DEDUCTIVE MATHEMATICS
—an Introduction to Proof and Discovery.
Second Edition.

Andrew Wohlgemuth

DEDUCTIVE MATHEMATICS
—an Introduction to Proof and Discovery.
Second Edition.

Contents

Logical Deduction ... is the one and only true powerhouse of mathematical thinking.

Jean Dieudonne

Introduction

If you asked an educated person where scientific knowledge comes from, you very well could get the answer: "From the scientific method". If you asked an educated person where mathematical knowledge comes from, you probably would not get an answer. This text is written to provide that answer. And it will do it, by leading readers to discover their own, completely rigorous, completely new (to them) mathematical results.

There are two sorts of things that are called axioms in mathematics. The first sort is a set of obviously true statements about an idealized object, which statements are taken as a given starting point for logical deductions about other objects. The axioms of Euclidean geometry, the geometry we studied in high school, were self-evident truths about our idealizations of planes, lines, points, circles. The second sort depends on the fact that in mathematics a true statement about (almost) anything depends entirely on the definition of that thing. To show something is true about a mathematical object, one must show it follows logically from the object's definition.

The way an object is defined is to say what general category it falls in, and then add what makes this thing special – within that category. For example, a square is defined as a rectangle that has all sides of equal length. Of course one has to know beforehand what a rectangle is: a quadrilateral with interior angles all right angles. And, of course, this process of using previously defined categories can't go on forever. There have to be some undefined things to start with. Axioms (of the second sort) are just the statements that are assumed to be true about these undefined objects.

Mathematics that is developed from the second sort of axioms is frequently called *abstract* or *formal* mathematics. Axioms in formal mathematics are not "self-evident" truths. Logically, they would have to be seen as pure conventions. But efforts at starting with truly unmotivated and arbitrary axioms and objects have never produced anything of any interest. In practice, mathematicians have "examples" that motivate the things they study formally – so that the facts (called theorems) derived from the formal axioms are true about their examples. And, if the theorems are going to be useful, true about other examples.

Logical deduction is a very powerful tool that is useful for studying all sorts of things. Non-Euclidean geometries – the geometries that actually model our real universe – were discovered by tweaking one of the axioms of Euclidean geometry, and studying the results formally. And, remarkably, what is self evident about our idealization of a plane and space is not self evident about our universe. And, remarkaby again, what is self evident about our idealization of the natural numbers, 1, 2, 3, ... and so on, is self evident about our universe.

Axioms of the first sort have been part of education for a long time. The second paragraph of our Declaration of Independence starts out with, "We hold these truths to be self evident … ." The entire context for axioms of the second sort (formal mathematics) is, however, typically absent from all students' education, unless they may become mathematics majors.

Mathematics has two fundamental aspects: (1) discovery/logical deduction and (2) description/ computation. Discovery/deductive mathematics asks the questions:

1. What is true about this thing being studied?
2. How do we know it is true?

On the other hand, descriptive/computational mathematics asks questions of the type:

3. What is the particular number, function, and so on, that satisfies ... ?
4. How can we find the number, function, and so on?

In descriptive/computational mathematics, typically some pictorial, physical, or business situation is described mathematically, and then computational techniques are applied to the

mathematical description, in order to find values of interest. The foregoing is frequently called "problem solving". Examples of the third question such as "How many feet of fence will be needed by a farmer to enclose ..." are familiar. The first two questions, however, are unfamiliar to most. The teaching of computational techniques continues to be the overwhelming focus of mathematics education. For most people, the techniques, and their application to real world or business problems, *are* mathematics. Mathematics is understood only in its descriptive role in providing a language for scientific, technical, and business areas.

Mathematics, however, is really a deductive science. Mathematical knowledge comes from people looking at examples, and getting an idea of what may be true in general. Their idea is put down formally as a statement—a conjecture. The statement is then shown to be a logical consequence of what we already know. The way this is done is by logical deduction. The mathematician Jean Dieudonne has called logical deduction "the one and only true powerhouse of mathematical thinking"[1]. And learning how to construct a logical argument is at least as worthy a component of a general education as is learning how to compute.

The deductive and descriptive aspects of mathematics are complementary—not antagonistic—they motivate and enrich each other. The relation between the two aspects has been a source of wonder to thoughtful people[2].

