bc$. Therefore, if $ac \leq bc$ then $c \leq 0$. □

Notice that, although we have used the symbols of logic freely in the scratch work, we have not used them in the final write-up of the proof. Although it would not be incorrect to use logical symbols in a proof, mathematicians usually try to avoid it. Using the notation and rules of logic can be very helpful when you are figuring out the strategy for a proof, but in the final write-up you should try to stick to ordinary English as much as possible.

The reader may be wondering how we knew in Example 3.1.3 that we should use the second method for proving a goal of the form $P \rightarrow Q$

rather than the first. The answer is simple: We tried both methods, and the second worked. When there is more than one strategy for proving a goal of a particular form, you may have to try a few different strategies before you hit on one that works. With practice, you will get better at guessing which strategy is most likely to work for a particular proof.

Notice that in each of the examples we have given our strategy involved making changes in our givens and goal to try to make the problem easier. The beginning and end of the proof, which were supplied for us in the statement of the proof technique, serve to tell a reader of the proof that these changes have been made and how the solution to this revised problem solves the original problem. The rest of the proof contains the solution to this easier, revised problem.

Most of the other proof techniques in this chapter also suggest that you revise your givens and goal in some way. These revisions result in a new proof problem, and in every case the revisions have been designed so that a solution to the new problem, when combined with some beginning or ending sentences explaining these revisions, would also solve the original problem. This means that whenever you use one of these strategies you can write a sentence or two at the beginning or end of the proof and then forget about the original problem and work instead on the new problem, which will usually be easier. Often you will be able to figure out a proof by using the techniques in this chapter to revise your givens and goal repeatedly, making the remaining problem easier and easier until you reach a point at which it is completely obvious that the goal follows from the givens.

Exercises

*1. Consider the following theorem. (This theorem was proven in the introduction.)

Theorem. *Suppose n is an integer larger than 1 and n is not prime. Then* $2^n - 1$ *is not prime.*

(a) Identify the hypotheses and conclusion of the theorem. Are the hypotheses true when $n = 6$? What does the theorem tell you in this instance? Is it right?

(b) What can you conclude from the theorem in the case $n = 15$? Check directly that this conclusion is correct.

(c) What can you conclude from the theorem in the case $n = 11$?

2. Consider the following theorem. (The theorem is correct, but we will not ask you to prove it here.)

Theorem. *Suppose that* $b^2 > 4ac$*. Then the quadratic equation* $ax^2 + bx + c = 0$ *has exactly two real solutions.*

(a) Identify the hypotheses and conclusion of the theorem.
(b) To give an instance of the theorem, you must specify values for a, b, and c, but not x. Why?
(c) What can you conclude from the theorem in the case $a = 2, b = -5$, $c = 3$? Check directly that this conclusion is correct.
(d) What can you conclude from the theorem in the case $a = 2$, $b = 4$, $c = 3$?

3. Consider the following incorrect theorem:

Incorrect Theorem. *Suppose n is a natural number larger than 2, and n is not a prime number. Then 2n + 13 is not a prime number.*

What are the hypotheses and conclusion of this theorem? Show that the theorem is incorrect by finding a counterexample.

*4. Complete the following alternative proof of the theorem in Example 3.1.2.

Proof. Suppose $0 < a < b$. Then $b - a > 0$.
[Fill in a proof of $b^2 - a^2 > 0$ here.]
Since $b^2 - a^2 > 0$, it follows that $a^2 < b^2$. Therefore if $0 < a < b$ then $a^2 < b^2$. □

5. Suppose a and b are real numbers. Prove that if $a < b < 0$ then $a^2 > b^2$.
6. Suppose a and b are real numbers. Prove that if $0 < a < b$ then $1/b < 1/a$.
7. Suppose that a is a real number. Prove that if $a^3 > a$ then $a^5 > a$. (Hint: One approach is to start by completing the following equation: $a^5 - a = (a^3 - a) \cdot \underline{\ ?\ }$.)
8. Suppose $A \setminus B \subseteq C \cap D$ and $x \in A$. Prove that if $x \notin D$ then $x \in B$.

*9. Suppose a and b are real numbers. Prove that if $a < b$ then $\frac{a+b}{2} < b$.

10. Suppose x is a real number and $x \neq 0$. Prove that if $\frac{\sqrt[3]{x}+5}{x^2+6} = \frac{1}{x}$ then $x \neq 8$.

*11. Suppose a, b, c, and d are real numbers, $0 < a < b$, and $d > 0$. Prove that if $ac \geq bd$ then $c > d$.

12. Suppose x and y are real numbers, and $3x + 2y \leq 5$. Prove that if $x > 1$ then $y < 1$.
13. Suppose that x and y are real numbers. Prove that if $x^2 + y = -3$ and $2x - y = 2$ then $x = -1$.

*14. Prove the first theorem in Example 3.1.1. (Hint: You might find it useful to apply the theorem from Example 3.1.2.)

15. Consider the following theorem.

    Theorem. *Suppose x is a real number and $x \neq 4$. If $\frac{2x-5}{x-4} = 3$ then $x = 7$.*

    (a) What's wrong with the following proof of the theorem?

    Proof. Suppose $x = 7$. Then $\frac{2x-5}{x-4} = \frac{2(7)-5}{7-4} = \frac{9}{3} = 3$. Therefore if $\frac{2x-5}{x-4} = 3$ then $x = 7$. □

    (b) Give a correct proof of the theorem.

16. Consider the following incorrect theorem:

    Incorrect Theorem. *Suppose that x and y are real numbers and $x \neq 3$. If $x^2y = 9y$ then $y = 0$.*

    (a) What's wrong with the following proof of the theorem?

    Proof. Suppose that $x^2y = 9y$. Then $(x^2 - 9)y = 0$. Since $x \neq 3$, $x^2 \neq 9$, so $x^2 - 9 \neq 0$. Therefore we can divide both sides of the equation $(x^2 - 9)y = 0$ by $x^2 - 9$, which leads to the conclusion that $y = 0$. Thus, if $x^2y = 9y$ then $y = 0$. □

    (b) Show that the theorem is incorrect by finding a counterexample.

3.2. Proofs Involving Negations and Conditionals

We turn now to proofs in which the goal has the form $\neg P$. Usually it's easier to prove a positive than a negative statement, so it is often helpful to reexpress a goal of the form $\neg P$ before proving it. Instead of using a goal that says what *shouldn't* be true, see if you can rephrase it as a goal that says what *should* be true. Fortunately, we have already studied several equivalences that will help with this reexpression. Thus, our first strategy for proving negated statements is:

To prove a goal of the form $\neg P$:

If possible, reexpress the goal in some other form and then use one of the proof strategies for this other goal form.

Example 3.2.1. Suppose $A \cap C \subseteq B$ and $a \in C$. Prove that $a \notin A \setminus B$.

Scratch Work

Givens	*Goal*
$A \cap C \subseteq B$	$a \notin A \setminus B$
$a \in C$	

Because the goal is a negated statement, we try to reexpress it:

$a \notin A \setminus B$ is equivalent to $\neg(a \in A \wedge a \notin B)$ (definition of $A \setminus B$),
which is equivalent to $a \notin A \vee a \in B$ (DeMorgan's law),
which is equivalent to $a \in A \rightarrow a \in B$ (conditional law).

Rewriting the goal in this way gives us:

Givens	*Goal*
$A \cap C \subseteq B$	$a \in A \rightarrow a \in B$
$a \in C$	

We now prove the goal in this new form, using the first strategy from Section 3.1. Thus, we add $a \in A$ to our list of givens and make $a \in B$ our goal:

Givens	*Goal*
$A \cap C \subseteq B$	$a \in B$
$a \in C$	
$a \in A$	

The proof is now easy: From the givens $a \in A$ and $a \in C$ we can conclude that $a \in A \cap C$, and then, since $A \cap C \subseteq B$, it follows that $a \in B$.

Solution

Theorem. *Suppose $A \cap C \subseteq B$ and $a \in C$. Then $a \notin A \setminus B$.*
Proof. Suppose $a \in A$. Then since $a \in C$, $a \in A \cap C$. But then since $A \cap C \subseteq B$ it follows that $a \in B$. Thus, it cannot be the case that a is an element of A but not B, so $a \notin A \setminus B$. □

Sometimes a goal of the form $\neg P$ cannot be reexpressed as a positive statement, and therefore this strategy cannot be used. In this case it is usually best to do a *proof by contradiction*. Start by assuming that P is true, and try to use this assumption to prove something that you know is false. Often this is done by proving a statement that contradicts one of the givens. Because you know that the statement you have proven is false, the assumption that P was true must have been incorrect. The only remaining possibility then is that P is false.

To prove a goal of the form $\neg P$:

Assume P is true and try to reach a contradiction. Once you have reached a contradiction, you can conclude that P must be false.

Scratch work

Before using strategy:

Givens	*Goal*
—	$\neg P$
—	

After using strategy:

Givens	*Goal*
—	Contradiction
—	
P	

Form of final proof:

Suppose P is true.
[Proof of contradiction goes here.]
Thus, P is false.

Example 3.2.2. Prove that if $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.

Scratch work

The goal is a conditional statement, so according to the first proof strategy in Section 3.1 we can treat the antecedent as given and make the consequent our new goal:

Givens	*Goal*
$x^2 + y = 13$	$x \neq 3$
$y \neq 4$	

This proof strategy also suggests what form the final proof should take. According to the strategy, the proof should look like this:

Suppose $x^2 + y = 13$ and $y \neq 4$.
[Proof of $x \neq 3$ goes here.]
Thus, if $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.

In other words, the first and last sentences of the final proof have already been written, and the problem that remains to be solved is to fill in a proof of $x \neq 3$

between these two sentences. The givens–goal list summarizes what we know and what we have to prove in order to solve this problem.

The goal $x \neq 3$ means $\neg(x = 3)$, but because $x = 3$ has no logical connectives in it, none of the equivalences we know can be used to reexpress this goal in a positive form. We therefore try proof by contradiction and transform the problem as follows:

Givens	*Goal*
$x^2 + y = 13$	Contradiction
$y \neq 4$	
$x = 3$	

Once again, the proof strategy that suggested this transformation also tells us how to fill in a few more sentences of the final proof. As we indicated earlier, these sentences go between the first and last sentences of the proof, which were written before.

> Suppose $x^2 + y = 13$ and $y \neq 4$.
>
> > Suppose $x = 3$.
> >
> > > [Proof of contradiction goes here.]
> >
> > Therefore $x \neq 3$.
>
> Thus, if $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.

The indenting in this outline of the proof will not be part of the final proof. We have done it here to make the underlying structure of the proof clear. The first and last lines go together and indicate that we are proving a conditional statement by assuming the antecedent and proving the consequent. Between these lines is a proof of the consequent, $x \neq 3$, which we have set off from the first and last lines by indenting it. This inner proof has the form of a proof by contradiction, as indicated by its first and last lines. Between these lines we still need to fill in a proof of a contradiction.

At this point we don't have a particular statement as our goal; any impossible conclusion will do. We must therefore look more closely at the givens to see if some of them contradict others. In this case, the first and third together imply that $y = 4$, which contradicts the second.

Solution

Theorem. *If* $x^2 + y = 13$ *and* $y \neq 4$ *then* $x \neq 3$.

Proof. Suppose $x^2 + y = 13$ and $y \neq 4$. Suppose $x = 3$. Substituting this into the equation $x^2 + y = 13$, we get $9 + y = 13$, so $y = 4$. But this contradicts the fact that $y \neq 4$. Therefore $x \neq 3$. Thus, if $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$. □

You may be wondering at this point why we were justified in concluding, when we reached a contradiction in the proof, that $x \neq 3$. After all, the second list of givens in our scratch work contained three given. How could we be sure, when we reached a contradiction, that the culprit was the third given, $x = 3$? To answer this question, look back at the first givens and goal analysis for this example. According to that analysis, there were two givens, $x^2 + y = 13$ and $y \neq 4$, from which we had to prove the goal $x \neq 3$. Remember that a proof only has to guarantee that the goal is true *if* the givens are. Thus, we didn't have to show that $x \neq 3$, only that *if* $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$. When we reached a contradiction, we knew that one of the three statements in the second list of givens had to be false. We didn't try to figure out which one it was because we didn't need to. We were certainly justified in concluding that *if* neither of the first two was the culprit, then it had to be the third, and that was all that was required to finish the proof.

Proving a goal by contradiction has the advantage that it allows you to assume that your conclusion is false, providing you with another given to work with. But it has the disadvantage that it leaves you with a rather vague goal: produce a contradiction by proving something that you know is false. Because all the proof strategies we have discussed so far depend on analyzing the logical form of the goal, it appears that none of them will help you to achieve the goal of producing a contradiction. In the preceding proof we were forced to look more closely at our givens to find a contradiction. In this case we did it by proving that $y = 4$, contradicting the given $y \neq 4$. This illustrates a pattern that occurs often in proofs by contradiction: If one of the givens has the form $\neg P$, then you can produce a contradiction by proving P. This is our first strategy based on the logical form of a *given*.

To use a given of the form $\neg P$:

If you're doing a proof by contradiction, try making P your goal. If you can prove P, then the proof will be complete, because P contradicts the given $\neg P$.

Scratch work

Before using strategy:

Givens	*Goal*
$\neg P$	Contradiction
—	
—	

After using strategy:

Givens	*Goal*
$\neg P$	P
—	
—	

Form of final proof:

[Proof of P goes here.]
Since we already know $\neg P$, this is a contradiction.

Although we have recommended proof by contradiction for proving goals of the form $\neg P$, it can be used for any goal. Usually it's best to try the other strategies first if any of them apply; but if you're stuck, you can try proof by contradiction in any proof.

The next example illustrates this and also another important rule of proof-writing: In many cases the logical form of a statement can be discovered by *writing out the definition* of some mathematical word or symbol that occurs in the statement. For this reason, knowing the precise statements of the definitions of all mathematical terms is extremely important when you're writing a proof.

Example 3.2.3. Suppose *A, B,* and C are sets, $A \setminus B \subseteq C$, and x is anything at all. Prove that if $x \in A \setminus C$ then $x \in B$.

Scratch work

We're given that $A \setminus B \subseteq C$, and our goal is $x \in A \setminus C \to x \in B$. Because the goal is a conditional statement, our first step is to transform the problem by adding $x \in A \setminus C$ as a second given and making $x \in B$ our goal:

Givens	*Goal*
$A \setminus B \subseteq C$	$x \in B$
$x \in A \setminus C$	

The form of the final proof will therefore be as follows:

Suppose $x \in A \setminus C$.
[Proof of $x \in B$ goes here.]
Thus, if $x \in A \setminus C$ then $x \in B$.

The goal $x \in B$ contains no logical connectives, so none of the techniques we have studied so far apply, and it is not obvious why the goal follows from the givens. Lacking anything else to do, we try proof by contradiction:

Givens	*Goal*
$A \setminus B \subseteq C$	Contradiction
$x \in A \setminus C$	
$x \notin B$	

As before, this transformation of the problem also enables us to fill in a few more sentences of the proof:

Suppose $x \in A \setminus C$.
  Suppose $x \notin B$.
    [Proof of contradiction goes here.]
  Therefore $x \in B$.
Thus, if $x \in A \setminus C$ then $x \in B$.

Because we're doing a proof by contradiction and our last given is now a negated statement, we could try using our strategy for using givens of the form $\neg P$. Unfortunately, this strategy suggests making $x \in B$ our goal, which just gets us back to where we started. We must look at the other givens to try to find the contradiction.

In this case, writing out the definition of the second given is the key to the proof, since this definition also contains a negated statement. By definition, $x \in A \setminus C$ means $x \in A$ and $x \notin C$. Replacing this given by its definition gives us:

Givens	*Goal*
$A \setminus B \subseteq C$	Contradiction
$x \in A$	
$x \notin C$	
$x \notin B$	

Now the third given also has the form $\neg P$, where P is the statement $x \in C$, so we can apply the strategy for using givens of the form $\neg P$ and make $x \in C$ our goal. Showing that $x \in C$ would complete the proof because it would contradict the given $x \notin C$.

Givens	*Goal*
$A \setminus B \subseteq C$	$x \in C$
$x \in A$	
$x \notin C$	
$x \notin B$	

Once again, we can add a little more to the proof we are gradually writing by filling in the fact that we plan to derive our contradiction by proving $x \in C$.

We also add the definition of $x \in A \setminus C$ to the proof, inserting it in what seems like the most logical place, right after we stated that $x \in A \setminus C$:

> Suppose $x \in A \setminus C$. This means that $x \in A$ and $x \notin C$.
>   Suppose $x \notin B$.
>   [Proof of $x \in C$ goes here.]
>   This contradicts the fact that $x \notin C$.
>   Therefore $x \in B$.
> Thus, if $x \in A \setminus C$ then $x \in B$.

We have finally reached a point where the goal follows easily from the givens. From $x \in A$ and $x \notin B$ we conclude that $x \in A \setminus B$. Since $A \setminus B \subseteq C$ it follows that $x \in C$.

Solution

Theorem. *Suppose A, B, and C are sets, $A \setminus B \subseteq C$, and x is anything at all. If $x \in A \setminus C$ then $x \in B$.*

Proof. Suppose $x \in A \setminus C$. This means that $x \in A$ and $x \notin C$. Suppose $x \notin B$. Then $x \in A \setminus B$, so since $A \setminus B \subseteq C$, $x \in C$. But this contradicts the fact that $x \notin C$. Therefore $x \in B$. Thus, if $x \in A \setminus C$ then $x \in B$. □

The strategy we've recommended for using givens of the form $\neg P$ only applies if you are doing a proof by contradiction. For other kinds of proofs, the next strategy can be used. This strategy is based on the fact that givens of the form $\neg P$, like goals of this form, may be easier to work with if they are reexpressed as positive statements.

To use a given of the form $\neg P$:

If possible, reexpress this given in some other form.

We have discussed strategies for working with both givens and goals of the form $\neg P$, but only strategies for goals of the form $P \to Q$. We now fill this gap by giving two strategies for using givens of the form $P \to Q$. We said before that many strategies for using givens suggest ways of drawing inferences from the givens. Such strategies are called *rules of inference*. Both of our strategies for using givens of the form $P \to Q$ are examples of rules of inference.

To use a given of the form $P \to Q$:

If you are also given P, or if you can prove that P is true, then you can use this given to conclude that Q is true. Since it is equivalent to $\neg Q \to \neg P$, if you can prove that Q is false, you can use this given to conclude that P is false.

The first of these rules of inference says that if you know that both P and $P \to Q$ are true, you can conclude that Q must also be true. Logicians call this rule *modus ponens*. We saw this rule used in one of our first examples of valid deductive reasoning in Chapter 1, argument 2 in Example 1.1.1. The validity of this form of reasoning was verified using the truth table for the conditional connective in Section 1.5.

The second rule, called *modus tollens*, says that if you know that $P \to Q$ is true and Q is false, you can conclude that P must also be false. The validity of this rule can also be checked with truth tables, as you are asked to show in exercise 13. Usually you won't find a given of the form $P \to Q$ to be much use until you are able to prove either P or $\neg Q$. However, if you ever reach a point in your proof where you have determined that P is true, you should probably use this given immediately to conclude that Q is true. Similarly, if you ever establish $\neg Q$, immediately use this given to conclude $\neg P$.

Although most of our examples will involve specific mathematical statements, occasionally we will do examples of proofs containing letters standing for unspecified statements. Later in this chapter we will be able to use this method to verify some of the equivalences from Chapter 2 that could only be justified on intuitive grounds before. Here's an example of this kind, illustrating the use of modus ponens and modus tollens.

Example 3.2.4. Suppose $P \to (Q \to R)$. Prove that $\neg R \to (P \to \neg Q)$.