This text presents a system designed to enable students to find and construct their own logical arguments. The system is first applied to elementary ideas about sets and subsets and the set operations of union, intersection, and difference—which are now generally introduced prior to high school. These set operations and relations so closely follow the logic used in elementary mathematical arguments, that students using the system are naturally prepared to prove any (true) conjectures they might discover about them. It is an easy entry into the world of discovery/ deductive mathematics. It enables students to verify the validity of their own conjectures—as the conjectures are being made.

The system is based on a bottom-up approach. Certain things are best learned from the bottom up: programming in a specific programming language, for example, or learning how to play chess. In the bottom-up learning, there ought to be no doubt of what constitutes a valid chess move on a valid chess board. Other things, such as speaking in one's own native language, are learned from the top down. As we learn to speak, grammar (which would be analogous to the rules of the game for chess) is not even part of our consciousness. Grammatical rules are followed only because they are used implicitly by those that we imitate. If the people around us use poor grammar, we nevertheless learn to feel it is "right"—and we speak the same way.

The system in this text is based on a number of formal inference rules that model what a mathematician would do naturally to prove certain sorts of statements. The rules make explicit the logic used implicitly by mathematicians.[3] After experience is gained, the explicit use of the formal rules is replaced by implicit reference. Thus, in our bottom-up approach, the explicit precedes the implicit. The initial, formal step-by-step format (which allows for the explicit reference to the rules) is replaced by a narrative format—where only critical things need to be mentioned Thus the student is lead up to the sort of narrative proofs traditionally found in text books. At every stage in the process, the student is always aware of what is and what is not a proof—and has specific guidance in the form of a "step discovery procedure" that leads to a proof outline.

.

---

[1] J. Dieudonne, *Linear Algebra and Geometry*, Hermann, Paris, 1969, page 14.

[2] John Polkinghorne in his *The Way the World Is* (Wm B. Eerdmans, Grand Rapids, MI, 1984, page 9) states, "Again and again in physical science we find that it is the abstract structures of pure mathematics which provide the clue to understanding the world. It is a recognized *technique* in fundamental physics to seek theories which have an elegant and economical (you can say beautiful) mathematical form, in the expectation that they will prove the ones realized in nature. General relativity, the modern theory of gravitation, was invented by Einstein in just such a way. Now mathematics is the free creation of the human mind, and it is surely a surprising and significant thing that a discipline apparently so unearthed should provide the key with which to turn the lock of the world."

[3] Although the rules resemble those of formal logic, they were developed solely to help students struggling with proof—without any input from formal logic.

Propositions

A set is a collection of things viewed as a whole—as a single thing itself. Our primary examples will be sets of *natural numbers*—the numbers $1, 2, 3, 4, 5, \ldots$. The things in a set are called *elements* or *members* of the set. The expression "$x \in A$" means that x is a member of set A, and is read "x is an element of A" or "x is a member of A". We frequently define a set by listing its elements between braces. Thus $\{1, 2, 3, 4\}$ and $\{2, 4, 6, 8, \ldots\}$ are sets. $\{1, 2, 3, 4, 5, 6, \ldots\}$ would be the entire set of natural numbers. This set is also denoted by $\mathbb{N}$. Thus $\mathbb{N} = \{1, 2, 3, 4, 5, 6, \ldots\}$. We will frequently take $\mathbb{N}$ to be our *universal set;* that is, all sets that we form will have elements taken from $\mathbb{N}$.

Example 1:

$2 \in \{1, 2, 3\}$, $1 \in \{1, 2, 3\}$, and $3 \in \{1, 2, 3\}$.

Most people think of mathematics in terms of computation and problem solving. In mathematics, however, logical deduction plays a more fundamental role than either computation or problem solving. Mathematics is deductive in nature. Deductive mathematics is concerned with mathematical *statements*, which are formal assertions that are either *true* or *false*. The set $\{1, 2, 3\}$ is *defined* to have the elements $1, 2,$ and 3, and no other elements, so the statement $2 \in \{1, 2, 3\}$ in Example 1 is true by the definition of the set $\{1, 2, 3\}$.

The statement $4 \in \{1, 2, 3\}$ is false. This fact can either be expressed informally, as in the preceding English sentence, or it can be expressed formally by the expression $\neg(4 \in \{1, 2, 3\})$. Since statements are the basis for deductive mathematics, we need some notation so that we can talk about statements in general. We will use script capital letters to denote statements. For example $\mathcal{P}$ might represent the statement $2 \in \{1, 2, 3\}$. If $\mathcal{Q}$ represents the statement $4 \in \{1, 2, 3\}$, then $\neg\mathcal{Q}$ represents the statement $\neg(4 \in \{1, 2, 3\})$. The expression "$\neg\mathcal{Q}$" is read "not $\mathcal{Q}$". The formal statement $\neg\mathcal{Q}$ is *true*, since $\mathcal{Q}$ is false. The notation "$\neg(x \in A)$" is almost always abbreviated "$x \notin A$", which we read "x is not in A." If the variable x occurs in the statement $\mathcal{P}$ (for example, if $\mathcal{P}$ is the statement $x \in \{1, 2, 3, 4, 5\}$), we may write $\mathcal{P}(x)$, instead of just $\mathcal{P}$— to emphasize the fact.

Example 2:

Let $\mathcal{P}$ represent the statement $1 \in \{1, 2, 3\}$, $\mathcal{Q}$ represent $2 \notin \{1, 2, 3\}$, and $\mathcal{R}$ represent $4 \in \{1, 2, 3\}$. Then:
$\mathcal{P}$ is true.
$\neg\mathcal{P}$ is false.
$\mathcal{Q}$ is false.
$\neg\mathcal{Q}$ is true.
$\mathcal{R}$ is false.
$\neg\mathcal{R}$ is true.

If $\mathcal{P}$ is any mathematical statement, the *negation* of $\mathcal{P}$ is the statement $\neg\mathcal{P}$. $\neg\mathcal{P}$ is defined to be true if $\mathcal{P}$ is false, and false if $\mathcal{P}$ is true.

In order not to complicate things too quickly, the only aspect of the natural numbers we will be concerned with for a while is the *order relation* $<$ (which is read "is less than"). Thus, for example, $1 < 2$ (read "one is less than two"), $36 < 42$, and so on. Later, we will consider the relation $<$ on the natural numbers from first principles, and define what it means, for example, for

$36 < 42$ to be true. For the moment, however, we use the relation $<$ only to provide computational examples for working with sets—the real objects of our current interest.

Mathematical knowledge comes from making conjectures (from examples) and showing that the conjectures are logical consequences of what we already know. Thus in mathematics we always need to assume something as a starting point. We assume as "given" facts such as $2 < 3$, $36 < 42$, and so on. Thus the statement $2 < 3$ is true, and $\neg(2 < 3)$ is false.

Letters and words that are part of formal statements are italicized. Thus far we have seen formal statements of the form $element \in set$ and $number < number$; for example, $2 \in A$ and $36 < 42$.

People do mathematics by first looking at examples—usually in small, easily understood special cases. By considering these examples, they get an idea of what may be true in general. The idea is then put down in precise mathematical language and called a *conjecture* or *proposition*. (It is "proposed".) The proposition is usually a general statement about what may be true about the thing being investigated. There is then an attempt to prove the proposition (to show that it is true) or to find a special case where the general statement does not hold (to show that it is false). Such a special case is called a *counterexample*.

The first step in finding either a proof or a counterexample is to break up the proposition into two pieces. One piece, the *conclusion*, is the formal statement that the proposition asserts to be true. The other piece consists of an identification of all the variables in the proposition, and all the conditions, called *hypotheses*, under which the conclusion is true. In our approach, we take the identification of symbols as part of the hypotheses.

Propositions are written in informal language, but contain formal statements. The conclusion is always a formal statement. The hypotheses contain formal statements and an identification of all symbols that appear in these statements and the conclusion.

Example 3:

Proposition: For sets A and B and a natural number x, if $x \in A$, then $x \in B$.

The hypotheses and conclusion are:

Hypotheses: A, B sets
x a natural number
$x \in A$

Conclusion: $x \in B$

It is probably easiest first to decide what formal statement the proposition asserts to be true (the conclusion), and second to decide on the formal conditions under which the conclusion is true (the hypotheses). The phrase "x a natural number" in the hypotheses above can be written "$x \in \mathbb{N}$".

Example 4:

Proposition: For natural numbers x, y, and z, if $x < y$ and $y < z$, then $x < z$.