Scratch work

This could actually be done with a truth table, as you are asked to show in exercise 14, but let's do it using the proof strategies we've been discussing. We start with the following situation:

Givens	*Goal*
$P \to (Q \to R)$	$\neg R \to (P \to \neg Q)$

Our only given is a conditional statement. By the rules of inference just discussed, if we knew P we could use modus ponens to conclude $Q \to R$, and if we knew $\neg(Q \to R)$ we could use modus tollens to conclude $\neg P$. Because we don't, at this point, know either of these, we can't yet do anything with this given. If either P or $\neg(Q \to R)$ ever gets added to the givens list, then we should consider using modus ponens or modus tollens. For now, we need to concentrate on the goal.

The goal is also a conditional statement, so we assume the antecedent and set the consequent as our new goal:

Givens	*Goal*
$P \rightarrow (Q \rightarrow R)$	$P \rightarrow \neg Q$
$\neg R$	

We can also now write a little bit of the proof:

Suppose $\neg R$.
[Proof of $P \rightarrow \neg Q$ goes here.]
Therefore $\neg R \rightarrow (P \rightarrow \neg Q)$.

We still can't do anything with the givens, but the goal is another conditional, so we use the same strategy again:

Givens	*Goal*
$P \rightarrow (Q \rightarrow R)$	$\neg Q$
$\neg R$	
P	

Now the proof looks like this:

Suppose $\neg R$.
Suppose P.
[Proof of $\neg Q$ goes here.]
Therefore $P \rightarrow \neg Q$.
Therefore $\neg R \rightarrow (P \rightarrow \neg Q)$.

We've been watching for our chance to use our first given by applying either modus ponens or modus tollens, and now we can do it. Since we know $P \rightarrow (Q \rightarrow R)$ and P, by modus ponens we can infer $Q \rightarrow R$. Any conclusion inferred from the givens can be added to the givens column:

Givens	*Goal*
$P \rightarrow (Q \rightarrow R)$	$\neg Q$
$\neg R$	
P	
$Q \rightarrow R$	

We also add one more line to the proof:

Suppose $\neg R$.
Suppose P.
Since P and $P \rightarrow (Q \rightarrow R)$, it follows that $Q \rightarrow R$.
[Proof of $\neg Q$ goes here.]
Therefore $P \rightarrow \neg Q$.
Therefore $\neg R \rightarrow (P \rightarrow \neg Q)$.

Finally, our last step is to use modus tollens. We now know $Q \to R$ and $\neg R$, so by modus tollens we can conclude $\neg Q$. This is our goal, so the proof is done.

Solution

Theorem. *Suppose $P \to (Q \to R)$. Then $\neg R \to (P \to \neg Q)$.*
Proof. Suppose $\neg R$. Suppose P. Since P and $P \to (Q \to R)$, it follows that $Q \to R$. But then, since $\neg R$, we can conclude $\neg Q$. Thus, $P \to \neg Q$. Therefore $\neg R \to (P \to \neg Q)$. □

Sometimes if you're stuck you can use rules of inference to work backward. For example, suppose one of your givens has the form $P \to Q$ and your goal is Q. If only you could prove P, you could use modus ponens to reach your goal. This suggests treating P as your goal instead of Q. If you can prove P, then you'll just have to add one more step to the proof to reach your original goal Q.

Example 3.2.5. Suppose that $A \subseteq B$, $a \in A$, and $a \notin B \setminus C$. Prove that $a \in C$.

Scratch work

Givens	*Goal*
$A \subseteq B$	$a \in C$
$a \in A$	
$a \notin B \setminus C$	

Our third given is a negative statement, so we begin by reexpressing it as an equivalent positive statement. According to the definition of the difference of two sets, this given means $\neg(a \in B \wedge a \notin C)$, and by one of DeMorgan's laws, this is equivalent to $a \notin B \vee a \in C$. Because our goal is $a \in C$, it is probably more useful to rewrite this in the equivalent form $a \in B \to a \in C$:

Givens	*Goal*
$A \subseteq B$	$a \in C$
$a \in A$	
$a \in B \to a \in C$	

Now we can use our strategy for using givens of the form $P \to Q$. Our goal is $a \in C$, and we are given that $a \in B \to a \in C$. If we could prove that $a \in B$, then we could use modus ponens to reach our goal. So let's try treating $a \in B$ as our goal and see if that makes the problem easier:

Givens	*Goal*
$A \subseteq B$	$a \in B$
$a \in A$	
$a \in B \rightarrow a \in C$	

Now it is clear how to reach the goal. Since $a \in A$ and $A \subseteq B$, $a \in B$.

Solution

Theorem. *Suppose that $A \subseteq B$, $a \in A$, and $a \notin B \setminus C$. Then $a \in C$.*

Proof. Since $a \in A$ and $A \subseteq B$, we can conclude that $a \in B$. But $a \notin B \setminus C$, so it follows that $a \in C$. □

Exercises

*1. This problem could be solved by using truth tables, but don't do it that way. Instead, use the methods for writing proofs discussed so far in this chapter. (See Example 3.2.4.)
   (a) Suppose $P \rightarrow Q$ and $Q \rightarrow R$ are both true. Prove that $P \rightarrow R$ is true.
   (b) Suppose $\neg R \rightarrow (P \rightarrow \neg Q)$ is true. Prove that $P \rightarrow (Q \rightarrow R)$ is true.

2. This problem could be solved by using truth tables, but don't do it that way. Instead, use the methods for writing proofs discussed so far in this chapter. (See Example 3.2.4.)
   (a) Suppose $P \rightarrow Q$ and $R \rightarrow \neg Q$ are both true. Prove that $P \rightarrow \neg R$ is true.
   (b) Suppose that P is true. Prove that $Q \rightarrow \neg(Q \rightarrow \neg P)$ is true.

3. Suppose $A \subseteq C$, and B and C are disjoint. Prove that if $x \in A$ then $x \notin B$.

4. Suppose that $A \setminus B$ is disjoint from C and $x \in A$. Prove that if $x \in C$ then $x \in B$.

*5. Use the method of proof by contradiction to prove the theorem in Example 3.2.1.

6. Use the method of proof by contradiction to prove the theorem in Example 3.2.5.

7. Suppose that $y + x = 2y - x$, and x and y are not both zero. Prove that $y \neq 0$.

*8. Suppose that a and b are nonzero real numbers. Prove that if $a < 1/a < b < 1/b$ then $a < -1$.

9. Suppose that x and y are real numbers. Prove that if $x^2y = 2x + y$, then if $y \neq 0$ then $x \neq 0$.

10. Suppose that x and y are real numbers. Prove that if $x \neq 0$, then if $y = \frac{3x^2+2y}{x^2+2}$ then $y = 3$.

*11. Consider the following incorrect theorem:

Incorrect Theorem. *Suppose x and y are real numbers and $x + y = 10$. Then $x \neq 3$ and $y \neq 8$.*

(a) What's wrong with the following proof of the theorem?

Proof. Suppose the conclusion of the theorem is false. Then $x = 3$ and $y = 8$. But then $x + y = 11$, which contradicts the given information that $x + y = 10$. Therefore the conclusion must be true. □

(b) Show that the theorem is incorrect by finding a counterexample.

12. Consider the following incorrect theorem:

Incorrect Theorem. *Suppose that $A \subseteq C$, $B \subseteq C$, and $x \in A$. Then $x \in B$.*

(a) What's wrong with the following proof of the theorem?

Proof. Suppose that $x \notin B$. Since $x \in A$ and $A \subseteq C$, $x \in C$. Since $x \notin B$ and $B \subseteq C$, $x \notin C$. But now we have proven both $x \in C$ and $x \notin C$, so we have reached a contradiction. Therefore $x \in B$. □

(b) Show that the theorem is incorrect by finding a counterexample.

13. Use truth tables to show that modus tollens is a valid rule of inference.

*14. Use truth tables to check the correctness of the theorem in Example 3.2.4.

15. Use truth tables to check the correctness of the statements in exercise 1.

16. Use truth tables to check the correctness of the statements in exercise 2.

17. Can the proof in Example 3.2.2 be modified to prove that if $x^2 + y = 13$ and $x \neq 3$ then $y \neq 4$? Explain.

3.3. Proofs Involving Quantifiers

Look again at Example 3.2.3. In that example we said that x could be anything at all, and we proved the statement $x \in A \setminus C \rightarrow x \in B$. Because the reasoning we used would apply no matter what x was, our proof actually shows that $x \in A \setminus C \rightarrow x \in B$ is true for all x. In other words, we can conclude $\forall x(x \in A \setminus C \rightarrow x \in B)$.

This illustrates the easiest and most straightforward way of proving a goal of the form $\forall x P(x)$. If you can give a proof of the goal $P(x)$ that would work no matter what x was, then you can conclude that $\forall x P(x)$ must be true. To make sure that your proof would work for any value of x, it is important to start your proof with no assumptions about x. Mathematicians express this by saying that x must be *arbitrary*. In particular, you must not assume that x is equal to any other object already under discussion in the proof. Thus, if the letter x is already being used in the proof to stand for some particular object, then you cannot use it to stand for an arbitrary object. In this case you must choose a different variable that is not already being used in the proof, say y, and replace the goal $\forall x P(x)$ with the equivalent statement $\forall y P(y)$. Now you can proceed by letting y stand for an arbitrary object and proving $P(y)$.

To prove a goal of the form $\forall x P(x)$:

Let x stand for an arbitrary object and prove $P(x)$. The letter x must be a new variable in the proof. If x is already being used in the proof to stand for something, then you must choose an unused variable, say y, to stand for the arbitrary object, and prove $P(y)$.

Scratch work

Before using strategy:

Givens	*Goal*
—	$\forall x P(x)$
—	

After using strategy:

Givens	*Goal*
—	$P(x)$
—	

Form of final proof:

Let x be arbitrary.

[Proof of $P(x)$ goes here.]

Since x was arbitrary, we can conclude that $\forall x P(x)$.

Example 3.3.1. Suppose A, B, and C are sets, and $A \setminus B \subseteq C$. Prove that $A \setminus C \subseteq B$.

Scratch work

Givens	*Goal*
$A \setminus B \subseteq C$	$A \setminus C \subseteq B$

As usual, we look first at the logical form of the goal to plan our strategy. In this case we must write out the definition of $\subseteq$ to determine the logical form of the goal.

Givens	*Goal*
$A \setminus B \subseteq C$	$\forall x(x \in A \setminus C \rightarrow x \in B)$

Because the goal has the form $\forall x P(x)$, where $P(x)$ is the statement $x \in A \setminus C \rightarrow x \in B$, we will introduce a new variable x into the proof to stand for an arbitrary object and then try to prove $x \in A \setminus C \rightarrow x \in B$. Note that x *is* a new variable in the proof. It appeared in the logical form of the goal as a bound variable, but remember that bound variables don't stand for anything in particular. We have not yet used x as a free variable in any statement, so it has not been used to stand for any particular object. To make sure x is arbitrary we must be careful not to add any assumptions about x to the givens column. However, we do change our goal:

Givens	*Goal*
$A \setminus B \subseteq C$	$x \in A \setminus C \rightarrow x \in B$

According to our strategy, the final proof should look like this:

> Let x be arbitrary.
> [Proof of $x \in A \setminus C \rightarrow x \in B$ goes here.]
> Since x was arbitrary, we can conclude that $\forall x(x \in A \setminus C \rightarrow x \in B)$, so $A \setminus C \subseteq B$.

The problem is now exactly the same as in Example 3.2.3, so the rest of the solution is the same as well. In other words, we can simply insert the proof we wrote in Example 3.2.3 between the first and last sentences of the proof written here.

Solution

Theorem. *Suppose A, B, and C are sets, and $A \setminus B \subseteq C$. Then $A \setminus C \subseteq B$.*

Proof. Let x be arbitrary. Suppose $x \in A \setminus C$. This means that $x \in A$ and $x \notin C$. Suppose $x \notin B$. Then $x \in A \setminus B$, so since $A \setminus B \subseteq C, x \in C$. But this contradicts the fact that $x \notin C$. Therefore $x \in B$. Thus, if $x \in A \setminus C$ then $x \in B$. Since x was arbitrary, we can conclude that $\forall x(x \in A \setminus C \rightarrow x \in B)$, so $A \setminus C \subseteq B$. □

Notice that, although this proof shows that every element of $A \setminus C$ is also an element of B, it does not contain phrases such as "every element of $A \setminus C$" or "all elements of $A \setminus C$." For most of the proof we simply reason about x, which is treated as a single, fixed element of $A \setminus C$. We pretend that x stands for some particular element of $A \setminus C$, being careful to make no assumptions about *which* element it stands for. It is only at the end of the proof that we observe that, because x was arbitrary, our conclusions about x would be true no matter what x was. This is the main advantage of using this strategy to prove a goal of the form $\forall x P(x)$. It enables you to prove a goal about *all* objects by reasoning about only *one* object, as long as that object is arbitrary. If you are proving a goal of the form $\forall x P(x)$ and you find yourself saying a lot about "all x's" or "every x," you are probably making your proof unnecessarily complicated by not using this strategy.

As we saw in Chapter 2, statements of the form $\forall x(P(x) \rightarrow Q(x))$ are quite common in mathematics. It might be worthwhile, therefore, to consider how the strategies we've discussed can be combined to prove a goal of this form. Because the goal starts with $\forall x$, the first step is to let x be arbitrary and try to prove $P(x) \rightarrow Q(x)$. To prove this goal, you will probably want to assume that $P(x)$ is true and prove $Q(x)$. Thus, the proof will probably start like this: "Let x be arbitrary. Suppose $P(x)$." It will then proceed with the steps needed to reach the goal $Q(x)$. Often in this type of proof the statement that x is arbitrary is left out, and the proof simply starts with "Suppose $P(x)$." When a new variable x is introduced into a proof in this way, it is usually understood that x is arbitrary. In other words, no assumptions are being made about x other than the stated one that $P(x)$ is true.

An important example of this type of proof is a proof in which the goal has the form $\forall x \in A\ P(x)$. Recall that $\forall x \in A\ P(x)$ means the same thing as $\forall x(x \in A \rightarrow P(x))$, so according to our strategy the proof should start with "Suppose $x \in A$" and then proceed with the steps needed to conclude that $P(x)$ is true. Once again, it is understood that no assumptions are being made about x other than the stated assumption that $x \in A$, so x stands for an arbitrary element of A.

Mathematicians sometimes skip other steps in proofs, if knowledgeable readers could be expected to fill them in themselves. In particular, many of our proof strategies have suggested that the proof end with a sentence that sums up why the reasoning that has been given in the proof leads to the desired conclusion.

In a proof in which several of these strategies have been combined, there might be several of these summing up sentences, one after another, at the end of the proof. Mathematicians often condense this summing up into one sentence, or even skip it entirely. When you are reading a proof written by someone else, you may find it helpful to fill in these skipped steps.

Example 3.3.2. Suppose A and B are sets. Prove that if $A \cap B = A$ then $A \subseteq B$.

Scratch work

Our goal is $A \cap B = A \to A \subseteq B$. Because the goal is a conditional statement, we add the antecedent to the givens list and make the consequent the goal. We will also write out the definition of $\subseteq$ in the new goal to show what its logical form is.

Givens	*Goal*
$A \cap B = A$	$\forall x(x \in A \to x \in B)$

Now the goal has the form $\forall x(P(x) \to Q(x))$, where $P(x)$ is the statement $x \in A$ and $Q(x)$ is the statement $x \in B$. We therefore let x be arbitrary, assume $x \in A$, and prove $x \in B$:

Givens	*Goal*
$A \cap B = A$	$x \in B$
$x \in A$	

Combining the proof strategies we have used, we see that the final proof will have this form:

```
Suppose $A \cap B = A$.
  Let $x$ be arbitrary.
    Suppose $x \in A$.
      [Proof of $x \in B$ goes here.]
    Therefore $x \in A \to x \in B$.
  Since $x$ was arbitrary, we can conclude that $\forall x(x \in A \to x \in B)$, so
  $A \subseteq B$.
Therefore, if $A \cap B = A$ then $A \subseteq B$.
```

As discussed earlier, when we write up the final proof we can skip the sentence "Let x be arbitrary," and we can also skip some or all of the last three sentences.

We have now reached the point at which we can analyze the logical form of the goal no further. Fortunately, when we look at the givens, we discover that the goal follows easily. Since $x \in A$ and $A \cap B = A$, it follows that $x \in A \cap B$, so $x \in B$. (In this last step we are using the definition of $\cap$: $x \in A \cap B$ means $x \in A$ and $x \in B$.)

Solution

Theorem. *Suppose A and B are sets. If $A \cap B = A$ then $A \subseteq B$.*

Proof. Suppose $A \cap B = A$, and suppose $x \in A$. Then since $A \cap B = A$, $x \in A \cap B$, so $x \in B$. Since x was an arbitrary element of A, we can conclude that $A \subseteq B$. □

Proving a goal of the form $\exists x\, P(x)$ also involves introducing a new variable x into the proof and proving $P(x)$, but in this case x will not be arbitrary. Because you only need to prove that $P(x)$ is true for *at least one* x, it suffices to assign a particular value to x and prove $P(x)$ for this one value of x.

To prove a goal of the form $\exists x\, P(x)$:

Try to find a value of x for which you think $P(x)$ will be true. Then start your proof with "Let $x =$ (the value you decided on)" and proceed to prove $P(x)$ for this value of x. Once again, x should be a new variable. If the letter x is already being used in the proof for some other purpose, then you should choose an unused variable, say y, and rewrite the goal in the equivalent form $\exists y\, P(y)$. Now proceed as before by starting your proof with "Let $y =$ (the value you decided on)" and prove $P(y)$.

Scratch work

Before using strategy:

Givens	*Goal*
—	$\exists x\, P(x)$
—	

After using strategy:

Givens	*Goal*
—	$P(x)$
—	

$x =$ (the value you decided on)

Form of final proof:

Let $x =$ (the value you decided on).

[Proof of $P(x)$ goes here.]

Thus, $\exists x\, P(x)$.

Finding the right value to use for x may be difficult in some cases. One method that is sometimes helpful is to assume that $P(x)$ is true and then see if you can figure out what x must be, based on this assumption. If $P(x)$ is an equation involving x, this amounts to solving the equation for x. However, if this doesn't work, you may use any other method you please to try to find a value to use for x, including trial-and-error and guessing. The reason you have such freedom with this step is that *the reasoning you use to find a value for x will not appear in the final proof.* This is because of our rule that a proof should only contain the reasoning needed to justify the conclusion of the proof, not an explanation of how you thought of that reasoning. To justify the conclusion that $\exists x\, P(x)$ is true it is only necessary to verify that $P(x)$ comes out true when x is assigned some particular value. How you thought of that value is your own business, and not part of the justification of the conclusion.

Example 3.3.3. Prove that for every real number x, if $x > 0$ then there is a real number y such that $y(y+1) = x$.

Scratch work

In symbols, our goal is $\forall x(x > 0 \to \exists y[y(y+1) = x])$, where the variables x and y in this statement are understood to range over $\mathbb{R}$. We therefore start by letting x be an arbitrary real number, and we then assume that $x > 0$ and try to prove that $\exists y[y(y+1) = x]$. Thus, we now have the following given and goal:

Givens	*Goal*
$x > 0$	$\exists y[y(y+1) = x]$

Because our goal has the form $\exists y P(y)$, where $P(y)$ is the statement $y(y+1) = x$, according to our strategy we should try to find a value of y for which $P(y)$ is true. In this case we can do it by solving the equation $y(y+1) = x$ for y. It's a quadratic equation and can be solved using the quadratic formula:

$$y(y+1) = x \quad \Rightarrow \quad y^2 + y - x = 0 \quad \Rightarrow \quad y = \frac{-1 \pm \sqrt{1+4x}}{2}.$$

Note that $\sqrt{1+4x}$ is defined, since we have $x > 0$ as a given. We have actually found two solutions for y, but to prove that $\exists y[y(y+1) = x]$ we only need to exhibit one value of y that makes the equation $y(y+1) = x$ true. Either of the two solutions could be used in the proof. We will use the solution $y = (-1 + \sqrt{1+4x})/2$.