Hypotheses: $x, y, z \in \mathbb{N}$
1. $x < y$
2. $y < z$

Conclusion: $x < z$

We call the determination of hypotheses and conclusion of a proposition an *hypotheses-conclusion interpretation* of the proposition. By identifying the proposition with its hypotheses-conclusion interpretation, we define the proposition to be true if for all possible values or examples of the variable symbols that make the hypotheses true, it is also the case that the conclusion is true. A proof establishes the truth of the proposition since it shows that the conclusion follows logically

from the hypotheses using valid rules of inference: thus the conclusion must be true if the hypotheses are true.

We define the proposition to be false if there is at least one assignment of the hypotheses variables that makes the hypotheses true but the conclusion false (a counterexample). Thus the proposition is true if there are no counterexamples.

Example 5:

Consider the proposition of Example 3:

For sets A and B and a natural number x, if $x \in A$, then $x \in B$.

Hypotheses: A, B sets
$x \in \mathbb{N}$
$x \in A$

Conclusion: $x \in B$

If we define $x = 2$, $A = \{1, 2, 3\}$, and $B = \{3, 4, 5\}$, we see that $x \in A$ is true but $x \in B$ is false. Thus we have a counterexample, and the proposition of Example 3 is false. If we define $x = 3$, $A = \{1, 2, 3\}$, and $B = \{3, 4, 5\}$, we see that $x \in A$ is true and $x \in B$ is also true. But this proves nothing.

An assignment of values to the variables in the hypotheses is called an "instance" of the proposition. A counterexample is therefore a single instance in which the hypotheses are true but the conclusion is false. Finding such an instance proves that the statement is false. In order to show that the statement is true by finding instances, we would need to find all instances in which the hypotheses were true, and then show that the conclusion was also true in these instances. This is almost never possible. Instead, statements are proved to be true by logical arguments.

Example 6:

Consider the proposition of Example 4:

For natural numbers x, y, and z, if $x < y$ and $y < z$, then $x < z$.

Hypotheses and conclusion are:

Hypotheses: $x, y, z \in \mathbb{N}$
1. $x < y$
2. $y < z$

Conclusion: $x < z$

An instance of the statement that makes the hypotheses and conclusion both true is:

Hypotheses: $4, 5, 6 \in \mathbb{N}$
$4 < 5$
$5 < 6$

Conclusion: $4 < 6$

There are no instances in which the hypotheses are true but the conclusion is false, since the proposition is true.

EXERCISES

1. For each proposition below, write the hypotheses and conclusion in the way they were written in Examples 3 through 6.

   (a) For all natural numbers x, y, z, if $x < y$ and $y < z$, then $x < z$.

   (b) If $a < b < c$ for natural numbers a, b, and c, then $b < 10$.

   (c) Let A and B be sets. Suppose $x \in A$. Prove $x \in B$.

   (d) Let $C = \{1, 2, 3, 4, 5\}$. If $a = 1$, then $a \in C$.

   (e) For sets X and Y: if $x \in X$, then $x \in Y$.

2. What propositions might be interpreted by the following hypotheses and conclusions?

   (a)

   Hypotheses: $x, y \in \mathbb{N}$
   $2 < x$
   $2 < y$

   Conclusion: $2 < xy$

   (b)

   Hypotheses: $x, y \in \mathbb{N}$
   $x < y$

   Conclusion: $2x < 2y$

   (c)

   Hypotheses: A, B sets
   $x \notin A$

   Conclusion: $x \in B$

3. Give a counterexample to each of the propositions in Exercise 1 that is false.

4. Give a counterexample to each of your statements in answer to Exercise 2 that is false.

Set Definitions

A proof is a sequence of formal statements (steps) such that each statement can be justified by an accepted form of reasoning. In our approach, justification for each step is given in parentheses after the step. Such justification includes (1) a list of the previous steps on which the new step depends, (2) a semicolon, and (3) a rule of inference or other accepted reason why the new step is a logical consequence of the earlier steps listed.

Example 1:

Consider the following steps, which might have come from a fragment of some proof:

4. $x < 3$
5. $3 < 9$
6. $x < 9$ (4, 5;_____)

In the proof fragment of Example 1, Step 6 is supposed to follow from Steps 4 and 5 by some justification that still needs to be filled in — in the underlined place. The property of the relation $<$ that allows us to do this is called *transitivity*. We will accept the transitive property of the relation $<$ as an *axiom*. Axioms have the same form as propositions, but we don't attempt to prove them. We merely accept them as true as a starting point.

Axiom Transitivity of $<$: For natural numbers $a, b,$ and c, if $a < b$ and $b < c$, then $a < c$.

Thus the underlined place in Example 1 is filled in as follows:

Solution:

4. $x < 3$
5. $3 < 9$
6. $x < 9$ (4, 5; Trans. $<$)

Example 2:

1. $x < 5$
2. $y < 7$
3. $5 < 7$
4. _____ (____; Trans. $<$)

Solution:

1. $x < 5$
2. $y < 7$
3. $5 < 7$
4. $x < 7$ (1, 3; Trans. $<$)

Example 2 illustrates a form we use for problems. You are to fill in the underlined places. In this example, we need to supply a step that will follow from previous steps by the transitivity axiom. We see that it is possible to conclude $x < 7$ from Steps 1 and 3 using this axiom.

A statement, such as $x < 6$, containing a variable can be used to define a set, namely, the set of all elements in the universal set that make the statement true when they are substituted for the variable. For example, the set of all natural numbers less than 6 is written $\{x \in \mathbb{N} \mid x < 6\}$. The set $S = \{y \in \mathbb{N} \mid 8 < y\}$ is read "the set of all y in $\mathbb{N}$ such that 8 is less than y". S can also be expressed by listing its elements. Thus $S = \{9, 10, 11, 12, 13, ...\}$.

In general, if $\mathcal{P}(x)$ is some statement about x, then we can define $\{x \in \mathbb{N} \mid \mathcal{P}(x)\}$ to be the set of all x in $\mathbb{N}$ such that $\mathcal{P}(x)$ is true. For example, if $\mathcal{P}(x)$ is the statement $100 < x$, then the set $\{x \in \mathbb{N} \mid \mathcal{P}(x)\}$ is the set $\{101, 102, 103, ...\}$. If the property $\mathcal{P}(x)$ is true for all x in $\mathbb{N}$, $\mathcal{P}(x)$ can still be used to define the set $\{x \in \mathbb{N} \mid \mathcal{P}(x)\}$, which would in this case be the entire set $\mathbb{N}$ of natural numbers. For example,

$$\{x \in \mathbb{N} \mid x + 3 = 3 + x\} = \mathbb{N}.$$

If $\mathcal{P}(x)$ is false for all x in $\mathbb{N}$, $\mathcal{P}(x)$ defines the set $\{x \in \mathbb{N} \mid \mathcal{P}(x)\}$, which will not have any elements in it at all. This set is called the *empty* set, and is denoted by $\emptyset$. Thus, for example,

$$\{x \in \mathbb{N} \mid x \neq x\} = \emptyset.$$

There are two general ways of defining a particular set: (1) by listing the elements of the set between braces, and (2) by giving a defining condition.

Example 3:

Define the set $A = \{3, 4, 5, 6, ...\}$ in terms of a defining condition that is a formal mathematical statement.

Solution:

$A = \{x \in \mathbb{N} \mid 2 < x\}$

Example 4:

Define the set $A = \{x \in \mathbb{N} \mid 7 < x\}$ by listing its elements.

Solution:

$A = \{8, 9, 10, 11, ...\}$

Suppose that $A = \{x \in \mathbb{N} \mid x < 5\}$. We consider the property $x < 5$ as the defining condition for the set A. If a is any natural number that satisfies the defining condition (that is, makes the property $x < 5$ true when substituted for x), then a is in the set A—by definition. Conversely, if c is any element in the set A, then c must satisfy the defining condition; that is, $c < 5$ must be true.

The following rule gives the two ways we can use the definition of a particular set in proof steps.

Inference Rule Using a set definition: If an element is in a set, then we may infer that it satisfies the condition defining the set. If an element satisfies the defining condition, then we may infer that it is in the set.

Example 5:

Let $B = \{x \in \mathbb{N} \mid x < 9\}$. The inference rule above allows us to infer Step 2 from Step 1 and Step 4 from Step 3 below.

1. $b \in B$
2. $b < 9$ (1; def. B)

3. $a < 9$
4. $a \in B$ (3; def. B)

In applying the rule for using set definitions, we assume that all elements are in our universal set, without asserting this explicitly in proof steps. Thus we assume that $a \in \mathbb{N}$ in Example 5, so that $a \in B$ follows solely from the fact (given in Step 3) that a satisfies the defining condition for B.