The steps we've used to solve for y should not appear in the final proof. In the final proof we will simply say "Let $y = (-1 + \sqrt{1 + 4x})/2$" and then prove that $y(y + 1) = x$. In other words, the final proof will have this form:

> Let x be an arbitrary real number.
>   Suppose $x > 0$.
>   Let $y = (-1 + \sqrt{1 + 4x})/2$.
>   [Proof of $y(y + 1) = x$ goes here.]
>   Thus, $\exists y[y(y + 1) = x]$.
>   Therefore $x > 0 \rightarrow \exists y[y(y + 1) = x]$.
> Since x was arbitrary, we can conclude that $\forall x(x > 0 \rightarrow \exists y[y(y + 1) = x])$.

To see what must be done to fill in the remaining gap in the proof, we add $y = (-1 + \sqrt{1 + 4x})/2$ to the givens list and make $y(y + 1) = x$ the goal:

Givens	*Goal*
$x > 0$	$y(y + 1) = x$
$y = \dfrac{-1 + \sqrt{1 + 4x}}{2}$	

We can now prove that the equation $y(y + 1) = x$ is true by simply substituting $(-1 + \sqrt{1 + 4x})/2$ for y and verifying that the resulting equation is true.

Solution

Theorem. *For every real number x, if $x > 0$ then there is a real number y such that $y(y + 1) = x$.*

Proof. Let x be an arbitrary real number, and suppose $x > 0$. Let

$$y = \frac{-1 + \sqrt{1 + 4x}}{2}$$

which is defined since $x > 0$. Then,

$$\begin{aligned} y(y + 1) &= \left(\frac{-1 + \sqrt{1 + 4x}}{2}\right) \cdot \left(\frac{-1 + \sqrt{1 + 4x}}{2} + 1\right) \\ &= \left(\frac{\sqrt{1 + 4x} - 1}{2}\right) \cdot \left(\frac{\sqrt{1 + 4x} + 1}{2}\right) \\ &= \frac{1 + 4x - 1}{4} = \frac{4x}{4} = x. \end{aligned}$$

□

Sometimes when you're proving a goal of the form $\exists y Q(y)$ you won't be able to tell just by looking at the statement $Q(y)$ what value you should plug in for y. In this case you may want to look more closely at the givens to see if they suggest a value to use for y. In particular, a given of the form $\exists x P(x)$ may be helpful in this situation. This given says that an object with a certain property exists. It is probably a good idea to imagine that a particular object with this property has been chosen and to introduce a new variable, say x_0, into the proof to stand for this object. Thus, for the rest of the proof you will be using x_0 to stand for some particular object, and you can assume that with x_0 standing for this object, $P(x_0)$ is true. In other words, you can add $P(x_0)$ to your givens list. This object x_0, or something related to it, might turn out to be the right thing to plug in for y to make $Q(y)$ come out true.

To use a given of the form $\exists x P(x)$:

Introduce a new variable x_0 into the proof to stand for an object for which $P(x_0)$ is true. This means that you can now assume that $P(x_0)$ is true. Logicians call this rule of inference *existential instantiation*.

Note that using a given of the form $\exists x P(x)$ is very different from proving a goal of the form $\exists x P(x)$, because when using a given of the form $\exists x P(x)$, *you don't get to choose a particular value to plug in for x*. You can assume that x_0 stands for some object for which $P(x_0)$ is true, but you can't assume anything else about x_0. On the other hand, a given of the form $\forall x P(x)$ says that $P(x)$ would be true *no matter what* value is assigned to x. You can therefore *choose any value you wish* to plug in for x and use this given to conclude that $P(x)$ is true.

To use a given of the form $\forall x P(x)$:

You can plug in any value, say a, for x and use this given to conclude that $P(a)$ is true. This rule is called *universal instantiation*.

Usually, if you have a given of the form $\exists x P(x)$, you should apply existential instantiation to it immediately. On the other hand, you won't be able to apply universal instantiation to a given of the form $\forall x P(x)$ unless you have a particular value a to plug in for x, so you might want to wait until a likely choice for a pops up in the proof. For example, consider a given of the form $\forall x(P(x) \to Q(x))$. You can use this given to conclude that $P(a) \to Q(a)$ for any a, but according to our rule for using givens that are conditional statements, this conclusion probably won't be very useful unless you know either $P(a)$ or $\neg Q(a)$. You should probably wait until an object a appears in the proof for which you know either $P(a)$ or $\neg Q(a)$, and plug this a in for x when it appears.

We've already used this technique in some of our earlier proofs when dealing with givens of the form $A \subseteq B$. For instance, in Example 3.2.5 we used the givens $A \subseteq B$ and $a \in A$ to conclude that $a \in B$. The justification for this reasoning is that $A \subseteq B$ means $\forall x(x \in A \rightarrow x \in B)$, so by universal instantiation we can plug in a for x and conclude that $a \in A \rightarrow a \in B$. Since we also know $a \in A$, it follows by modus ponens that $a \in B$.

Example 3.3.4. Suppose $\mathcal{F}$ and $\mathcal{G}$ are families of sets and $\mathcal{F} \cap \mathcal{G} \neq \varnothing$. Prove that $\cap\mathcal{F} \subseteq \cup\mathcal{G}$.

Scratch work

Our first step in analyzing the logical form of the goal is to write out the meaning of the subset symbol, which gives us the statement $\forall x(x \in \cap\mathcal{F} \rightarrow x \in \cup\mathcal{G})$. We could go further with this analysis by writing out the definitions of union and intersection, but the part of the analysis that we have already done will be enough to allow us to decide how to get started on the proof. The definitions of union and intersection will be needed later in the proof, but we will wait until they are needed before filling them in. When analyzing the logical forms of givens and goals in order to figure out a proof, it is usually best to do only as much of the analysis as is needed to determine the next step of the proof. Going further with the logical analysis usually just introduces unnecessary complication, without providing any benefit.

Because the goal means $\forall x(x \in \cap\mathcal{F} \rightarrow x \in \cup\mathcal{G})$, we let x be arbitrary, assume $x \in \cap\mathcal{F}$, and try to prove $x \in \cup\mathcal{G}$.

Givens	*Goal*
$\mathcal{F} \cap \mathcal{G} \neq \varnothing$	$x \in \cup\mathcal{G}$
$x \in \cap\mathcal{F}$	

The new goal means $\exists A \in \mathcal{G}(x \in A)$, so to prove it we should try to find a value that will "work" for A. Just looking at the goal doesn't make it clear how to choose A, so we look more closely at the givens. We begin by writing them out in logical symbols:

Givens	*Goal*
$\exists A(A \in \mathcal{F} \cap \mathcal{G})$	$\exists A \in \mathcal{G}(x \in A)$
$\forall A \in \mathcal{F}(x \in A)$	

The second given starts with $\forall A$, so we may not be able to use this given until a likely value to plug in for A pops up during the course of the proof. In particular, we should keep in mind that if we ever come across an element of $\mathcal{F}$ while trying to figure out the proof, we can plug it in for A in the second given and conclude that it contains x as an element. The first given, however, starts with $\exists A$, so we should use it immediately. It says that there is some object that is an element of $\mathcal{F} \cap \mathcal{G}$. By existential instantiation, we can introduce a name, say A_0, for this object. Thus, we can treat $A_0 \in \mathcal{F} \cap \mathcal{G}$ as a given from now on. Because we now have a name, A_0, for a particular element of $\mathcal{F} \cap \mathcal{G}$, it would be redundant to continue to discuss the given statement $\exists A(A \in \mathcal{F} \cap \mathcal{G})$, so we will drop it from our list of givens. Since our new given $A_0 \in \mathcal{F} \cap \mathcal{G}$ means $A_0 \in \mathcal{F}$ and $A_0 \in \mathcal{G}$, we now have the following situation:

Givens	*Goal*
$A_0 \in \mathcal{F}$	$\exists A \in \mathcal{G}(x \in A)$
$A_0 \in \mathcal{G}$	
$\forall A \in \mathcal{F}(x \in A)$	

If you've been paying close attention, you should know what the next step should be. We decided before to keep our eyes open for any elements of $\mathcal{F}$ that might come up during the proof, because we might want to plug them in for A in the last given. An element of $\mathcal{F}$ has come up: A_0! Plugging A_0 in for A in the last given, we can conclude that $x \in A_0$. Any conclusions can be treated in the future as givens, so you can add this statement to the givens column if you like.

Remember that we decided to look at the givens because we didn't know what value to assign to A in the goal. What we need is a value for A that is in $\mathcal{G}$ and that will make the statement $x \in A$ come out true. Has this consideration of the givens suggested a value to use for A? Yes! Use $A = A_0$.

Although we translated the given statements $x \in \cap\mathcal{F}$, $x \in \cup\mathcal{G}$, and $\mathcal{F} \cap \mathcal{G} \neq \varnothing$ into logical symbols in order to figure out how to use them in the proof, these translations are not usually written out when the proof is written up in final form. In the final proof we just write these statements in their original form and leave it to the reader of the proof to work out their logical forms in order to follow our reasoning.

Solution

Theorem. *Suppose $\mathcal{F}$ and $\mathcal{G}$ are families of sets, and $\mathcal{F} \cap \mathcal{G} \neq \varnothing$. Then $\cap\mathcal{F} \subseteq \cup\mathcal{G}$.*

Proof. Suppose $x \in \cap\mathcal{F}$. Since $\mathcal{F} \cap \mathcal{G} \neq \varnothing$, we can let A_0 be an element of $\mathcal{F} \cap \mathcal{G}$. Thus, $A_0 \in \mathcal{F}$ and $A_0 \in \mathcal{G}$. Since $x \in \cap\mathcal{F}$ and $A_0 \in \mathcal{F}$, it follows that $x \in A_0$. But we also know that $A_0 \in \mathcal{G}$, so we can conclude that $x \in \cup\mathcal{G}$. □

Proofs involving the quantifiers *for all* and *there exists* are often difficult for them.

That last sentence confused you, didn't it? You're probably wondering, "Who are *they*?" Readers of your proofs will experience the same sort of confusion if you use variables without explaining what they stand for. Beginning proof-writers are sometimes careless about this, and that's why proofs involving the quantifiers *for all* and *there exists* are often difficult for them. (It made more sense that time, didn't it?) When you use the strategies we've discussed in this section, you'll be introducing new variables into your proof, and when you do this, you must always be careful to make it clear to the reader what they stand for.

For example, if you were proving a goal of the form $\forall x \in A\ P(x)$, you would probably start by introducing a variable x to stand for an arbitrary element of A. Your reader won't know what x means, though, unless you begin your proof with "Let x be an arbitrary element of A," or "Suppose $x \in A$." Of course, you must be clear in your own mind about what x stands for. In particular, because x is to be arbitrary, you must be careful not to assume anything about x other than the fact that $x \in A$. It might help to think of x as being chosen by *someone else*; you have no control over which element of A they'll pick. Using a given of the form $\exists x P(x)$ is similar. This given tells you that you can introduce a new variable x_0 into the proof to stand for some object for which $P(x_0)$ is true, but you cannot assume anything else about x_0. On the other hand, if you are *proving* $\exists x P(x)$, your proof will probably start "Let $x = \ldots$" This time *you* get to choose the value of x, and you must tell the reader explicitly that you are choosing the value of x and what value you have chosen.

It's also important, when you're introducing a new variable x, to be sure you know what *kind* of object x is. Is it a number? a set? a function? a matrix? You'd better not write $a \in X$ unless X is a set, for example. If you aren't careful about this, you might end up writing nonsense. You also sometimes need to know what kind of object a variable stands for to figure out the logical form of a statement involving that variable. For example, $A = B$ means $\forall x(x \in A \leftrightarrow x \in B)$ if A and B are sets, but not if they're numbers.

The most important thing to keep in mind about introducing variables into a proof is simply the fact that variables must always be introduced before they are used. If you make a statement about x (i.e., a statement in which x occurs as a free variable) without first explaining what x stands for, a reader of your proof won't know what you're talking about – and there's a good chance that you won't know what you're talking about either!

Because proofs involving quantifiers may require more practice than the other proofs we have discussed so far, we end this section with two more examples.

Example 3.3.5. Suppose B is a set and $\mathcal{F}$ is a family of sets. Prove that if $\cup\mathcal{F} \subseteq B$ then $\mathcal{F} \subseteq \mathscr{P}(B)$.

Scratch Work

We assume $\cup\mathcal{F} \subseteq B$ and try to prove $\mathcal{F} \subseteq \mathscr{P}(B)$. Because this goal means $\forall x(x \in \mathcal{F} \to x \in \mathscr{P}(B))$, we let x be arbitrary, assume $x \in \mathcal{F}$, and set $x \in \mathscr{P}(B)$ as our goal. Recall that $\mathcal{F}$ is a family of sets, so since $x \in \mathcal{F}$, x is a set. Thus, we now have the following givens and goal:

Givens	*Goal*
$\cup\mathcal{F} \subseteq B$	$x \in \mathscr{P}(B)$
$x \in \mathcal{F}$	

To figure out how to prove this goal, we must use the definition of power set. The statement $x \in \mathscr{P}(B)$ means $x \subseteq B$, or in other words $\forall y(y \in x \to y \in B)$. We must therefore introduce another arbitrary object into the proof. We let y be arbitrary, assume $y \in x$, and try to prove $y \in B$.

Givens	*Goal*
$\cup\mathcal{F} \subseteq B$	$y \in B$
$x \in \mathcal{F}$	
$y \in x$	

The goal can be analyzed no further, so we must look more closely at the givens. Our goal is $y \in B$, and the only given that even mentions B is the first. In fact, the first given would enable us to reach this goal, if only we knew that $y \in \cup\mathcal{F}$. This suggests that we might try treating $y \in \cup\mathcal{F}$ as our goal. If we can reach this goal, then we can just add one more step, applying the first given, and the proof will be done.

Givens	*Goal*
$\cup\mathcal{F} \subseteq B$	$y \in \cup\mathcal{F}$
$x \in \mathcal{F}$	
$y \in x$	

Once again, we have a goal whose logical form can be analyzed, so we use the form of the goal to guide our strategy. The goal means $\exists A \in \mathcal{F}(y \in A)$, so to prove it we must find a set A such that $A \in \mathcal{F}$ and $y \in A$. Looking at the givens, we see that x is such a set, so the proof is done.

Solution

Theorem. *Suppose B is a set and $\mathcal{F}$ is a family of sets. If $\cup\mathcal{F} \subseteq B$ then $\mathcal{F} \subseteq \mathscr{P}(B)$.*

Proof. Suppose $\cup\mathcal{F} \subseteq B$. Let x be an arbitrary element of $\mathcal{F}$. Let y be an arbitrary element of x. Since $y \in x$ and $x \in \mathcal{F}$, clearly $y \in \cup\mathcal{F}$. But then since $\cup\mathcal{F} \subseteq B$, $y \in B$. Since y was an arbitrary element of x, we can conclude that $x \subseteq B$, so $x \in \mathscr{P}(B)$. But x was an arbitrary element of $\mathcal{F}$, so this shows that $\mathcal{F} \subseteq \mathscr{P}(B)$, as required. □

This is probably the most complex proof we've done so far. Read it again and make sure you understand its structure and the purpose of every sentence. Isn't it remarkable how much logical complexity has been packed into just a few lines?

It is not uncommon for a short proof to have such a rich logical structure. This efficiency of exposition is one of the most attractive features of proofs, but it also often makes them difficult to read. Although we've been concentrating so far on *writing* proofs, it is also important to learn how to *read* proofs written by other people. To give you some practice with this, we present our last proof in this section without the scratch work. See if you can follow the structure of the proof as you read it. We'll provide a commentary after the proof that should help you to understand it.

For this proof we need the following definition: For any integers x and y, we'll say that *x divides y* (or *y is divisible by x*) if $\exists k \in \mathbb{Z}(kx = y)$. We use the notation $x \mid y$ to mean "x divides y." For example, $4 \mid 20$, since $5 \cdot 4 = 20$.

Theorem 3.3.6. *For all integers a, b, and c, if $a \mid b$ and $b \mid c$ then $a \mid c$.*

Proof. Let a, b, and c be arbitrary integers and suppose $a \mid b$ and $b \mid c$. Since $a \mid b$, we can choose some integer m such that $ma = b$. Similarly, since $b \mid c$, we can choose an integer n such that $nb = c$. Therefore $c = nb = nma$, so since nm is an integer, $a \mid c$. □

Commentary. The theorem says $\forall a \in \mathbb{Z}\forall b \in \mathbb{Z}\forall c \in \mathbb{Z}(a \mid b \wedge b \mid c \rightarrow a \mid c)$, so the most natural way to proceed is to let a, b, and c be arbitrary integers, assume $a \mid b$ and $b \mid c$, and then prove $a \mid c$. The first sentence of the proof indicates that this strategy is being used, so the goal for the rest of the proof must be to prove that $a \mid c$. The fact that this is the goal for the rest of the proof is not explicitly stated. You are expected to figure this out for yourself by using your knowledge of proof strategies. You might even want to make a givens and goal list to help you keep track of what is known and what remains to be proven as you continue to read the proof. At this point in the proof, the list would look like this:

Givens	*Goal*
a, b, and c are integers	$a \mid c$
$a \mid b$	
$b \mid c$	

Because the new goal means $\exists k \in \mathbb{Z}(ka = c)$, the proof will probably proceed by finding an integer k such that $ka = c$. As with many proofs of existential statements, the first step in finding such a k involves looking more closely at the givens. The next sentence of the proof uses the given $a \mid b$ to conclude that we can choose an integer m such that $ma = b$. The proof doesn't say what rule of inference justifies this. It is up to you to figure it out by working out the logical form of the given statement $a \mid b$, using the definition of *divides*. Because this given means $\exists k \in \mathbb{Z}(ka = b)$, you should recognize that the rule of inference being used is existential instantiation. Existential instantiation is also used in the next sentence of the proof to justify choosing an integer n such that $nb = c$. The equations $ma = b$ and $nb = c$ can now be added to the list of givens.

Some steps have also been skipped in the last sentence of the proof. We expected that the goal $a \mid c$ would be proven by finding an integer k such that $ka = c$. From the equation $c = nma$ and the fact that nm is an integer, it follows that $k = nm$ will work, but the proof doesn't explicitly say that this value of k is being used; in fact, the variable k is not mentioned at all in the proof. Of course, the variable k is not mentioned in the statement of the theorem either. It is not uncommon for a proof of an existential statement to be written in this way, especially when, as in this case, the goal is not written out explicitly in the statement of the theorem as an existential statement. In this case, the existential nature of the goal became apparent only when we filled in the definition of *divides*.

Exercises

Note: Exercises marked with the symbol PD can be done with Proof Designer. For more information about Proof Designer, see Appendix 2.

*1. In exercise 7 of Section 2.2 you used logical equivalences to show that $\exists x(P(x) \to Q(x))$ is equivalent to $\forall x P(x) \to \exists x Q(x)$. Now use the methods of this section to prove that if $\exists x(P(x) \to Q(x))$ is true, then $\forall x P(x) \to \exists x Q(x)$ is true. (Note: The other direction of the equivalence is quite a bit harder to prove. See exercise 29 of Section 3.5.)

2. Prove that if A and $B \setminus C$ are disjoint, then $A \cap B \subseteq C$.

*3. Prove that if $A \subseteq B \setminus C$ then A and C are disjoint.

PD4. Suppose $A \subseteq \mathscr{P}(A)$. Prove that $\mathscr{P}(A) \subseteq \mathscr{P}(\mathscr{P}(A))$.

5. The hypothesis of the theorem proven in exercise 4 is $A \subseteq \mathscr{P}(A)$.
   (a) Can you think of a set A for which this hypothesis is true?
   (b) Can you think of another?

6. Suppose x is a real number.
   (a) Prove that if $x \neq 1$ then there is a real number y such that $\frac{y+1}{y-2} = x$.
   (b) Prove that if there is a real number y such that $\frac{y+1}{y-2} = x$, then $x \neq 1$.

*7. Prove that for every real number x, if $x > 2$ then there is a real number y such that $y + \frac{1}{y} = x$.

PD8. Prove that if $\mathcal{F}$ is a family of sets and $A \in \mathcal{F}$, then $A \subseteq \cup\mathcal{F}$.

*9. Prove that if $\mathcal{F}$ is a family of sets and $A \in \mathcal{F}$, then $\cap\mathcal{F} \subseteq A$.

10. Suppose that $\mathcal{F}$ is a nonempty family of sets, B is a set, and $\forall A \in \mathcal{F}(B \subseteq A)$. Prove that $B \subseteq \cap\mathcal{F}$.

11. Suppose that $\mathcal{F}$ is a family of sets. Prove that if $\varnothing \in \mathcal{F}$ then $\cap\mathcal{F} = \varnothing$.

PD*12. Suppose $\mathcal{F}$ and $\mathcal{G}$ are families of sets. Prove that if $\mathcal{F} \subseteq \mathcal{G}$ then $\cup\mathcal{F} \subseteq \cup\mathcal{G}$.

13. Suppose $\mathcal{F}$ and $\mathcal{G}$ are nonempty families of sets. Prove that if $\mathcal{F} \subseteq \mathcal{G}$ then $\cap\mathcal{G} \subseteq \cap\mathcal{F}$.

*14. Suppose $\{A_i \mid i \in I\}$ is an indexed family of sets. Prove that $\cup_{i \in I}\mathscr{P}(A_i) \subseteq \mathscr{P}(\cup_{i \in I}A_i)$. (Hint: First make sure you know what all the notation means!)

15. Suppose $\{A_i \mid i \in I\}$ is an indexed family of sets and $I \neq \varnothing$. Prove that $\cap_{i \in I}A_i \in \cap_{i \in I}\mathscr{P}(A_i)$.

PD16. Prove the converse of the statement proven in Example 3.3.5. In other words, prove that if $\mathcal{F} \subseteq \mathscr{P}(B)$ then $\cup\mathcal{F} \subseteq B$.

*17. Suppose $\mathcal{F}$ and $\mathcal{G}$ are nonempty families of sets, and every element of $\mathcal{F}$ is a subset of every element of $\mathcal{G}$. Prove that $\cup\mathcal{F} \subseteq \cap\mathcal{G}$.

18. In this problem all variables range over $\mathbb{Z}$, the set of all integers.
   (a) Prove that if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
   (b) Prove that if $ac \mid bc$ and $c \neq 0$, then $a \mid b$.

19. (a) Prove that for all real numbers x and y there is a real number z such that $x + z = y - z$.
   (b) Would the statement in part (a) be correct if "real number" were changed to "integer"? Justify your answer.

*20. Consider the following theorem:

   Theorem. *For every real number x, $x^2 \geq 0$.*

   What's wrong with the following proof of the theorem?

Proof. Suppose not. Then for every real number x, $x^2 < 0$. In particular, plugging in $x = 3$ we would get $9 < 0$, which is clearly false. This contradiction shows that for every number x, $x^2 \geq 0$. □

21. Consider the following incorrect theorem:

    Incorrect Theorem. *If* $\forall x \in A(x \neq 0)$ and $A \subseteq B$ then $\forall x \in B(x \neq 0)$.

    (a) What's wrong with the following proof of the theorem?

    Proof. Let x be an arbitrary element of A. Since $\forall x \in A(x \neq 0)$, we can conclude that $x \neq 0$. Also, since $A \subseteq B, x \in B$. Since $x \in B, x \neq 0$, and x was arbitrary, we can conclude that $\forall x \in B(x \neq 0)$. □

    (b) Find a counterexample to the theorem. In other words, find an example of sets A and B for which the hypotheses of the theorem are true but the conclusion is false.

*22. Consider the following incorrect theorem:

    Incorrect Theorem. $\exists x \in \mathbb{R} \forall y \in \mathbb{R}(xy^2 = y - x)$.

    What's wrong with the following proof of the theorem?

    Proof. Let $x = y/(y^2 + 1)$. Then

$$y - x = y - \frac{y}{y^2+1} = \frac{y^3}{y^2+1} = \frac{y}{y^2+1} \cdot y^2 = xy^2. \qquad \square$$

23. Consider the following incorrect theorem:

    Incorrect Theorem. *Suppose $\mathcal{F}$ and $\mathcal{G}$ are families of sets. If $\cup\mathcal{F}$ and $\cup\mathcal{G}$ are disjoint, then so are $\mathcal{F}$ and $\mathcal{G}$.*

    (a) What's wrong with the following proof of the theorem?

    Proof. Suppose $\cup\mathcal{F}$ and $\cup\mathcal{G}$ are disjoint. Suppose $\mathcal{F}$ and $\mathcal{G}$ are not disjoint. Then we can choose some set A such that $A \in \mathcal{F}$ and $A \in \mathcal{G}$. Since $A \in \mathcal{F}$, by exercise 8, $A \subseteq \cup\mathcal{F}$, so every element of A is in $\cup\mathcal{F}$. Similarly, since $A \in \mathcal{G}$, every element of A is in $\cup\mathcal{G}$. But then every element of A is in both $\cup\mathcal{F}$ and $\cup\mathcal{G}$, and this is impossible since $\cup\mathcal{F}$ and $\cup\mathcal{G}$ are disjoint. Thus, we have reached a contradiction, so $\mathcal{F}$ and $\mathcal{G}$ must be disjoint. □

    (b) Find a counterexample to the theorem.

24. Consider the following putative theorem:

    Theorem? *For all real numbers x and y,* $x^2 + xy - 2y^2 = 0$.

    (a) What's wrong with the following proof of the theorem?

    Proof. Let x and y be equal to some arbitrary real number r. Then
    $$x^2 + xy - 2y^2 = r^2 + r \cdot r - 2r^2 = 0.$$
    Since x and y were both arbitrary, this shows that for all real numbers x and y, $x^2 + xy - 2y^2 = 0$. □

    (b) Is the theorem correct? Justify your answer with either a proof or a counterexample.

*25. Prove that for every real number x there is a real number y such that for every real number z, $yz = (x + z)^2 - (x^2 + z^2)$.

26. (a) Comparing the various rules for dealing with quantifiers in proofs, you should see a similarity between the rules for goals of the form $\forall x P(x)$ and givens of the form $\exists x P(x)$. What is this similarity? What about the rules for goals of the form $\exists x P(x)$ and givens of the form $\forall x P(x)$?

    (b) Can you think of a reason why these similarities might be expected? (Hint: Think about how proof by contradiction works when the goal starts with a quantifier.)

3.4. Proofs Involving Conjunctions and Biconditionals

The method for proving a goal of the form $P \wedge Q$ is so simple it hardly seems worth mentioning:

To prove a goal of the form $P \wedge Q$:
Prove P and Q separately.

In other words, a goal of the form $P \wedge Q$ is treated as two separate goals: P, and Q. The same is true of givens of the form $P \wedge Q$:

To use a given of the form $P \wedge Q$:
Treat this given as two separate givens: P, and Q.

We've already used these ideas, without mention, in some of our previous examples. For example, the definition of the given $x \in A \setminus C$ in Example 3.2.3 was $x \in A \wedge x \notin C$, but we treated it as two separate givens: $x \in A$, and $x \notin C$.

Example 3.4.1. Suppose $A \subseteq B$, and A and C are disjoint. Prove that $A \subseteq B \setminus C$.

Scratch work

Givens	*Goal*
$A \subseteq B$	$A \subseteq B \setminus C$
$A \cap C = \varnothing$	

Analyzing the logical form of the goal, we see that it has the form $\forall x(x \in A \to x \in B \setminus C)$, so we let x be arbitrary, assume $x \in A$, and try to prove that $x \in B \setminus C$. The new goal $x \in B \setminus C$ means $x \in B \wedge x \notin C$, so according to our strategy we should split this into two goals, $x \in B$ and $x \notin C$, and prove them separately.

Givens	*Goals*
$A \subseteq B$	$x \in B$
$A \cap C = \varnothing$	$x \notin C$
$x \in A$	

The final proof will have this form:

Let x be arbitrary.
  Suppose $x \in A$.
    [Proof of $x \in B$ goes here.]
    [Proof of $x \notin C$ goes here.]
   Thus, $x \in B \wedge x \notin C$, so $x \in B \setminus C$.
  Therefore $x \in A \to x \in B \setminus C$.
Since x was arbitrary, $\forall x(x \in A \to x \in B \setminus C)$, so $A \subseteq B \setminus C$.

The first goal, $x \in B$, clearly follows from the fact that $x \in A$ and $A \subseteq B$. The second goal, $x \notin C$, follows from $x \in A$ and $A \cap C = \varnothing$. You can see this by analyzing the logical form of the statement $A \cap C = \varnothing$. It is a negative statement, but it can be reexpressed as an equivalent positive statement:

$A \cap C = \varnothing$ is equivalent to $\neg\exists y(y \in A \wedge y \in C)$ (definitions of $\cap$ and $\varnothing$),
which is equivalent to $\forall y\neg(y \in A \wedge y \in C)$ (quantifier negation law),
which is equivalent to $\forall y(y \notin A \vee y \notin C)$ (DeMorgan's law),
which is equivalent to $\forall y(y \in A \to y \notin C)$ (conditional law).

Plugging in x for y in this last statement, we see that $x \in A \to x \notin C$, and since we already know $x \in A$, we can conclude that $x \notin C$.

Solution

Theorem. *Suppose $A \subseteq B$, and A and C are disjoint. Then $A \subseteq B \setminus C$*

Proof. Suppose $x \in A$. Since $A \subseteq B$, it follows that $x \in B$, and since A and C are disjoint, we must have $x \notin C$. Thus, $x \in B \setminus C$. Since x was an arbitrary element of A, we can conclude that $A \subseteq B \setminus C$. □

Using our strategies for working with conjunctions, we can now work out the proper way to deal with statements of the form $P \leftrightarrow Q$ in proofs. Because $P \leftrightarrow Q$ is equivalent to $(P \to Q) \wedge (Q \to P)$, according to our strategies a given or goal of the form $P \leftrightarrow Q$ should be treated as two separate givens or goals: $P \to Q$, and $Q \to P$.

To prove a goal of the form $P \leftrightarrow Q$:
Prove $P \to Q$ and $Q \to P$ separately.

To use a given of the form $P \leftrightarrow Q$:
Treat this as two separate givens: $P \to Q$, and $Q \to P$.

This is illustrated in the next example, in which we use the following definitions: An integer x is *even* if $\exists k \in \mathbb{Z}(x = 2k)$, and x is *odd* if $\exists k \in \mathbb{Z}(x = 2k + 1)$. We also use the fact that every integer is either even or odd, but not both. We'll see a proof of this fact in Chapter 6.

Example 3.4.2. Suppose x is an integer. Prove that x is even iff x^2 is even.

Scratch work

The goal is (x is even) $\leftrightarrow$ (x^2 is even), so we prove the two goals (x is even) $\to$ (x^2 is even) and (x^2 is even) $\to$ (x is even) separately. For the first, we assume that x is even and prove that x^2 is even:

Givens	*Goal*
$x \in \mathbb{Z}$	x^2 is even
x is even	

Writing out the definition of *even* in both the given and the goal will reveal their logical forms:

Givens	*Goal*
$x \in \mathbb{Z}$	$\exists k \in \mathbb{Z}(x^2 = 2k)$
$\exists k \in \mathbb{Z}(x = 2k)$	

Because the second given starts with $\exists k$, we immediately use it and let k stand for some particular integer for which the statement $x = 2k$ is true. Thus, we have two new given statements: $k \in \mathbb{Z}$, and $x = 2k$.

Givens	*Goal*
$x \in \mathbb{Z}$	$\exists k \in \mathbb{Z}(x^2 = 2k)$
$k \in \mathbb{Z}$	
$x = 2k$	

The goal starts with $\exists k$, but since k is already being used to stand for a particular number, we cannot assign a new value to k to prove the goal. We must therefore switch to a different letter, say j. One way to understand this is to think of rewriting the goal in the equivalent form $\exists j \in \mathbb{Z}(x^2 = 2j)$. To prove this goal we must come up with a value to plug in for j. It must be an integer, and it must satisfy the equation $x^2 = 2j$. Using the given equation $x = 2k$, we see that $x^2 = (2k)^2 = 4k^2 = 2(2k^2)$, so it looks like the right value to choose for j is $j = 2k^2$. Clearly $2k^2$ is an integer, so this choice for j will work to complete the proof of our first goal.

To prove the second goal (x^2 is even) → (x is even), we'll prove the contrapositive (x is not even) → (x^2 is not even) instead. Since any integer is either even or odd but not both, this is equivalent to the statement (x is odd) → (x^2 is odd).

Givens	*Goal*
$x \in \mathbb{Z}$	x^2 is odd
x is odd	

The steps are now quite similar to the first part of the proof. As before, we begin by writing out the definition of *odd* in both the second given and the goal. This time, to avoid the conflict of variable names we ran into in the first part of the proof, we use different names for the bound variables in the two statements.

Givens	*Goal*
$x \in \mathbb{Z}$	$\exists j \in \mathbb{Z}(x^2 = 2j + 1)$
$\exists k \in \mathbb{Z}(x = 2k + 1)$	

Next we use the second given and let k stand for a particular integer for which $x = 2k + 1$.

Givens	*Goal*
$x \in \mathbb{Z}$	$\exists j \in \mathbb{Z}(x^2 = 2j + 1)$
$k \in \mathbb{Z}$	
$x = 2k + 1$	

We must now find an integer j such that $x^2 = 2j + 1$. Plugging in $2k + 1$ for x we get $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, so $j = 2k^2 + 2k$ looks like the right choice.

Before giving the final write-up of the proof, we should make a few explanatory remarks. The two conditional statements we've proven can be thought of as representing the two directions → and ← of the biconditional symbol ↔ in the original goal. These two parts of the proof are sometimes labeled with the symbols → and ←. In each part, we end up proving a statement that asserts the existence of a number with certain properties. We called this number j in the scratch work, but note that j was not mentioned explicitly in the statement of the problem. As in the proof of Theorem 3.3.6, we have chosen not to mention j explicitly in the final proof either.

Solution

Theorem. *Suppose x is an integer. Then x is even iff x^2 is even.*

Proof. (→) Suppose x is even. Then for some integer k, $x = 2k$. Therefore, $x^2 = 4k^2 = 2(2k^2)$, so since $2k^2$ is an integer, x^2 is even. Thus, if x is even then x^2 is even.

(←) Suppose x is odd. Then $x = 2k + 1$ for some integer k. Therefore, $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, so since $2k^2 + 2k$ is an integer, x^2 is odd. Thus, if x^2 is even then x is even. □

Using the proof techniques we've developed, we can now verify some of the equivalences that we were only able to justify on intuitive grounds in Chapter 2. As an example of this, let's prove that the formulas $\forall x \neg P(x)$ and $\neg\exists x\, P(x)$ are equivalent. To say that these formulas are equivalent means that they will always have the same truth value. In other words, no matter what statement $P(x)$ stands for, the statement $\forall x \neg P(x) \leftrightarrow \neg\exists x\, P(x)$ will be true. We can prove this using our technique for proving biconditional statements.

Example 3.4.3. Prove that $\forall x \neg P(x) \leftrightarrow \neg\exists x\, P(x)$.

Scratch work

(→) We must prove $\forall x \neg P(x) \rightarrow \neg\exists x\, P(x)$, so we assume $\forall x \neg P(x)$ and try to prove $\neg\exists x\, P(x)$. Our goal is now a negated statement, and reexpressing it would require the use of the very equivalence that we are trying to prove! We therefore fall back on our only other strategy for dealing with negative goals, proof by contradiction. We now have the following situation:

Givens	*Goal*
$\forall x \neg P(x)$	Contradiction
$\exists x\, P(x)$	

The second given starts with an existential quantifier, so we use it immediately and let x_0 stand for some object for which the statement $P(x_0)$ is true. But now plugging in x_0 for x in the first given we can conclude that $\neg P(x_0)$, which gives us the contradiction we need.

($\leftarrow$) For this direction of the biconditional we should assume $\neg\exists x\, P(x)$ and try to prove $\forall x \neg P(x)$. Because this goal starts with a universal quantifier, we let x be arbitrary and try to prove $\neg P(x)$. Once again, we now have a negated goal that can't be reexpressed, so we use proof by contradiction:

Givens	*Goal*
$\neg\exists x\, P(x)$	Contradiction
$P(x)$	

Our first given is also a negated statement, and this suggests that we could get the contradiction we need by proving $\exists x\, P(x)$. We therefore set this as our goal.

Givens	*Goal*
$\neg\exists x\, P(x)$	$\exists x\, P(x)$
$P(x)$	

To keep from confusing the x that appears as a free variable in the second given (the arbitrary x introduced earlier in the proof) with the x that appears as a bound variable in the goal, you might want to rewrite the goal in the equivalent form $\exists y\, P(y)$. To prove this goal we have to find a value of y that makes $P(y)$ come out true. But this is easy! Our second given, $P(x)$, tells us that our arbitrary x is the value we need.

Solution

Theorem. $\forall x \neg P(x) \leftrightarrow \neg\exists x\, P(x)$.

Proof. ($\rightarrow$) Suppose $\forall x \neg P(x)$, and suppose $\exists x\, P(x)$. Then we can choose some x_0 such that $P(x_0)$ is true. But since $\forall x \neg P(x)$, we can conclude that $\neg P(x_0)$, and this is a contradiction. Therefore $\forall x \neg P(x) \rightarrow \neg\exists x\, P(x)$.

($\leftarrow$) Suppose $\neg\exists x\, P(x)$. Let x be arbitrary, and suppose $P(x)$. Since we have a specific x for which $P(x)$ is true, it follows that $\exists x\, P(x)$, which is a contradiction. Therefore, $\neg P(x)$. Since x was arbitrary, we can conclude that $\forall x \neg P(x)$, so $\neg\exists x\, P(x) \rightarrow \forall x \neg P(x)$. □

Sometimes in a proof of a goal of the form $P \leftrightarrow Q$ the steps in the proof of $Q \rightarrow P$ are the same as the steps used to prove $P \rightarrow Q$, but in reverse order. In this case you may be able to simplify the proof by writing it as a string of equivalences, starting with P and ending with Q. For example, suppose you found that you could prove $P \rightarrow Q$ by first assuming P, then using P to infer some other statement R, and then using R to deduce Q; and suppose that the same steps could be used, in reverse order, to prove that $Q \rightarrow P$. In other words, you could assume Q, use this assumption to conclude that R was true, and then use R to prove P. Since you would be asserting both $P \rightarrow R$ and $R \rightarrow P$, you could sum up these two steps by saying $P \leftrightarrow R$. Similarly, the other two steps of the proof tell you that $R \leftrightarrow Q$. These two statements imply the goal $P \leftrightarrow Q$. Mathematicians sometimes present this kind of proof by simply writing the string of equivalences

$$P \text{ iff } R \text{ iff } Q.$$

You can think of this as an abbreviation for "P iff R and R iff Q (and therefore P iff Q)." This is illustrated in the next example.

Example 3.4.4. Suppose A, B, and C are sets. Prove that $A \cap (B \setminus C) = (A \cap B) \setminus C$.

Scratch work

As we saw in Chapter 2, the equation $A \cap (B \setminus C) = (A \cap B) \setminus C$ means $\forall x(x \in A \cap (B \setminus C) \leftrightarrow x \in (A \cap B) \setminus C)$, but it is also equivalent to the statement $[A \cap (B \setminus C) \subseteq (A \cap B) \setminus C] \wedge [(A \cap B) \setminus C \subseteq A \cap (B \setminus C)]$. This suggests two approaches to the proof. We could let x be arbitrary and then prove $x \in A \cap (B \setminus C) \leftrightarrow x \in (A \cap B) \setminus C$, or we could prove the two statements $A \cap (B \setminus C) \subseteq (A \cap B) \setminus C$ and $(A \cap B) \setminus C \subseteq A \cap (B \setminus C)$. In fact, almost every proof that two sets are equal will involve one of these two approaches. In this case we will use the first approach, so once we have introduced our arbitrary x, we will have an iff goal.