Example 6:

Define $A = \{x \in \mathbb{N} \mid x < 12\}$. The definition of A tells us why Step 2 follows from Step 1.

1. $a \in A$
2. $a < 12$ (1; def. A)

Example 7:

Define $A = \{x \in \mathbb{N} \mid x < 12\}$. If it is known, say from the hypotheses or from our universal set under consideration, that a is a natural number, then the definition of A tells us why Step 2 follows from Step 1.

1. $a < 12$
2. $a \in A$ (1; def. A)

Note in Example 7 that it is understood, but not stated in the proof steps, that $a \in \mathbb{N}$. Step 2 depends both on Step 1 and the fact that $a \in \mathbb{N}$, but it is not necessary to mention the latter.

Learning to do deductive mathematics can be compared with learning to play a game. The inference rules are like the rules of the game. We will also provide a very useful game strategy (a way of handling the inference rules) that will enable you to discover your own proofs. Your primary task for quite a while will be to learn the rules and the strategy. It is the explicit use of formal statements that allows us to explain the strategy.

Example 8:

Proposition

If $X = \{x \in \mathbb{N} \mid x < 12\}$ and $a \in X$, then $a < 20$.

We use the proposition of Example 8 to illustrate the strategy for discovering proof steps. The first step is to identify the hypotheses and conclusion. These are written down as "assume" and "show", when part of a proof. The hypotheses are numbered so that we can refer to them later.

Proof:

Assume: 1. $X = \{x \in \mathbb{N} \mid x < 12\}$
2. $a \in X$

Show: $a < 20$

Proofs are developed in a shaded area that represents a working area—such as a blackboard. The next step in writing the proof is to write the conclusion as the last step in the

proof. We identify this as Step k at this stage, since we have no idea how many steps will be needed to get there.

Proof:
Assume: 1. $X = \{x \in \mathbb{N} \mid x < 12\}$
2. $a \in X$
Show: $a < 20$

k. $a < 20$

The next thing to write down is the justification for the last step. This depends on the form of the last step—and what it means for the step to be true. Since the relation $<$ has not been defined, and since the only thing we know about $<$ is the axiom giving the transitive property of $<$, this must be the justification for the last step.

Proof:
Assume: 1. $X = \{x \in \mathbb{N} \mid x < 12\}$
2. $a \in X$
Show: $a < 20$

k. $a < 20$ (____; Trans. $<$)

Hypothesis 2 gives us Step 1:

Proof:
Assume: 1. $X = \{x \in \mathbb{N} \mid x < 12\}$
2. $a \in X$
Show: $a < 20$
1. $a \in X$ (hyp. 2)

k. $a < 20$ (____; Trans. $<$)

Step 1 is of the form $element \in set$. In order to use this information we use the definition of the set.

Proof:
Assume: 1. $X = \{x \in \mathbb{N} \mid x < 12\}$
2. $a \in X$
Show: $a < 20$

1. $a \in X$	(hyp. 2)
2. $a < 12$	(1, hyp.1; def.X)
.	
k. $a < 20$	(____; Trans. $<$)

In order to complete the proof, we need only to supply the step $12 < 20$ and use the transitive property.

1. $a \in X$	(hyp. 2)
2. $a < 12$	(1, hyp.1; def.X)
3. $12 < 20$	(given)
4. $a < 20$	(2, 3; Trans. $<$)

Step 2 follows from Step 1 and Hypothesis 1, by the definition of X. Since X is defined in Hypothesis 1, we leave out the redundant information. This gives the final version of the proof:

Proof:

Assume: 1. $X = \{x \in \mathbb{N} \mid x < 12\}$
2. $a \in X$

Show: $a < 20$

1. $a \in X$	(hyp. 2)
2. $a < 12$	(1; def.X)
3. $12 < 20$	(given)
4. $a < 20$	(2, 3; Trans. $<$)

□

The symbol □ signals the end of a complete proof.

Theorems are proven propositions that are important enough to be referred to later. The only important thing about the proposition of Example 8 is that you see how the proof works, so we won't call it a theorem.

In doing proofs, we assume that the hypotheses of the proposition being proved are *true* (for the sake of argument). Thus a proof is a sequence of statements (steps) the truth of each of which follows (by an accepted form of justification) from previous steps, hypotheses, theorems, and axioms.