For the ($\rightarrow$) half of the proof we assume $x \in A \cap (B \setminus C)$ and try to prove $x \in (A \cap B) \setminus C$:

Givens	*Goal*
$x \in A \cap (B \setminus C)$	$x \in (A \cap B) \setminus C$

To see the logical forms of the given and goal, we write out their definitions as follows:

$$x \in A \cap (B \setminus C) \text{ iff } x \in A \wedge x \in B \setminus C \text{ iff } x \in A \wedge x \in B \wedge x \notin C;$$
$$x \in (A \cap B) \setminus C \text{ iff } x \in A \cap B \wedge x \notin C \text{ iff } x \in A \wedge x \in B \wedge x \notin C.$$

At this point it is clear that the given implies the goal, since the last steps in both strings of equivalences turned out to be identical. In fact, it is also clear that the reasoning involved in the ($\leftarrow$) direction of the proof will be exactly the same, but with the given and goal columns reversed. Thus, we might try to shorten the proof by writing it as a string of equivalences, starting with $x \in A \cap (B \setminus C)$ and ending with $x \in (A \cap B) \setminus C$. In this case, if we start with $x \in A \cap (B \setminus C)$ and follow the first string of equivalences displayed above, we come to a statement that is the same as the last statement in the second string of equivalences. We can then continue by following the second string of equivalences *backward*, ending with $x \in (A \cap B) \setminus C$.

Solution

Theorem. *Suppose A, B, and C are sets. Then* $A \cap (B \setminus C) = (A \cap B) \setminus C$.

Proof. Let x be arbitrary. Then

$$\begin{aligned} x \in A \cap (B \setminus C) &\text{ iff } x \in A \wedge x \in B \setminus C \\ &\text{ iff } x \in A \wedge x \in B \wedge x \notin C \\ &\text{ iff } x \in (A \cap B) \wedge x \notin C \\ &\text{ iff } x \in (A \cap B) \setminus C. \end{aligned}$$

Thus, $\forall x(x \in A \cap (B \setminus C) \leftrightarrow x \in (A \cap B) \setminus C)$, so $A \cap (B \setminus C) = (A \cap B) \setminus C$. □

The technique of figuring out a sequence of equivalences in one order and then writing it in the reverse order is used quite often in proofs. The order in which the steps should be written in the final proof is determined by our rule that an assertion should never be made until it can be justified. In particular, if you are trying to prove $P \leftrightarrow Q$, it is wrong to start your write-up of the proof with the unjustified statement $P \leftrightarrow Q$ and then work out the meanings of the two sides P and Q, showing that they are the same. You should instead start with equivalences you can justify and string them together to produce a justification of the goal $P \leftrightarrow Q$ before you assert this goal. A similar technique can sometimes be used to figure out proofs of equations, as the next example shows.

Example 3.4.5. Prove that for any real numbers a and b,

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

Scratch work

The goal has the form $\forall a \forall b((a + b)^2 - 4(a - b)^2 = (3b - a)(3a - b))$, so we start by letting a and b be arbitrary real numbers and try to prove the equation.

Multiplying out both sides gives us:

$$\begin{aligned}(a+b)^2 - 4(a-b)^2 &= a^2 + 2ab + b^2 - 4(a^2 - 2ab + b^2)\\ &= -3a^2 + 10ab - 3b^2;\\ (3b-a)(3a-b) = 9ab - 3a^2 - 3b^2 + ab &= -3a^2 + 10ab - 3b^2.\end{aligned}$$

Clearly the two sides are equal. The simplest way to write the proof of this is to write a string of equalities starting with $(a+b)^2 - 4(a-b)^2$ and ending with $(3b-a)(3a-b)$. We can do this by copying down the first string of equalities displayed above, and then following it with the second line, written backward.

Solution

Theorem. *For any real numbers a and b,*

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

Proof. Let a and b be arbitrary real numbers. Then

$$\begin{aligned}(a+b)^2 - 4(a-b)^2 &= a^2 + 2ab + b^2 - 4(a^2 - 2ab + b^2)\\ &= -3a^2 + 10ab - 3b^2\\ &= 9ab - 3a^2 - 3b^2 + ab = (3b-a)(3a-b). \quad \square\end{aligned}$$

We end this section by presenting another proof without preliminary scratch work, but with a commentary to help you read the proof.

Theorem 3.4.6. *For every integer* n, $6 \mid n$ iff $2 \mid n$ *and* $3 \mid n$.

Proof. Let n be an arbitrary integer.

($\rightarrow$) Suppose $6 \mid n$. Then we can choose an integer k such that $6k = n$. Therefore $n = 6k = 2(3k)$, so $2 \mid n$, and similarly $n = 6k = 3(2k)$, so $3 \mid n$.

($\leftarrow$) Suppose $2 \mid n$ and $3 \mid n$. Then we can choose integers j and k such that $n = 2j$ and $n = 3k$. Therefore $6(j-k) = 6j - 6k = 3(2j) - 2(3k) = 3n - 2n = n$, so $6 \mid n$. □

Commentary. The statement to be proven is $\forall n \in \mathbb{Z}(6 \mid n \leftrightarrow (2 \mid n \wedge 3 \mid n))$, and the most natural strategy for proving a goal of this form is to let n be arbitrary and then prove both directions of the biconditional separately. It should be clear that this is the strategy being used in the proof.

For the left-to-right direction of the biconditional, we assume $6 \mid n$ and then prove $2 \mid n$ and $3 \mid n$, treating this as two separate goals. The introduction of the integer k is justified by existential instantiation, since the assumption $6 \mid n$ means $\exists k \in \mathbb{Z}(6k = n)$. At this point in the proof we have the following givens and goals:

Givens	*Goals*
$n \in \mathbb{Z}$	$2 \mid n$
$k \in \mathbb{Z}$	$3 \mid n$
$6k = n$	

The first goal, $2 \mid n$, means $\exists j \in \mathbb{Z}(2j = n)$, so we must find an integer j such that $2j = n$. Although the proof doesn't say so explicitly, the equation $n = 2(3k)$, which is derived in the proof, suggests that the value being used for j is $j = 3k$. Clearly, $3k$ is an integer (another step skipped in the proof), so this choice for j works. The proof of $3 \mid n$ is similar.

For the right-to-left direction we assume $2 \mid n$ and $3 \mid n$ and prove $6 \mid n$. Once again, the introduction of j and k is justified by existential instantiation. No explanation is given for why we should compute $6(j - k)$, but a proof need not provide such explanations. The reason for the calculation should become clear when, surprisingly, it turns out that $6(j - k) = n$. Such surprises provide part of the pleasure of working with proofs. As in the first half of the proof, since $j - k$ is an integer, this shows that $6 \mid n$.

Exercises

*1. Use the methods of this chapter to prove that $\forall x(P(x) \land Q(x))$ is equivalent to $\forall x P(x) \land \forall x Q(x)$.

Pd2. Prove that if $A \subseteq B$ and $A \subseteq C$ then $A \subseteq B \cap C$.

Pd3. Suppose $A \subseteq B$. Prove that for every set C, $C \setminus B \subseteq C \setminus A$.

Pd*4. Prove that if $A \subseteq B$ and $A \nsubseteq C$ then $B \nsubseteq C$.

Pd5. Prove that if $A \subseteq B \setminus C$ and $A \neq \varnothing$ then $B \nsubseteq C$.

6. Prove that for any sets A, B, and C, $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$, by finding a string of equivalences starting with $x \in A \setminus (B \cap C)$ and ending with $x \in (A \setminus B) \cup (A \setminus C)$. (See Example 3.4.4.)

Pd*7. Use the methods of this chapter to prove that for any sets A and B, $\mathscr{P}(A \cap B) = \mathscr{P}(A) \cap \mathscr{P}(B)$.

Pd8. Prove that $A \subseteq B$ iff $\mathscr{P}(A) \subseteq \mathscr{P}(B)$.

*9. Prove that if x and y are odd integers, then xy is odd.

10. Prove that for every integer n, n^3 is even iff n is even.

11. Consider the following putative theorem:

    Theorem? *Suppose m is an even integer and n is an odd integer. Then $n^2 - m^2 = n + m$.*

    (a) What's wrong with the following proof of the theorem?

    Proof. Since m is even, we can choose some integer k such that $m = 2k$. Similarly, since n is odd we have $n = 2k + 1$. Therefore

    $$\begin{aligned} n^2 - m^2 &= (2k+1)^2 - (2k)^2 = 4k^2 + 4k + 1 - 4k^2 = 4k + 1 \\ &= (2k+1) + (2k) = n + m. \end{aligned}$$ □

    (b) Is the theorem correct? Justify your answer with either a proof or a counterexample.

*12. Prove that $\forall x \in \mathbb{R}[\exists y \in \mathbb{R}(x + y = xy) \leftrightarrow x \neq 1]$.

13. Prove that $\exists z \in \mathbb{R} \forall x \in \mathbb{R}^+[\exists y \in \mathbb{R}(y - x = y/x) \leftrightarrow x \neq z]$.

PD14. Suppose B is a set and $\mathcal{F}$ is a family of sets. Prove that $\cup\{A \setminus B \mid A \in \mathcal{F}\} \subseteq \cup(\mathcal{F} \setminus \mathscr{P}(B))$.

*15. Suppose $\mathcal{F}$ and $\mathcal{G}$ are nonempty families of sets and every element of $\mathcal{F}$ is disjoint from some element of $\mathcal{G}$. Prove that $\cup\mathcal{F}$ and $\cap\mathcal{G}$ are disjoint.

PD16. Prove that for any set A, $A = \cup\mathscr{P}(A)$.

PD*17. Suppose $\mathcal{F}$ and $\mathcal{G}$ are families of sets.

    (a) Prove that $\cup(\mathcal{F} \cap \mathcal{G}) \subseteq (\cup\mathcal{F}) \cap (\cup\mathcal{G})$.

    (b) What's wrong with the following proof that $(\cup\mathcal{F}) \cap (\cup\mathcal{G}) \subseteq \cup(\mathcal{F} \cap \mathcal{G})$?

    Proof. Suppose $x \in (\cup\mathcal{F}) \cap (\cup\mathcal{G})$. This means that $x \in \cup\mathcal{F}$ and $x \in \cup\mathcal{G}$, so $\exists A \in \mathcal{F}(x \in A)$ and $\exists A \in \mathcal{G}(x \in A)$. Thus, we can choose a set A such that $A \in \mathcal{F}$, $A \in \mathcal{G}$, and $x \in A$. Since $A \in \mathcal{F}$ and $A \in \mathcal{G}$, $A \in \mathcal{F} \cap \mathcal{G}$. Therefore $\exists A \in \mathcal{F} \cap \mathcal{G}(x \in A)$, so $x \in \cup(\mathcal{F} \cap \mathcal{G})$. Since x was arbitrary, we can conclude that $(\cup\mathcal{F}) \cap (\cup\mathcal{G}) \subseteq \cup(\mathcal{F} \cap \mathcal{G})$. □

    (c) Find an example of families of sets $\mathcal{F}$ and $\mathcal{G}$ for which $\cup(\mathcal{F} \cap \mathcal{G}) \neq (\cup\mathcal{F}) \cap (\cup\mathcal{G})$.

PD18. Suppose $\mathcal{F}$ and $\mathcal{G}$ are families of sets. Prove that $(\cup\mathcal{F}) \cap (\cup\mathcal{G}) \subseteq \cup(\mathcal{F} \cap \mathcal{G})$ iff $\forall A \in \mathcal{F} \forall B \in \mathcal{G}(A \cap B \subseteq \cup(\mathcal{F} \cap \mathcal{G}))$.

PD19. Suppose $\mathcal{F}$ and $\mathcal{G}$ are families of sets. Prove that $\cup\mathcal{F}$ and $\cup\mathcal{G}$ are disjoint iff for all $A \in \mathcal{F}$ and $B \in \mathcal{G}$, A and B are disjoint.

PD20. Suppose $\mathcal{F}$ and $\mathcal{G}$ are families of sets.

    (a) Prove that $(\cup\mathcal{F}) \setminus (\cup\mathcal{G}) \subseteq \cup(\mathcal{F} \setminus \mathcal{G})$.

    (b) What's wrong with the following proof that $\cup(\mathcal{F} \setminus \mathcal{G}) \subseteq (\cup\mathcal{F}) \setminus (\cup\mathcal{G})$?

Proof. Suppose $x \in \cup(\mathcal{F} \setminus \mathcal{G})$. Then we can choose some $A \in \mathcal{F} \setminus \mathcal{G}$ such that $x \in A$. Since $A \in \mathcal{F} \setminus \mathcal{G}$, $A \in \mathcal{F}$ and $A \notin \mathcal{G}$. Since $x \in A$ and $A \in \mathcal{F}$, $x \in \cup\mathcal{F}$. Since $x \in A$ and $A \notin \mathcal{G}$, $x \notin \cup\mathcal{G}$. Therefore $x \in (\cup\mathcal{F}) \setminus (\cup\mathcal{G})$. □

(c) Prove that $\cup(\mathcal{F} \setminus \mathcal{G}) \subseteq (\cup\mathcal{F}) \setminus (\cup\mathcal{G})$ iff $\forall A \in (\mathcal{F} \setminus \mathcal{G})\forall B \in \mathcal{G}(A \cap B = \varnothing)$.

(d) Find an example of families of sets $\mathcal{F}$ and $\mathcal{G}$ for which $\cup(\mathcal{F} \setminus \mathcal{G}) \neq (\cup\mathcal{F}) \setminus (\cup\mathcal{G})$.

PD*21. Suppose $\mathcal{F}$ and $\mathcal{G}$ are families of sets. Prove that if $\cup\mathcal{F} \not\subseteq \cup\mathcal{G}$, then there is some $A \in \mathcal{F}$ such that for all $B \in \mathcal{G}$, $A \not\subseteq B$.

22. Suppose B is a set, $\{A_i \mid i \in I\}$ is an indexed family of sets, and $I \neq \varnothing$.

(a) What proof strategies are used in the following proof that $B \cap (\cup_{i \in I} A_i) = \cup_{i \in I}(B \cap A_i)$?

Proof. Let x be arbitrary. Suppose $x \in B \cap (\cup_{i \in I} A_i)$. Then $x \in B$ and $x \in \cup_{i \in I} A_i$, so we can choose some $i_0 \in I$ such that $x \in A_{i_0}$. Since $x \in B$ and $x \in A_{i_0}$, $x \in B \cap A_{i_0}$. Therefore $x \in \cup_{i \in I}(B \cap A_i)$.

Now suppose $x \in \cup_{i \in I}(B \cap A_i)$. Then we can choose some $i_0 \in I$ such that $x \in B \cap A_{i_0}$. Therefore $x \in B$ and $x \in A_{i_0}$. Since $x \in A_{i_0}$, $x \in \cup_{i \in I} A_i$. Since $x \in B$ and $x \in \cup_{i \in I} A_i$, $x \in B \cap (\cup_{i \in I} A_i)$.

Since x was arbitrary, we have shown that $\forall x[x \in B \cap (\cup_{i \in I} A_i) \leftrightarrow x \in \cup_{i \in I}(B \cap A_i)]$, so $B \cap (\cup_{i \in I} A_i) = \cup_{i \in I}(B \cap A_i)$. □

(b) Prove that $B \setminus (\cup_{i \in I} A_i) = \cap_{i \in I}(B \setminus A_i)$.

(c) Can you discover and prove a similar theorem about $B \setminus (\cap_{i \in I} A_i)$? (Hint: Try to guess the theorem, and then try to prove it. If you can't finish the proof, it might be because your guess was wrong. Change your guess and try again.)

*23. Suppose $\{A_i \mid i \in I\}$ and $\{B_i \mid i \in I\}$ are indexed families of sets and $I \neq \varnothing$.

(a) Prove that $\cup_{i \in I}(A_i \setminus B_i) \subseteq (\cup_{i \in I} A_i) \setminus (\cap_{i \in I} B_i)$.

(b) Find an example for which $\cup_{i \in I}(A_i \setminus B_i) \neq (\cup_{i \in I} A_i) \setminus (\cap_{i \in I} B_i)$.

24. Suppose $\{A_i \mid i \in I\}$ and $\{B_i \mid i \in I\}$ are indexed families of sets.

(a) Prove that $\cup_{i \in I}(A_i \cap B_i) \subseteq (\cup_{i \in I} A_i) \cap (\cup_{i \in I} B_i)$.

(b) Find an example for which $\cup_{i \in I}(A_i \cap B_i) \neq (\cup_{i \in I} A_i) \cap (\cup_{i \in I} B_i)$.

25. Prove that for all integers a and b there is an integer c such that $a \mid c$ and $b \mid c$.

26. (a) Prove that for every integer n, $15 \mid n$ iff $3 \mid n$ and $5 \mid n$.

(b) Prove that it is *not* true that for every integer n, $60 \mid n$ iff $6 \mid n$ and $10 \mid n$.

3.5. Proofs Involving Disjunctions

Suppose one of your givens in a proof has the form $P \vee Q$. This given tells you that either P or Q is true, but it doesn't tell you which. Thus, there are two possibilities that you must take into account. One way to do the proof would be to consider these two possibilities in turn. In other words, first assume that P is true and use this assumption to prove your goal. Then assume Q is true and give another proof that the goal is true. Although you don't know which of these assumptions is correct, the given $P \vee Q$ tells you that *one* of them must be correct. Whichever one it is, you have shown that it implies the goal. Thus, the goal must be true.

The two possibilities that are considered separately in this type of proof – the possibility that P is true and the possibility that Q is true – are called *cases*. The given $P \vee Q$ justifies the use of these two cases by guaranteeing that these cases cover all of the possibilities. Mathematicians say in this situation that the cases are *exhaustive*. Any proof can be broken into two or more cases at any time, as long as the cases are exhaustive.

To use a given of the form $P \vee Q$:

Break your proof into cases. For case 1, assume that P is true and use this assumption to prove the goal. For case 2, assume Q is true and give another proof of the goal.

Scratch work

Before using strategy:

Givens	*Goal*
$P \vee Q$	—
—	

After using strategy:

Case 1: Givens	*Goal*
P	—
—	
Case 2: Givens	*Goal*
Q	—
—	

Form of final proof:

Case 1. P is true.
[Proof of goal goes here.]

Case 2. Q is true.

[Proof of goal goes here.]

Since we know $P \vee Q$, these cases cover all the possibilities. Therefore the goal must be true.

Example 3.5.1. Suppose that A, B, and C are sets. Prove that if $A \subseteq C$ and $B \subseteq C$ then $A \cup B \subseteq C$.

Scratch work

We assume $A \subseteq C$ and $B \subseteq C$ and prove $A \cup B \subseteq C$. Writing out the goal using logical symbols gives us the following givens and goal:

Givens	*Goal*
$A \subseteq C$	$\forall x(x \in A \cup B \rightarrow x \in C)$
$B \subseteq C$	

To prove the goal we let x be arbitrary, assume $x \in A \cup B$, and try to prove $x \in C$. Thus, we now have a new given $x \in A \cup B$, which we write as $x \in A \vee x \in B$, and our goal is now $x \in C$.

Givens	*Goal*
$A \subseteq C$	$x \in C$
$B \subseteq C$	
$x \in A \vee x \in B$	

Because the goal cannot be analyzed any further at this point, we look more closely at the givens. The first given will be useful if we ever come across an object that is an element of A, since it would allow us to conclude immediately that this object must also be an element of C. Similarly, the second given will be useful if we come across an element of B. Keeping in mind that we should watch for any elements of A or B that might come up, we move on to the third given. Because this given has the form $P \vee Q$, we try proof by cases. For the first case we assume $x \in A$, and for the second we assume $x \in B$. In the first case we therefore have the following givens and goal:

Givens	*Goal*
$A \subseteq C$	$x \in C$
$B \subseteq C$	
$x \in A$	

We've already decided that if we ever come across an element of A, we can use the first given to conclude that it is also an element of C. Since we now have $x \in A$ as a given, we can conclude that $x \in C$, which is our goal. The reasoning for the second case is quite similar, using the second given instead of the first.

Solution

Theorem. *Suppose that A, B, and C are sets. If $A \subseteq C$ and $B \subseteq C$ then $A \cup B \subseteq C$.*

Proof. Suppose $A \subseteq C$ and $B \subseteq C$, and let x be an arbitrary element of $A \cup B$. Then either $x \in A$ or $x \in B$.

Case 1. $x \in A$. Then since $A \subseteq C$, $x \in C$.

Case 2. $x \in B$. Then since $B \subseteq C$, $x \in C$.

Since we know that either $x \in A$ or $x \in B$, these cases cover all the possibilities, so we can conclude that $x \in C$. Since x was an arbitrary element of $A \cup B$, this means that $A \cup B \subseteq C$. □

Note that the cases in this proof are not *exclusive*. In other words, it is possible for both $x \in A$ and $x \in B$ to be true, so some values of x might fall under both cases. There is nothing wrong with this. The cases in a proof by cases must cover all possibilities, but there is no harm in covering some possibilities more than once. In other words, the cases must be exhaustive, but they need not be exclusive.

Proof by cases is sometimes also helpful if you are proving a goal of the form $P \vee Q$. If you can prove P in some cases and Q in others, then as long as your cases are exhaustive you can conclude that $P \vee Q$ is true. This method is particularly useful if one of the givens also has the form of a disjunction, because then you can use the cases suggested by this given.

To prove a goal of the form $P \vee Q$:

Break your proof into cases. In each case, either prove P or prove Q.

Example 3.5.2. Suppose that *A, B* and *C* are sets. Prove that $A \setminus (B \setminus C) \subseteq (A \setminus B) \cup C$.

Scratch work

Because the goal is $\forall x(x \in A \setminus (B \setminus C) \rightarrow x \in (A \setminus B) \cup C)$, we let x be arbitrary, assume $x \in A \setminus (B \setminus C)$, and try to prove $x \in (A \setminus B) \cup C$. Writing these statements out in logical symbols gives us:

Givens	*Goal*
$x \in A \wedge \neg(x \in B \wedge x \notin C)$	$(x \in A \wedge x \notin B) \vee x \in C$

We split the given into two separate givens, $x \in A$ and $\neg(x \in B \wedge x \notin C)$, and since the second is a negated statement we use one of DeMorgan's laws to reexpress it as the positive statement $x \notin B \vee x \in C$.

Givens	*Goal*
$x \in A$	$(x \in A \wedge x \notin B) \vee x \in C$
$x \notin B \vee x \in C$	

Now the second given and the goal are both disjunctions, so we'll try considering the two cases $x \notin B$ and $x \in C$ suggested by the second given. According to our strategy for proving goals of the form $P \vee Q$, if in each case we can either prove $x \in A \wedge x \notin B$ or prove $x \in C$, then the proof will be complete. For the first case we assume $x \notin B$.

Givens	*Goal*
$x \in A$	$(x \in A \wedge x \notin B) \vee x \in C$
$x \notin B$	

In this case the goal is clearly true, because in fact we can conclude that $x \in A \wedge x \notin B$. For the second case we assume $x \in C$, and once again the goal is clearly true.

Solution

Theorem. *Suppose that A, B, and C are sets. Then* $A \setminus (B \setminus C) \subseteq (A \setminus B) \cup C$.

Proof. Suppose $x \in A \setminus (B \setminus C)$. Then $x \in A$ and $x \notin B \setminus C$. Since $x \notin B \setminus C$, it follows that either $x \notin B$ or $x \in C$. We will consider these cases separately.

Case 1. $x \notin B$. Then since $x \in A$, $x \in A \setminus B$, so $x \in (A \setminus B) \cup C$.

Case 2. $x \in C$. Then clearly $x \in (A \setminus B) \cup C$.

Since x was an arbitrary element of $A \setminus (B \setminus C)$, we can conclude that $A \setminus (B \setminus C) \subseteq (A \setminus B) \cup C$. □

Sometimes you may find it useful to break a proof into cases even if the cases are not suggested by a given of the form $P \vee Q$. Any proof can be broken into cases at any time, as long as the cases exhaust all of the possibilities.

Example 3.5.3. Prove that for every integer x, the remainder when x^2 is divided by 4 is either 0 or 1.

Scratch work

We start by letting x be an arbitrary integer and then try to prove that the remainder when x^2 is divided by 4 is either 0 or 1.

Givens	*Goal*
$x \in \mathbb{Z}$	$(x^2 \div 4 \text{ has remainder } 0) \vee (x^2 \div 4 \text{ has remainder } 1)$

Because the goal is a disjunction, breaking the proof into cases seems like a likely approach, but there is no given that suggests what cases to use. However, trying out a few values for x suggests the right cases:

x	x^2	quotient of $x^2 \div 4$	remainder of $x^2 \div 4$
1	1	0	1
2	4	1	0
3	9	2	1
4	16	4	0
5	25	6	1
6	36	9	0

It appears that the remainder is 0 when x is even and 1 when x is odd. These are the cases we will use. Thus, for case 1 we assume x is even and try to prove that the remainder is 0, and for case 2 we assume x is odd and prove that the remainder is 1. Because every integer is either even or odd, these cases are exhaustive.

Filling in the definition of *even*, here are our givens and goal for case 1:

Givens	*Goal*
$x \in \mathbb{Z}$	$x^2 \div 4$ has remainder 0
$\exists k \in \mathbb{Z}(x = 2k)$	

We immediately use the second given and let k stand for some particular integer for which $x = 2k$. Then $x^2 = (2k)^2 = 4k^2$, so clearly when we divide x^2 by 4 the quotient is k^2 and the remainder is 0.

Case 2 is quite similar:

Givens	*Goal*
$x \in \mathbb{Z}$	$x^2 \div 4$ has remainder 1
$\exists k \in \mathbb{Z}(x = 2k + 1)$	

Once again we use the second given immediately and let k stand for an integer for which $x = 2k + 1$. Then $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, so when x^2 is divided by 4 the quotient is $k^2 + k$ and the remainder is 1.

Solution

Theorem. *For every integer x, the remainder when x^2 is divided by 4 is either 0 or 1.*

Proof. Suppose x is an integer. We consider two cases.

Case 1. x is even. Then $x = 2k$ for some integer k, so $x^2 = 4k^2$. Clearly the remainder when x^2 is divided by 4 is 0.

Case 2. x is odd. Then $x = 2k + 1$ for some integer k, so $x^2 = 4k^2 + 4k + 1$. Clearly in this case the remainder when x^2 is divided by 4 is 1. □

Sometimes in a proof of a goal that has the form $P \vee Q$ it is hard to figure out how to break the proof into cases. Here's a way of doing it that is often helpful. Simply assume that P is true in case 1 and assume that it is false in case 2. Certainly P is either true or false, so these cases are exhaustive. In the first case you have assumed that P is true, so certainly the goal $P \vee Q$ is true. Thus, no further reasoning is needed in case 1. In the second case you have assumed that P is false, so the only way the goal $P \vee Q$ could be true is if Q is true. Thus, to complete this case you should try to prove Q.

To prove a goal of the form $P \vee Q$:

If P is true, then clearly the goal $P \vee Q$ is true, so you only need to worry about the case in which P is false. You can complete the proof in this case by proving that Q is true.

Scratch work

Before using strategy:

Givens	*Goal*
—	$P \vee Q$
—	

After using strategy:

Givens	*Goal*
—	Q
—	
$\neg P$	

Form of final proof:

> If P is true, then of course $P \vee Q$ is true. Now suppose P is false.
>
> [Proof of Q goes here.]
>
> Thus, $P \vee Q$ is true.

Thus, this strategy for proving $P \vee Q$ suggests that you transform the problem by adding $\neg P$ as a new given and changing the goal to Q. It is interesting to note that this is exactly the same as the transformation you would use if you were proving the goal $\neg P \rightarrow Q$! This is not really surprising, because we already know that the statements $P \vee Q$ and $\neg P \rightarrow Q$ are equivalent. But we derived this equivalence before from the truth table for the conditional connective, and this truth table may have been hard to understand at first. Perhaps the reasoning we've given makes this equivalence, and therefore the truth table for the conditional connective, seem more natural.

Of course, the roles of P and Q could be reversed in using this strategy. Thus, you can also prove $P \vee Q$ by assuming that Q is false and proving P.

Example 3.5.4. Prove that for every real number x, if $x^2 \geq x$ then either $x \leq 0$ or $x \geq 1$.

Scratch work

Our goal is $\forall x(x^2 \geq x \rightarrow (x \leq 0 \vee x \geq 1))$, so to get started we let x be an arbitrary real number, assume $x^2 \geq x$, and set $x \leq 0 \vee x \geq 1$ as our goal:

Givens	*Goal*
$x^2 \geq x$	$x \leq 0 \vee x \geq 1$

According to our strategy, to prove this goal we can either assume $x > 0$ and prove $x \geq 1$ or assume $x < 1$ and prove $x \leq 0$. The assumption that x is positive seems more likely to be useful in reasoning about inequalities, so we take the first approach.

Givens	*Goal*
$x^2 \geq x$	$x \geq 1$
$x > 0$	

The proof is now easy. Since $x > 0$, we can divide the given inequality $x^2 \geq x$ by x to get the goal $x \geq 1$.

Solution

Theorem. *For every real number x, if $x^2 \geq x$ then either $x \leq 0$ or $x \geq 1$.*

Proof. Suppose $x^2 \geq x$. If $x \leq 0$, then of course $x \leq 0$ or $x \geq 1$. Now suppose $x > 0$. Then we can divide both sides of the inequality $x^2 \geq x$ by x to conclude that $x \geq 1$. Thus, either $x \leq 0$ or $x \geq 1$. □

The equivalence of $P \vee Q$ and $\neg P \rightarrow Q$ also suggests a rule of inference called *disjunctive syllogism* for using a given statement of the form $P \vee Q$:

To use a given of the form $P \vee Q$:

If you are also given $\neg P$, or you can prove that P is false, then you can use this given to conclude that Q is true. Similarly, if you are given $\neg Q$ or can prove that Q is false, then you can conclude that P is true.

In fact, this rule is the one we used in our first example of deductive reasoning in Chapter 1!

Once again, we end this section with a proof for you to read without the benefit of a preliminary scratch work analysis.

Theorem 3.5.5. *Suppose m and n are integers. If mn is even, then either m is even or n is even.*

Proof. Suppose mn is even. Then we can choose an integer k such that $mn = 2k$. If m is even then there is nothing more to prove, so suppose m is odd. Then $m = 2j + 1$ for some integer j. Substituting this into the equation $mn = 2k$, we get $(2j + 1)n = 2k$, so $2jn + n = 2k$, and therefore $n = 2k - 2jn = 2(k - jn)$. Since $k - jn$ is an integer, it follows that n is even. □

Commentary. The overall form of the proof is the following:

> Suppose mn is even.
>
> > If m is even, then clearly either m is even or n is even. Now suppose m is not even. Then m is odd.
> >
> > > [Proof that n is even goes here.]
> >
> > Therefore either m is even or n is even.
>
> Therefore if mn is even then either m is even or n is even.

The assumptions that mn is even and m is odd lead, by existential instantiation, to the equations $mn = 2k$ and $m = 2j + 1$. Although the proof doesn't say so explicitly, you are expected to work out for yourself that in order to prove that n is even it suffices to find an integer c such that $n = 2c$. Straightforward algebra leads to the equation $n = 2(k - jn)$, so the choice $c = k - jn$ works.

Exercises

PD*1. Suppose A, B, and C are sets. Prove that $A \cap (B \cup C) \subseteq (A \cap B) \cup C$.

PD2. Suppose A, B, and C are sets. Prove that $(A \cup B) \setminus C \subseteq A \cup (B \setminus C)$.

PD3. Suppose A and B are sets. Prove that $A \setminus (A \setminus B) = A \cap B$.

PD*4. Suppose $A \cap C \subseteq B \cap C$ and $A \cup C \subseteq B \cup C$. Prove that $A \subseteq B$.

PD5. Recall from Section 1.4 that the symmetric difference of two sets A and B is the set $A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$. Prove that if $A \triangle B \subseteq A$ then $B \subseteq A$.

PD6. Suppose A, B, and C are sets. Prove that $A \cup C \subseteq B \cup C$ iff $A \setminus C \subseteq B \setminus C$.

PD*7. Prove that for any sets A and B, $\mathscr{P}(A) \cup \mathscr{P}(B) \subseteq \mathscr{P}(A \cup B)$.

PD8. Prove that for any sets A and B, if $\mathscr{P}(A) \cup \mathscr{P}(B) = \mathscr{P}(A \cup B)$ then either $A \subseteq B$ or $B \subseteq A$.

9. Suppose x and y are real numbers and $x \neq 0$. Prove that $y + 1/x = 1 + y/x$ iff either $x = 1$ or $y = 1$.

10. Prove that for every real number x, if $|x - 3| > 3$ then $x^2 > 6x$. (Hint: According to the definition of $|x - 3|$, if $x - 3 \geq 0$ then $|x - 3| = x - 3$, and if $x - 3 < 0$ then $|x - 3| = 3 - x$. The easiest way to use this fact is to break your proof into cases. Assume that $x - 3 \geq 0$ in case 1, and $x - 3 < 0$ in case 2.)

*11. Prove that for every real number x, $|2x - 6| > x$ iff $|x - 4| > 2$. (Hint: Read the hint for exercise 10.)

12. (a) Prove that for all real numbers a and b, $|a| \leq b$ iff $-b \leq a \leq b$.
 (b) Prove that for any real number x, $-|x| \leq x \leq |x|$. (Hint: Use part (a).)
 (c) Prove that for all real numbers x and y, $|x + y| \leq |x| + |y|$. (This is called the *triangle inequality*. One way to prove this is to combine parts (a) and (b), but you can also do it by considering a number of cases.)

13. Prove that for every integer x, $x^2 + x$ is even.

14. Prove that for every integer x, the remainder when x^4 is divided by 8 is either 0 or 1.

*15. Suppose $\mathcal{F}$ and $\mathcal{G}$ are nonempty families of sets.
 PD(a) Prove that $\cup(\mathcal{F} \cup \mathcal{G}) = (\cup\mathcal{F}) \cup (\cup\mathcal{G})$.
 (b) Can you discover and prove a similar theorem about $\cap(\mathcal{F} \cup \mathcal{G})$?

16. Suppose $\mathcal{F}$ is a nonempty family of sets and B is a set.
 PD(a) Prove that $B \cup (\cup\mathcal{F}) = \cup(\mathcal{F} \cup \{B\})$.
 (b) Prove that $B \cup (\cap\mathcal{F}) = \cap_{A \in \mathcal{F}}(B \cup A)$.
 (c) Can you discover and prove a similar theorem about $B \cap (\cap\mathcal{F})$?

17. Suppose $\mathcal{F}$, $\mathcal{G}$, and $\mathcal{H}$ are nonempty families of sets and for every $A \in \mathcal{F}$ and every $B \in \mathcal{G}$, $A \cup B \in \mathcal{H}$. Prove that $\cap\mathcal{H} \subseteq (\cap\mathcal{F}) \cup (\cap\mathcal{G})$.

PD18. Suppose A and B are sets. Prove that $\forall x(x \in A \triangle B \leftrightarrow (x \in A \leftrightarrow x \notin B))$.

PD*19. Suppose A, B, and C are sets. Prove that $A \triangle B$ and C are disjoint iff $A \cap C = B \cap C$.

PD20. Suppose A, B, and C are sets. Prove that $A \triangle B \subseteq C$ iff $A \cup C = B \cup C$.

PD21. Suppose A, B, and C are sets. Prove that $C \subseteq A \triangle B$ iff $C \subseteq A \cup B$ and $A \cap B \cap C = \varnothing$.

PD*22. Suppose A, B, and C are sets.
 (a) Prove that $A \setminus C \subseteq (A \setminus B) \cup (B \setminus C)$.
 (b) Prove that $A \triangle C \subseteq (A \triangle B) \cup (B \triangle C)$.

PD*23. Suppose A, B, and C are sets.

(a) Prove that $(A \cup B) \triangle C \subseteq (A \triangle C) \cup (B \triangle C)$.

(b) Find an example of sets A, B, and C such that $(A \cup B) \triangle C \neq (A \triangle C) \cup (B \triangle C)$

PD24. Suppose A, B, and C are sets.

(a) Prove that $(A \triangle C) \cap (B \triangle C) \subseteq (A \cap B) \triangle C$.

(b) Is it always true that $(A \cap B) \triangle C \subseteq (A \triangle C) \cap (B \triangle C)$? Give either a proof or a counterexample.

PD25. Suppose A, B, and C are sets. Consider the sets $(A \setminus B) \triangle C$ and $(A \triangle C) \setminus (B \triangle C)$. Can you prove that either is a subset of the other? Justify your conclusions with either proofs or counterexamples.

*26. Consider the following putative theorem.

Theorem? *For every real number x, if $|x - 3| < 3$ then $0 < x < 6$.*

Is the following proof correct? If so, what proof strategies does it use? If not, can it be fixed? Is the theorem correct?

Proof. Let x be an arbitrary real number, and suppose $|x - 3| < 3$. We consider two cases:

Case 1. $x - 3 \geq 0$. Then $|x - 3| = x - 3$. Plugging this into the assumption that $|x - 3| < 3$, we get $x - 3 < 3$, so clearly $x < 6$.

Case 2. $x - 3 < 0$. Then $|x - 3| = 3 - x$, so the assumption $|x - 3| < 3$ means that $3 - x < 3$. Therefore $3 < 3 + x$, so $0 < x$.

Since we have proven both $0 < x$ and $x < 6$, we can conclude that $0 < x < 6$. □

27. Consider the following putative theorem.

Theorem? *For any sets A, B, and* C, *if $A \setminus B \subseteq C$ and $A \nsubseteq C$ then $A \cap B \neq \varnothing$.*

Is the following proof correct? If so, what proof strategies does it use? If not, can it be fixed? Is the theorem correct?

Proof. Since $A \nsubseteq C$, we can choose some x such that $x \in A$ and $x \notin C$. Since $x \notin C$ and $A \setminus B \subseteq C, x \notin A \setminus B$. Therefore either $x \notin A$ or $x \in B$. But we already know that $x \in A$, so it follows that $x \in B$. Since $x \in A$ and $x \in B, x \in A \cap B$. Therefore $A \cap B \neq \varnothing$. □

*28. Consider the following putative theorem.

Theorem? $\forall x \in \mathbb{R} \exists y \in \mathbb{R}(xy^2 \neq y - x)$.

Is the following proof correct? If so, what proof strategies does it use? If not, can it be fixed? Is the theorem correct?

Proof. Let x be an arbitrary real number.

Case 1. $x = 0$. Let $y = 1$. Then $xy^2 = 0$ and $y - x = 1 - 0 = 1$, so $xy^2 \neq y - x$.

Case 2. $x \neq 0$. Let $y = 0$. Then $xy^2 = 0$ and $y - x = -x \neq 0$, so $xy^2 \neq y - x$.

Since these cases are exhaustive, we have shown that $\exists y \in \mathbb{R}(xy^2 \neq y - x)$. Since x was arbitrary, this shows that $\forall x \in \mathbb{R} \exists y \in \mathbb{R}(xy^2 \neq y - x)$. □

29. Prove that if $\forall x P(x) \to \exists x Q(x)$ then $\exists x(P(x) \to Q(x))$. (Hint: Remember that $P \to Q$ is equivalent to $\neg P \vee Q$).