EXERCISES

1. For each set below with elements listed explicitly, write the set in terms of a rule that states which elements from the universal set $\mathbb{N}$ are in the given set.

(a) $\{1, 2, 3, 4\} =$ _____

(b) $\{5, 6, 7, 8, ...\} =$ _____

2. For each set below given by a defining rule, give the same set by listing the elements explicitly.

   (a) $\{y \in \mathbb{N} \mid 3 < y\} =$ _____

   (b) $\{x \in \mathbb{N} \mid x < 1\} =$ _____

   (c) $\{x \in \mathbb{N} \mid x < 3\} =$ _____

3. Define $A = \{z \in \mathbb{N} \mid z \neq 1\}$. ($z \neq 1$ is an abbreviation of $\neg(z = 1)$, of course.)

   (a) 4. $b \in A$

   5. _____ (4; def. A)

   (b) 4. _____

   5. $c \in A$ (4; def. A).

4. Suppose we are given the following:

   5. $x \in B$

   6. $x < 7$ (5; def. B)

   7. $7 < 8$ (given)

   8. $x < 8$ (6, 7; Trans. $<$)

   9. $x \in C$ (8; def. C)

   What must the definitions of sets B and C be?

5. Suppose we are given the following:

   5. $1 < a$

   6. $a \in X$ (5; def. X)

   7. $b \in X$

   8. _____ (7; def. X)

   What must the definition of X be? What must Step 8 be?

6. Let $B = \{a \in \mathbb{N} \mid a < 7\}$ and $C = \{a \in \mathbb{N} \mid a < 2\}$. Provide justification for each of the indicated steps below.

   1. $q \in C$

   2. $q < 2$ _____

   3. $2 < 7$ _____

   4. $q < 7$ _____

   5. $q \in B$ _____

REVIEW EXERCISES

7. For each proposition below, identify the hypotheses and conclusion.

   (a) For all natural numbers a and b, if $a < 10$, then $b < 11$.

   (b) If $a < b$ for natural numbers a and b, then $a \neq b$.

   (c) For sets A and B, if $x \in A$, then $x \in B$.

Subsets; Proving *For All* Statements

Mathematical proof at its most basic level rests on the idea of formal definition. We now get to our first definition—the idea of *subset.* Informally, we say that a set A is a subset of a set B if every element of A is an element of B.

Example 1:

$\{1, 2, 3, 4\}$ is a subset of $\{1, 2, 3, 4, 5, 6, 7\}$.

Example 2:

If $A = \{1, 2, 3\}$ and $B = \{1, 2, 3\}$, then A is a subset of B, since every element of A is in B.

The definitions and theorems that we have about sets apply to any sets whatever—not only to sets of numbers. In order to illustrate the meaning of our definitions and theorems about sets, we will consider their application both to sets of numbers and to sets of points in a plane—represented by a sketch on a page. Thus we may take, as our universal set, either the natural numbers $\mathbb{N}$, or the set of points in a plane. Sketches of such point sets that illustrate some definition or theorem are called *Venn diagrams.* A Venn diagram that illustrates the definition of subset is shown in Figure 1. The set A is represented by all points inside its circle. The set B is represented by all points inside its circle. Since all points inside circle A are also inside circle B, we have that A is a subset of B.

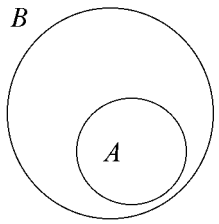


Figure 1. A is a subset of B

It is necessary that formal mathematics be intuitively meaningful. Venn diagrams help us visualize the content of a definition or theorem, and thereby aid in our intuitive understanding of it. It is also necessary that things that are intuitively meaningful be subject to formal articulation and proof. In mathematics, our imagination is not just allowed to run wild. It must be subject to unquestionable logic.

We now give a formal definition of *subset*. A formal definition involves three things. (1) A phrase identifying the symbols involved:

"For sets A and B,"

(2) a formal statement of the newly defined relationship:

"A is a *subset* of B"

and (3) a formal statement of the defining condition:

"$for\,all\,x \in A : x \in B$"

The newly defined relationship and its defining condition are *equivalent*, by which we mean that if the relationship is true, then we may infer that the defining condition holds, and if the defining condition holds, then we may infer that the relationship is true. In mathematics, equivalence is frequently denoted by the phrase "if and only if". Thus in the definition of "subset" we have:

"A is a *subset* of B if and only if $for\,all\,x \in A : x \in B$"

The phrase "if and only if" is often abbreviated "iff". Our formal definition is as follows:

Definition For sets A and B, A is a *subset* of B (written $A \subseteq B$) iff $for\,all\,x \in A : x \in B$.