*30. Consider the following putative theorem.

Theorem? *Suppose A, B, and C are sets and $A \subseteq B \cup C$. Then either $A \subseteq B$ or $A \subseteq C$.*

Is the following proof correct? If so, what proof strategies does it use? If not, can it be fixed? Is the theorem correct?

Proof. Let x be an arbitrary element of A. Since $A \subseteq B \cup C$, it follows that either $x \in B$ or $x \in C$.

Case 1. $x \in B$. Since x was an arbitrary element of A, it follows that $\forall x \in A(x \in B)$, which means that $A \subseteq B$.

Case 2. $x \in C$. Similarly, since x was an arbitrary element of A, we can conclude that $A \subseteq C$.

Thus, either $A \subseteq B$ or $A \subseteq C$. □

31. Prove $\exists x(P(x) \to \forall y\, P(y))$.

3.6. Existence and Uniqueness Proofs

In this section we consider proofs in which the goal has the form $\exists! x\, P(x)$. As we saw in Section 2.2, this can be thought of as an abbreviation for the formula $\exists x(P(x) \wedge \neg\exists y(P(y) \wedge y \neq x))$. According to the proof strategies discussed in previous sections, we could therefore prove this goal by finding a particular value of x for which we could prove both $P(x)$ and $\neg\exists y(P(y) \wedge y \neq x)$. The last part of this proof would involve proving a negated statement, but we can reexpress it as an equivalent positive statement:

$\neg\exists y(P(y) \wedge y \neq x)$

is equivalent to $\forall y \neg(P(y) \wedge y \neq x)$ (quantifier negation law),

which is equivalent to $\forall y(\neg P(y) \vee y = x)$ (DeMorgan's law),

which is equivalent to $\forall y(P(y) \to y = x)$ (conditional law).

Thus, we see that $\exists! x\, P(x)$ could also be written as $\exists x(P(x) \wedge \forall y(P(y) \rightarrow y = x))$. In fact, as the next example shows, several other formulas are also equivalent to $\exists! x\, P(x)$, and they suggest other approaches to proving goals of this form.

Example 3.6.1. Prove that the following formulas are all equivalent:

1. $\exists x(P(x) \wedge \forall y(P(y) \rightarrow y = x))$.
2. $\exists x \forall y(P(y) \leftrightarrow y = x)$.
3. $\exists x\, P(x) \wedge \forall y \forall z((P(y) \wedge P(z)) \rightarrow y = z)$.

Scratch work

If we prove directly that each of these statements is equivalent to each of the others, then we will have three biconditionals to prove: statement 1 iff statement 2, statement 1 iff statement 3, and statement 2 iff statement 3. If we prove each biconditional by the methods of Section 3.4, then each will involve two conditional proofs, so we will need a total of six conditional proofs. Fortunately, there is an easier way. We will prove that statement 1 implies statement 2, statement 2 implies statement 3, and statement 3 implies statement 1 – just three conditionals. Although we will not give a separate proof that statement 2 implies statement 1, it will follow from the fact that statement 2 implies statement 3 and statement 3 implies statement 1. Similarly, the other two conditionals follow from the three we will prove. Mathematicians almost always use some such shortcut when proving that several statements are all equivalent. Because we'll be proving three conditional statements, our proof will have three parts, which we will label $1 \rightarrow 2$, $2 \rightarrow 3$, and $3 \rightarrow 1$. We'll need to work out our strategy for the three parts separately.

$1 \rightarrow 2$. We assume statement 1 and prove statement 2. Because statement 1 starts with an existential quantifier, we choose a name, say x_0, for some object for which both $P(x_0)$ and $\forall y(P(y) \rightarrow y = x_0)$ are true. Thus, we now have the following situation:

Givens	*Goal*
$P(x_0)$	$\exists x \forall y(P(y) \leftrightarrow y = x)$
$\forall y(P(y) \rightarrow y = x_0)$	

Our goal also starts with an existential quantifier, so to prove it we should try to find a value of x that makes the rest of the statement come out true. Of course, the obvious choice is $x = x_0$. Plugging in x_0 for x, we see that we must now prove $\forall y(P(y) \leftrightarrow y = x_0)$. We let y be arbitrary and prove both directions of the biconditional. The → direction is clear by the second given.

For the ← direction, suppose $y = x_0$. We also have $P(x_0)$ as a given, and plugging in y for x_0 in this given we get $P(y)$.

$2 \rightarrow 3$. Statement 2 is an existential statement, so we let x_0 be some object such that $\forall y(P(y) \leftrightarrow y = x_0)$. The goal, statement 3, is a conjunction, so we treat it as two separate goals.

Givens	*Goals*
$\forall y(P(y) \leftrightarrow y = x_0)$	$\exists x P(x)$
	$\forall y \forall z((P(y) \wedge P(z)) \rightarrow y = z)$

To prove the first goal we must choose a value for x, and of course the obvious value is $x = x_0$ again. Thus, we must prove $P(x_0)$. The natural way to use our only given is to plug in something for y; and to prove the goal $P(x_0)$, the obvious thing to plug in is x_0. This gives us $P(x_0) \leftrightarrow x_0 = x_0$. Of course, $x_0 = x_0$ is true, so by the ← direction of the biconditional, we get $P(x_0)$.

For the second goal, we let y and z be arbitrary, assume $P(y)$ and $P(z)$, and try to prove $y = z$.

Givens	*Goal*
$\forall y(P(y) \leftrightarrow y = x_0)$	$y = z$
$P(y)$	
$P(z)$	

Plugging in each of y and z in the first given we get $P(y) \leftrightarrow y = x_0$ and $P(z) \leftrightarrow z = x_0$. Since we've assumed $P(y)$ and $P(z)$, this time we use the → directions of these biconditionals to conclude that $y = x_0$ and $z = x_0$. Our goal $y = z$ clearly follows.

$3 \rightarrow 1$. Because statement 3 is a conjunction, we treat it as two separate givens. The first is an existential statement, so we let x_0 stand for some object such that $P(x_0)$ is true. To prove statement 1 we again let $x = x_0$, so we have this situation:

Givens	*Goal*
$P(x_0)$	$P(x_0) \wedge \forall y(P(y) \rightarrow y = x_0)$
$\forall y \forall z((P(y) \wedge P(z)) \rightarrow y = z)$	

We already know the first half of the goal, so we only need to prove the second. For this we let y be arbitrary, assume $P(y)$, and make $y = x_0$ our goal.

Givens	*Goal*
$P(x_0)$	$y = x_0$
$\forall y \forall z((P(y) \wedge P(z)) \rightarrow y = z)$	
$P(y)$	

But now we know both $P(y)$ and $P(x_0)$, so the goal $y = x_0$ follows from the second given.

Solution

Theorem. *The following are equivalent:*

1. $\exists x(P(x) \land \forall y(P(y) \to y = x))$.
2. $\exists x \forall y(P(y) \leftrightarrow y = x)$.
3. $\exists x P(x) \land \forall y \forall z((P(y) \land P(z)) \to y = z)$.

Proof. 1 → 2. By statement 1, we can let x_0 be some object such that $P(x_0)$ and $\forall y(P(y) \to y = x_0)$. To prove statement 2 we will show that $\forall y(P(y) \leftrightarrow y = x_0)$. We already know the → direction. For the ← direction, suppose $y = x_0$. Then since we know $P(x_0)$, we can conclude $P(y)$.

2 → 3. By statement 2, choose x_0 such that $\forall y(P(y) \leftrightarrow y = x_0)$. Then, in particular, $P(x_0) \leftrightarrow x_0 = x_0$, and since clearly $x_0 = x_0$, it follows that $P(x_0)$ is true. Thus, $\exists x P(x)$. To prove the second half of statement 3, let y and z be arbitrary and suppose $P(y)$ and $P(z)$. Then by our choice of x_0 (as something for which $\forall y(P(y) \leftrightarrow y = x_0)$ is true), it follows that $y = x_0$ and $z = x_0$, so $y = z$.

3 → 1. By the first half of statement 3, let x_0 be some object such that $P(x_0)$. Statement 1 will follow if we can show that $\forall y(P(y) \to y = x_0)$, so suppose $P(y)$. Since we now have both $P(x_0)$ and $P(y)$, by the second half of statement 3 we can conclude that $y = x_0$, as required. □

Because all three of the statements in the theorem are equivalent to $\exists! x P(x)$, we can prove a goal of this form by proving any of the three statements in the theorem. Probably the most common technique for proving a goal of the form $\exists! x P(x)$ is to prove statement 3 of the theorem.

To prove a goal of the form $\exists! x P(x)$:

Prove $\exists x P(x)$ and $\forall y \forall z((P(y) \land P(z)) \to y = z)$. The first of these goals shows that there exists an x such that $P(x)$ is true, and the second shows that it is unique. The two parts of the proof are therefore sometimes labeled *existence* and *uniqueness*. Each part is proven using strategies discussed earlier.

Form of final proof:

Existence: [Proof of $\exists x P(x)$ goes here.]
Uniqueness: [Proof of $\forall y \forall z((P(y) \land P(z)) \to y = z)$ goes here.]

Example 3.6.2. Prove that there is a unique set A such that for every set B, $A \cup B = B$.

Scratch work

Our goal is $\exists! A\, P(A)$, where $P(A)$ is the statement $\forall B(A \cup B = B)$. According to our strategy, we can prove this by proving existence and uniqueness separately. For the existence half of the proof we must prove $\exists A\, P(A)$, so we try to find a value of A that makes $P(A)$ true. There is no formula for finding this set A, but if you think about what the statement $P(A)$ means, you should realize that the right choice is $A = \varnothing$. Plugging this value in for A, we see that to complete the existence half of the proof we must show that $\forall B(\varnothing \cup B = B)$. This is clearly true. (If you're not sure of this, work out the proof!)

For the uniqueness half of the proof we prove $\forall C \forall D((P(C) \wedge P(D)) \rightarrow C = D)$. To do this, we let C and D be arbitrary, assume $P(C)$ and $P(D)$, and prove $C = D$. Writing out what the statements $P(C)$ and $P(D)$ mean, we have the following givens and goal:

Givens	*Goal*
$\forall B(C \cup B = B)$	$C = D$
$\forall B(D \cup B = B)$	

To use the givens, we should try to find something to plug in for B in each of them. There is a clever choice that makes the rest of the proof easy: We plug in D for B in the first given, and C for B in the second. This gives us $C \cup D = D$ and $D \cup C = C$. But clearly $C \cup D = D \cup C$. (If you don't see why, prove it!) The goal $C = D$ follows immediately.

Solution

Theorem. *There is a unique set A such that for every set B*, $A \cup B = B$.

Proof. Existence: Clearly $\forall B(\varnothing \cup B = B)$, so $\varnothing$ has the required property.

Uniqueness: Suppose $\forall B(C \cup B = B)$ and $\forall B(D \cup B = B)$. Applying the first of these assumptions to D we see that $C \cup D = D$, and applying the second to C we get $D \cup C = C$. But clearly $C \cup D = D \cup C$, so $C = D$. □

Sometimes a statement of the form $\exists! x\, P(x)$ is proven by proving statement 1 from Example 3.6.1. This leads to the following proof strategy.

To prove a goal of the form $\exists! x\, P(x)$:

Prove $\exists x(P(x) \wedge \forall y(P(y) \rightarrow y = x))$, using strategies from previous sections.

Example 3.6.3. Prove that for every real number x, if $x \neq 2$ then there is a unique real number y such that $2y/(y + 1) = x$.

Scratch work

Our goal is $\forall x(x \neq 2 \rightarrow \exists! y(2y/(y+1) = x))$. We therefore let x be arbitrary, assume $x \neq 2$, and prove $\exists! y(2y/(y+1) = x)$. According to the preceding strategy, we can prove this goal by proving the equivalent statement $\exists y(2y/(y+1) = x \wedge \forall z(2z/(z+1) = x \rightarrow z = y))$. We start by trying to find a value of y that will make the equation $2y/(y+1) = x$ come out true. In other words, we solve this equation for y:

$$\frac{2y}{y+1} = x \;\Rightarrow\; 2y = x(y+1) \;\Rightarrow\; y(2-x) = x \;\Rightarrow\; y = \frac{x}{2-x}.$$

Note that we have $x \neq 2$ as a given, so the division by $2 - x$ in the last step makes sense. Of course, these steps will not appear in the proof. We simply let $y = x/(2-x)$ and try to prove both $2y/(y+1) = x$ and $\forall z(2z/(z+1) = x \rightarrow z = y)$.

Givens	*Goals*
$x \neq 2$	$\dfrac{2y}{y+1} = x$
$y = \dfrac{x}{2-x}$	$\forall z\left(\dfrac{2z}{z+1} = x \rightarrow z = y\right)$

The first goal is easy to verify by simply plugging in $x/(2-x)$ for y. For the second, we let z be arbitrary, assume $2z/(z+1) = x$, and prove $z = y$:

Givens	*Goal*
$x \neq 2$	$z = y$
$y = \dfrac{x}{2-x}$	
$\dfrac{2z}{z+1} = x$	

We can show that $z = y$ now by solving for z in the third given:

$$\frac{2z}{z+1} = x \quad\Rightarrow\quad 2z = x(z+1) \quad\Rightarrow\quad z(2-x) = x \quad\Rightarrow\quad z = \frac{x}{2-x} = y.$$

Note that the steps we used here are exactly the same as the steps we used earlier in solving for y. This is a common pattern in existence and uniqueness proofs. Although the scratch work for figuring out an existence proof should not appear in the proof, this scratch work, or reasoning similar to it, can sometimes be used to prove that the object shown to exist is unique.

Solution

Theorem. *For every real number x, if $x \neq 2$ then there is a unique real number y such that $2y/(y+1) = x$.*

Proof. Let x be an arbitrary real number, and suppose $x \neq 2$. Let $y = x/(2-x)$, which is defined since $x \neq 2$. Then

$$\frac{2y}{y+1} = \frac{\frac{2x}{2-x}}{\frac{x}{2-x}+1} = \frac{\frac{2x}{2-x}}{\frac{2}{2-x}} = \frac{2x}{2} = x.$$

To see that this solution is unique, suppose $2z/(z+1) = x$. Then $2z = x(z+1)$, so $z(2-x) = x$. Since $x \neq 2$ we can divide both sides by $2-x$ to get $z = x/(2-x) = y$. □

The theorem in Example 3.6.1 can also be used to formulate strategies for using givens of the form $\exists! x\, P(x)$. Once again, statement 3 of the theorem is the one used most often.

To use a given of the form $\exists! x\, P(x)$:

Treat this as two given statements, $\exists x\, P(x)$ and $\forall y \forall z((P(y) \wedge P(z)) \rightarrow y = z)$. To use the first statement you should probably choose a name, say x_0, to stand for some object such that $P(x_0)$ is true. The second tells you that if you ever come across two objects y and z such that $P(y)$ and $P(z)$ are both true, you can conclude that $y = z$.

Example 3.6.4. Suppose *A, B,* and *C* are sets, *A* and *B* are not disjoint, *A* and *C* are not disjoint, and *A* has exactly one element. Prove that *B* and *C* are not disjoint.

Scratch work

Givens	*Goal*
$A \cap B \neq \varnothing$	$B \cap C \neq \varnothing$
$A \cap C \neq \varnothing$	
$\exists! x(x \in A)$	

We treat the last given as two separate givens, as suggested by our strategy. Writing out the meanings of the other givens and the goal, we have the following situation:

Givens	*Goal*
$\exists x(x \in A \wedge x \in B)$	$\exists x(x \in B \wedge x \in C)$
$\exists x(x \in A \wedge x \in C)$	
$\exists x(x \in A)$	
$\forall y \forall z((y \in A \wedge z \in A) \rightarrow y = z)$	

To prove the goal, we must find something that is an element of both *B* and *C*. To do this, we turn to the givens. The first given tells us that we can choose a name, say b, for something such that $b \in A$ and $b \in B$. Similarly, by the second given we can let c be something such that $c \in A$ and $c \in C$. At this point the third given is redundant. We already know that there's something in A, because in fact we already know that $b \in A$ and $c \in A$. We may as well skip to the last given, which says that if we ever come across two objects that are elements of A, we can conclude that they are equal. But as we have just observed, we know that $b \in A$ and $c \in A$! We can therefore conclude that $b = c$. Since $b \in B$ and $b = c \in C$, we have found something that is an element of both B and C, as required to prove the goal.

Solution

Theorem. *Suppose A, B, and C are sets, A and B are not disjoint, A and C are not disjoint, and A has exactly one element. Then B and C are not disjoint.*

Proof. Since A and B are not disjoint, we can let b be something such that $b \in A$ and $b \in B$. Similarly, since A and C are not disjoint, there is some object c such that $c \in A$ and $c \in C$. Since A has only one element, we must have $b = c$. Thus $b = c \in B \cap C$ and therefore B and C are not disjoint. □

Exercises

*1. Prove that for every real number x there is a unique real number y such that $x^2 y = x - y$.

2. Prove that there is a unique real number x such that for every real number y, $xy + x - 4 = 4y$.

3. Prove that for every real number x, if $x \neq 0$ and $x \neq 1$ then there is a unique real number y such that $y/x = y - x$.

*4. Prove that for every real number x, if $x \neq 0$ then there is a unique real number y such that for every real number z, $zy = z/x$.

5. Recall that if $\mathcal{F}$ is a family of sets, then $\cup\mathcal{F} = \{x \mid \exists A(A \in \mathcal{F} \wedge x \in A)\}$. Suppose we define a new set $\cup!\mathcal{F}$ by the formula $\cup!\mathcal{F} = \{x \mid \exists! A(A \in \mathcal{F} \wedge x \in A)\}$.
   (a) Prove that for any family of sets $\mathcal{F}$, $\cup!\mathcal{F} \subseteq \cup\mathcal{F}$.
   (b) A family of sets $\mathcal{F}$ is said to be *pairwise disjoint* if every pair of distinct elements of $\mathcal{F}$ are disjoint; that is, $\forall A \in \mathcal{F} \forall B \in \mathcal{F}(A \neq B \rightarrow A \cap B = \varnothing)$. Prove that for any family of sets $\mathcal{F}$, $\cup!\mathcal{F} = \cup\mathcal{F}$ iff $\mathcal{F}$ is pairwise disjoint.

PD*6. Let U be any set.
   (a) Prove that there is a unique $A \in \mathscr{P}(U)$ such that for every $B \in \mathscr{P}(U)$, $A \cup B = B$.

(b) Prove that there is a unique $A \in \mathscr{P}(U)$ such that for every $B \in \mathscr{P}(U)$, $A \cup B = A$.

PD7. Let U be any set.

(a) Prove that there is a unique $A \in \mathscr{P}(U)$ such that for every $B \in \mathscr{P}(U)$, $A \cap B = B$.

(b) Prove that there is a unique $A \in \mathscr{P}(U)$ such that for every $B \in \mathscr{P}(U)$, $A \cap B = A$.

PD8. Let U be any set.

(a) Prove that for every $A \in \mathscr{P}(U)$ there is a unique $B \in \mathscr{P}(U)$ such that for every $C \in \mathscr{P}(U)$, $C \setminus A = C \cap B$.

(b) Prove that for every $A \in \mathscr{P}(U)$ there is a unique $B \in \mathscr{P}(U)$ such that for every $C \in \mathscr{P}(U)$, $C \cap A = C \setminus B$.

PD9. Recall that you showed in exercise 12 of Section 1.4 that symmetric difference is associative; in other words, for all sets A, B, and C, $A \triangle (B \triangle C) = (A \triangle B) \triangle C$. You may also find it useful in this problem to note that symmetric difference is clearly commutative; in other words, for all sets A and B, $A \triangle B = B \triangle A$.

(a) Prove that there is a unique identity element for symmetric difference. In other words, there is a unique set X such that for every set A, $A \triangle X = A$.

(b) Prove that every set has a unique inverse for the operation of symmetric difference. In other words, for every set A there is a unique set B such that $A \triangle B = X$, where X is the identity element from part (a).

(c) Prove that for any sets A and B there is a unique set C such that $A \triangle C = B$.

(d) Prove that for every set A there is a unique set $B \subseteq A$ such that for every set $C \subseteq A$, $B \triangle C = A \setminus C$.

PD10. Suppose A is a set, and for every family of sets $\mathcal{F}$, if $\cup\mathcal{F} = A$ then $A \in \mathcal{F}$. Prove that A has exactly one element. (Hint: For both the existence and uniqueness parts of the proof, try proof by contradiction.)

PD*11. Suppose $\mathcal{F}$ is a family of sets that has the property that for every $\mathcal{G} \subseteq \mathcal{F}$, $\cup\mathcal{G} \in \mathcal{F}$. Prove that there is a unique set A such that $A \in \mathcal{F}$ and $\forall B \in \mathcal{F}(B \subseteq A)$.

12. (a) Suppose $P(x)$ is a statement with a free variable x. Find a formula, using the logical symbols we have studied, that means "there are exactly two values of x for which $P(x)$ is true."

(b) Based on your answer to part (a), design a proof strategy for proving a statement of the form "there are exactly two values of x for which $P(x)$ is true."

(c) Prove that there are exactly two solutions to the equation $x^3 = x^2$.

3.7. More Examples of Proofs

So far, most of our proofs have involved fairly straightforward applications of the proof techniques we've discussed. We end this chapter with a few examples of somewhat more difficult proofs. These proofs use the techniques of this chapter, but for various reasons they're a little harder than most of our earlier proofs. Some are simply longer, involving the application of more proof strategies. Some require clever choices of which strategies to use. In some cases it's clear what strategy to use, but some insight is required to see exactly how to use it. Our earlier examples, which were intended only to illustrate and clarify the proof techniques, may have made proof-writing seem mechanical and dull. We hope that by studying these more difficult examples you will begin to see that mathematical reasoning can also be surprising and beautiful.

Some proof techniques are particularly difficult to apply. For example, when you're proving a goal of the form $\exists x\, P(x)$, the obvious way to proceed is to try to find a value of x that makes the statement $P(x)$ true, but sometimes it will not be obvious how to find that value of x. Using a given of the form $\forall x\, P(x)$ is similar. You'll probably want to plug in a particular value for x, but to complete the proof you may have to make a clever choice of what to plug in. Proofs that must be broken down into cases are also sometimes difficult to figure out. It is sometimes hard to know when to use cases and what cases to use.

We begin by looking again at the proofs from the introduction. Some aspects of these proofs probably seemed somewhat mysterious when you read them in the introduction. See if they make more sense to you now that you have a better understanding of how proofs are constructed. We will present each proof exactly as it appeared in the introduction and then follow it with a commentary discussing the proof techniques used.

Theorem 3.7.1. *Suppose n is an integer larger than 1 and n is not prime. Then $2^n - 1$ is not prime.*

Proof. Since n is not prime, there are positive integers a and b such that $a < n$, $b < n$, and $n = ab$. Let $x = 2^b - 1$ and $y = 1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}$. Then

$$\begin{aligned}
xy &= (2^b - 1) \cdot (1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) \\
&= 2^b \cdot (1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) - (1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) \\
&= (2^b + 2^{2b} + 2^{3b} + \cdots + 2^{ab}) - (1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) \\
&= 2^{ab} - 1 \\
&= 2^n - 1.
\end{aligned}$$

Since $b < n$, we can conclude that $x = 2^b - 1 < 2^n - 1$. Also, since $ab = n > a$, it follows that $b > 1$. Therefore, $x = 2^b - 1 > 2^1 - 1 = 1$, so $y < xy = 2^n - 1$. Thus, we have shown that $2^n - 1$ can be written as the product of two positive integers x and y, both of which are smaller than $2^n - 1$, so $2^n - 1$ is not prime. □

Commentary. We are given that n is not prime, and we must prove that $2^n - 1$ is not prime. Both of these are negative statements, but fortunately it is easy to reexpress them as positive statements. To say that an integer larger than 1 is not prime means that it can be written as a product of two smaller positive integers. Thus, the hypothesis that n is not prime means $\exists a \in \mathbb{Z}^+ \exists b \in \mathbb{Z}^+(ab = n \wedge a < n \wedge b < n)$, and what we must prove is that $2^n - 1$ is not prime, which means $\exists x \in \mathbb{Z}^+ \exists y \in \mathbb{Z}^+(xy = 2^n - 1 \wedge x < 2^n - 1 \wedge y < 2^n - 1)$. In the second sentence of the proof we apply existential instantiation to the hypothesis that n is not prime, and the rest of the proof is devoted to exhibiting numbers x and y with the properties required to prove that $2^n - 1$ is not prime.

As usual in proofs of existential statements, the proof doesn't explain how the values of x and y were chosen, it simply demonstrates that these values work. After the values of x and y have been given, the goal remaining to be proven is $xy = 2^n - 1 \wedge x < 2^n - 1 \wedge y < 2^n - 1$. Of course, this is treated as three separate goals, which are proven one at a time. The proofs of these three goals involve only elementary algebra.

One of the attractive features of this proof is the calculation used to show that $xy = 2^n - 1$. The formulas for x and y are somewhat complicated, and at first their product looks even more complicated. It is a pleasant surprise when most of the terms in this product cancel and, as if by magic, the answer $2^n - 1$ appears. Of course, we can see with hindsight that it was this calculation that motivated the choice of x and y. There is, however, one aspect of this calculation that may bother you. The use of "$\cdots$" in the formulas indicates that the proof depends on a pattern in the calculation that is not being spelled out. We'll give a more rigorous proof that $xy = 2^n - 1$ in Chapter 6, after we have introduced the method of proof by mathematical induction.

Theorem 3.7.2. *There are infinitely many prime numbers.*

Proof. Suppose there are only finitely many prime numbers. Let $p_1, p_2, \ldots, p_n$ be a list of all prime numbers. Let $m = p_1 p_2 \cdots p_n + 1$. Note that m is not divisible by p_1, since dividing m by p_1 gives a quotient of $p_2 p_3 \cdots p_n$ and a remainder of 1. Similarly, m is not divisible by any of $p_2, p_3 \ldots, p_n$.

We now use the fact that every integer larger than 1 is either prime or can be written as a product of primes. (We'll see a proof of this fact in Chapter 6.) Clearly m is larger than 1, so m is either prime or a product of primes. Suppose first that m is prime. Note that m is larger than all of the numbers in the list $p_1, p_2, \ldots, p_n$, so we've found a prime number not in this list. But this contradicts our assumption that this was a list of *all* prime numbers.

Now suppose m is a product of primes. Let q be one of the primes in this product. Then m is divisible by q. But we've already seen that m is not divisible by any of the numbers in the list $p_1, p_2, \ldots, p_n$, so once again we have a contradiction with the assumption that this list included all prime numbers.

Since the assumption that there are finitely many prime numbers has led to a contradiction, there must be infinitely many prime numbers. □

Commentary. Because *infinite* means *not finite*, the statement of the theorem might be considered to be a negative statement. It is therefore not surprising that the proof proceeds by contradiction. The assumption that there are finitely many primes means that there exists a natural number n such that there are n primes, and the statement that there are n primes means that there is a list of distinct numbers $p_1, p_2, \ldots, p_n$ such that every number in the list is prime, and there are no primes that are not in the list. Thus, the second sentence of the proof applies existential instantiation to introduce the numbers n and $p_1, p_2, \ldots, p_n$ into the proof. At this point in the proof we have the following situation:

Givens	*Goal*
$p_1, p_2, \ldots, p_n$ are all prime	Contradiction
$\neg\exists q(q \text{ is prime} \wedge q \notin \{p_1, p_2 \ldots, p_n\})$	

The second given could be reexpressed as a positive statement, but since we are doing a proof by contradiction, another reasonable approach would be to try to reach a contradiction by proving that $\exists q(q \text{ is prime} \wedge q \notin \{p_1, p_2, \ldots, p_n\})$. This is the strategy used in the proof. Thus, the goal for the rest of the proof is to show that there is a prime number not in the list $p_1, p_2, \ldots, p_n$ – an "unlisted prime."

Because our goal is now an existential statement, it is not surprising that the next step in the proof is to introduce the new number m, without any explanation of how m was chosen. What *is* surprising is that m may or may not be the unlisted prime we are looking for. The problem is that m might not be prime. All we can be sure of is that m is either prime or a product of primes. Because this statement is a disjunction, it suggests proof by cases, and this is the method used in the rest of the proof. Although the cases are not explicitly labeled as cases in the proof, it is important to realize that the rest of the proof has the form of a proof by cases. In case 1 we assume that m is prime, and in case 2 we assume that it is a product of primes. In both cases we are able to produce an unlisted prime as required to complete the proof.

Theorem 3.7.3. *For every positive integer n, there is a sequence of n consecutive positive integers containing no primes.*

Proof. Suppose n is a positive integer. Let $x = (n+1)! + 2$. We will show that none of the numbers $x, x+1, x+2, \cdots, x+(n-1)$ is prime. Since this is a sequence of n consecutive positive integers, this will prove the theorem.

To see that x is not prime, note that

$$\begin{aligned} x &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n+1) + 2 \\ &= 2 \cdot (1 \cdot 3 \cdot 4 \cdots (n+1) + 1). \end{aligned}$$

Thus, x can be written as a product of two smaller positive integers, so x is not prime.

Similarly, we have

$$\begin{aligned} x+1 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n+1) + 3 \\ &= 3 \cdot (1 \cdot 2 \cdot 4 \cdots (n+1) + 1), \end{aligned}$$

so $x+1$ is also not prime. In general, consider any number $x+i$, where $0 \leq i \leq n-1$. Then we have

$$\begin{aligned} x+i &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n+1) + (i+2) \\ &= (i+2) \cdot (1 \cdot 2 \cdot 3 \cdots (i+1) \cdot (i+3) \cdots (n+1) + 1), \end{aligned}$$

so $x+i$ is not prime. □

Commentary. A sequence of n consecutive positive integers is a sequence of the form $x, x+1, x+2, \ldots, x+(n-1)$, where x is a positive integer. Thus, the logical form of the statement to be proven is $\forall n > 0 \exists x > 0 \forall i (0 \leq i \leq n-1 \rightarrow x+i$ is not prime), where all variables range over the integers. The overall plan of the proof is exactly what one would expect for a proof of a statement of this form: We let $n > 0$ be arbitrary, specify a value for x, let i be arbitrary, and then assume that $0 \leq i \leq n-1$ and prove that $x+i$ is not prime. As in the proof of Theorem 3.7.1, to prove that $x+i$ is not prime we show how to write it as a product of two smaller integers.

Before the demonstration that $x+i$ is not prime, where i is an arbitrary integer between 0 and $n-1$, the proof includes verifications that x and $x+1$

are not prime. These are completely unnecessary and are only included to make the proof easier to read.

For readers who are familiar with the definition of limits from calculus, we give one more example, showing how proofs involving limits can be worked out using the techniques in this chapter. Readers who are not familiar with this definition should skip this example.

Example 3.7.4. Show that $\lim_{x \to 3} \dfrac{2x^2 - 5x - 3}{x - 3} = 7$.

Scratch work

According to the definition of limits, our goal means that for every positive number ε there is a positive number δ such that if x is any number such that $0 < |x - 3| < \delta$, then $\left|\frac{2x^2-5x-3}{x-3} - 7\right| < \varepsilon$. Translating this into logical symbols, we have

$$\forall \varepsilon > 0 \exists \delta > 0 \forall x \left(0 < |x - 3| < \delta \rightarrow \left|\frac{2x^2 - 5x - 3}{x - 3} - 7\right| < \varepsilon\right).$$

We therefore start by letting ε be an arbitrary positive number and then try to find a positive number δ for which we can prove

$$\forall x \left(0 < |x - 3| < \delta \rightarrow \left|\frac{2x^2 - 5x - 3}{x - 3} - 7\right| < \varepsilon\right).$$

The scratch work involved in finding δ will not appear in the proof, of course. In the final proof we'll just write "Let δ = (some positive number)" and then proceed to prove

$$\forall x \left(0 < |x - 3| < \delta \rightarrow \left|\frac{2x^2 - 5x - 3}{x - 3} - 7\right| < \varepsilon\right).$$

Before working out the value of δ, let's figure out what the rest of the proof will look like. Based on the form of the goal at this point, we should proceed by letting x be arbitrary, assuming $0 < |x - 3| < \delta$, and then proving $\left|\frac{2x^2-5x-3}{x-3} - 7\right| < \varepsilon$. Thus, the entire proof will have the following form:

```
Let $\varepsilon$ be an arbitrary positive number.
  Let $\delta$ = (some positive number).
    Let $x$ be arbitrary.
      Suppose $0 < |x - 3| < \delta$.
        [Proof of $\left|\frac{2x^2-5x-3}{x-3} - 7\right| < \varepsilon$ goes here.]
      Therefore $0 < |x - 3| < \delta \rightarrow \left|\frac{2x^2-5x-3}{x-3} - 7\right| < \varepsilon$.
```

Since x was arbitrary, we can conclude that $\forall x(0 < |x-3| < \delta \to \left|\frac{2x^2-5x-3}{x-3} - 7\right| < \varepsilon)$.

Therefore $\exists\delta > 0\forall x\big(0 < |x-3| < \delta \to \left|\frac{2x^2-5x-3}{x-3} - 7\right| < \varepsilon\big)$.

Since ε was arbitrary, it follows that $\forall\varepsilon > 0\exists\delta > 0\forall x\big(0 < |x-3| < \delta \to \left|\frac{2x^2-5x-3}{x-3} - 7\right| < \varepsilon\big)$.

Two steps remain to be worked out. We must decide what value to assign to δ, and we must fill in the proof of $\left|\frac{2x^2-5x-3}{x-3} - 7\right| < \varepsilon$. We'll work on the second of these steps first, and in the course of working out this step it will become clear what value we should use for δ. The givens and goal for this second step are as follows:

Givens	*Goal*
$\varepsilon > 0$	$\left\lvert\dfrac{2x^2-5x-3}{x-3} - 7\right\rvert < \varepsilon$
$\delta =$ (some positive number)	
$0 < \lvert x-3\rvert < \delta$	

First of all, note that we have $0 < |x-3|$ as a given, so $x \neq 3$ and therefore the fraction $\frac{2x^2-5x-3}{x-3}$ is defined. Factoring the numerator, we find that

$$\begin{aligned}\left|\frac{2x^2-5x-3}{x-3} - 7\right| &= \left|\frac{(2x+1)(x-3)}{x-3} - 7\right| \\ &= |2x+1-7| = |2x-6| = 2|x-3|.\end{aligned}$$

Now we also have as a given that $|x-3| < \delta$, so $2|x-3| < 2\delta$. Combining this with the previous equation, we get $\left|\frac{2x^2-5x-3}{x-3} - 7\right| < 2\delta$, and our goal is $\left|\frac{2x^2-5x-3}{x-3} - 7\right| < \varepsilon$. Thus, if we chose δ so that $2\delta = \varepsilon$, we'd be done. In other words, we should let $\delta = \varepsilon/2$. Note that since $\varepsilon > 0$, this is a positive number, as required.

Solution

Theorem. $\lim\limits_{x\to 3} \frac{2x^2-5x-3}{x-3} = 7$.

Proof. Suppose $\varepsilon > 0$. Let $\delta = \varepsilon/2$, which is also clearly positive. Let x be an arbitrary real number, and suppose that $0 < |x-3| < \delta$. Then

$$\begin{aligned}\left|\frac{2x^2-5x-3}{x-3} - 7\right| &= \left|\frac{(2x+1)(x-3)}{x-3} - 7\right| \\ &= |2x+1-7| = |2x-6| \\ &= 2|x-3| < 2\delta = 2\left(\frac{\varepsilon}{2}\right) = \varepsilon.\end{aligned}$$

□

Exercises

*1. Suppose $\mathcal{F}$ is a family of sets. Prove that there is a unique set A that has the following two properties:
(a) $\mathcal{F} \subseteq \mathscr{P}(A)$.
(b) $\forall B(\mathcal{F} \subseteq \mathscr{P}(B) \rightarrow A \subseteq B)$.
(Hint: First try an example. Let $\mathcal{F} = \{\{1, 2, 3\}, \{2, 3, 4\}, \{3, 4, 5\}\}$. Can you find the set A that has properties (a) and (b)?)

2. Suppose A and B are sets. What can you prove about $\mathscr{P}(A \setminus B) \setminus (\mathscr{P}(A) \setminus \mathscr{P}(B))$? (No, it's not equal to $\varnothing$. Try some examples and see what you get.)

3. Suppose that A, B, and C are sets. Prove that the following statements are equivalent:
(a) $(A \triangle C) \cap (B \triangle C) = \varnothing$.
(b) $A \cap B \subseteq C \subseteq A \cup B$.
(c) $A \triangle C \subseteq A \triangle B$.

*4. Suppose $\{A_i \mid i \in I\}$ is a family of sets. Prove that if $\mathscr{P}(\cup_{i \in I} A_i) \subseteq \cup_{i \in I} \mathscr{P}(A_i)$, then there is some $i \in I$ such that $\forall j \in I(A_j \subseteq A_i)$.

5. Suppose $\mathcal{F}$ is a nonempty family of sets. Let $I = \cup\mathcal{F}$ and $J = \cap\mathcal{F}$. Suppose also that $J \neq \varnothing$, and notice that it follows that for every $X \in \mathcal{F}$, $X \neq \varnothing$, and also that $I \neq \varnothing$. Finally, suppose that $\{A_i \mid i \in I\}$ is an indexed family of sets.
(a) Prove that $\cup_{i \in I} A_i = \cup_{X \in \mathcal{F}}(\cup_{i \in X} A_i)$.
(b) Prove that $\cap_{i \in I} A_i = \cap_{X \in \mathcal{F}}(\cap_{i \in X} A_i)$.
(c) Prove that $\cup_{i \in J} A_i \subseteq \cap_{X \in \mathcal{F}}(\cup_{i \in X} A_i)$. Is it always true that $\cup_{i \in J} A_i = \cap_{X \in \mathcal{F}}(\cup_{i \in X} A_i)$? Give either a proof or a counterexample to justify your answer.
(d) Discover and prove a theorem relating $\cap_{i \in J} A_i$ and $\cup_{X \in \mathcal{F}}(\cap_{i \in X} A_i)$.

6. Prove that $\lim\limits_{x \to 2} \frac{3x^2 - 12}{x - 2} = 12$.

*7. Prove that if $\lim\limits_{x \to c} f(x) = L$ and $L > 0$, then there is some number $\delta > 0$ such that for all x, if $0 < |x - c| < \delta$ then $f(x) > 0$.

8. Prove that if $\lim\limits_{x \to c} f(x) = L$ then $\lim\limits_{x \to c} 7f(x) = 7L$.

*9. Consider the following putative theorem.

Theorem. *There are irrational numbers a and b such that a^b is rational.*

Is the following proof correct? If so, what proof strategies does it use? If not, can it be fixed? Is the theorem correct? (Note: The proof uses the fact that $\sqrt{2}$ is irrational, which we'll prove in Chapter 6.)

Proof. Either $\sqrt{2}^{\sqrt{2}}$ is rational or it's irrational.

Case 1. $\sqrt{2}^{\sqrt{2}}$ is rational. Let $a = b = \sqrt{2}$. Then a and b are irrational, and $a^b = \sqrt{2}^{\sqrt{2}}$, which we are assuming in this case is rational.

Case 2. $\sqrt{2}^{\sqrt{2}}$ is irrational. Let $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$. Then a is irrational by assumption, and we know that b is also irrational. Also, $a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} = (\sqrt{2})^2 = 2$, which is rational. □