The definition of subset is given in terms of a formal statement called a $for\,all$ statement. By definition, the relationship $A \subseteq B$ is equivalent to its defining condition: $for\,all\,x \in A : x \in B$. The following inference rule allows us to replace a step $A \subseteq B$ in a proof with the formal statement $for\,all\,x \in A : x \in B$.

Inference Rule Using equivalence: Any mathematical statement may be replaced by an equivalent statement.

Example 3:

1. $C \subseteq D$
2. _____ (1; def. $\subseteq$)

Solution:

1. $C \subseteq D$
2. $for\,all\,x \in C : x \in D$ (1; def. $\subseteq$)

In this example we know that Step 2 must come from Step 1 as a result of using the definition of $\subseteq$. By the rule for using equivalence, Step 2 must give the equivalent defining property.

The variable x in the statement $for\,all\,x \in A : x \in B$ is called a *local* variable (as opposed to a *global* variable). The local variable x doesn't mean anything outside the $for\,all$ statement, and any other letter inside the statement would do as well. Thus, for example, the following two statements mean exactly the same thing:

$$for\,all\,x \in A : \mathcal{P}(x)$$
$$for\,all\,t \in A : \mathcal{P}(t)$$

The statement $for\,all\,x \in A : x \in B$ is a statement about A and B. It means that everything in A is in B. It is not a statement about x. We don't get any information about x from the statement, but we do get information about A and B. It is permissible to use any letter at all (except letters already in use that have their meaning already defined) to play the role of the x in the $for\,all$ statement.

Example 4:

1. _____
2. $for\,all\,y \in S : y \in T$ (1; def. $\subseteq$)

Solution:

1. $S \subseteq T$
2. $for\,all\ y \in S : y \in T$ (1; def. $\subseteq$)

Example 5:

1. _____
2. $X \subseteq Y$ (1; def. $\subseteq$)

Solution:

1. $for\,all\ t \in X$: $t \in Y$
2. $X \subseteq Y$ (1; def. $\subseteq$)

Example 6:

1. $for\,all\ x \in A : x \in B$
2. $A \subseteq B$ (1; _____)

Solution:

1. $for\,all\ x \in A : x \in B$
2. $A \subseteq B$ (1; def. $\subseteq$)

Replacing a statement of the form $set \subseteq set$ in a proof with its $for\,all$ defining condition isn't going to do us any good unless we have means to handle the $for\,all$ statement.

The rule for proving a $for\ all$ statement is somewhat subtle. In order to prove the statement $for\ all\ x \in A : x < 7$, for example, we select an element of A, give it a name, and show that it must be less than 7 by virtue only of its being in A. That is, the fact that it is less than 7 follows from the single fact that it is in A. It follows that every element in A must be less than 7. The chosen element of A, about which we assume nothing except that it is in A, is called an *arbitrary* element of A.

Example 7:

Suppose $A = \{n \in \mathbb{N} \mid n < 12\}$. Steps 1 through 4 below prove the $for\,all$ statement of Step 5.

1. Let $t \in A$ be arbitrary
2. $t < 12$ (1; def. A)
3. $12 < 45$ (given)
4. $t < 45$ (2, 3; Trans. $<$)

5. $for\ all\ x \in A : x < 45$ (1—4; pr. $\forall$)

In Example 7, Steps 1 through 4 are indented. Their only purpose is to prove Step 5. The reason for indenting steps in proofs is to keep track of assumptions. Steps 1 through 4 are based on the assumption that A is not empty (we'll consider the other possibility in a moment), and that t is chosen arbitrarily in A. The variable t is defined only for Steps 1 through 4—its *scope* being Steps 1 through 4. The variable t can be considered as ceasing to exist after we pass from the block of Steps 1 through 4. It is no longer in use. It is legitimate, therefore, to use t as the local variable in Step 5—instead of x:

1. Let $t \in A$ be arbitrary
2. $t < 12$ (1; def. A)
3. $12 < 45$ (given)
4. $t < 45$ (2, 3; Trans. $<$)

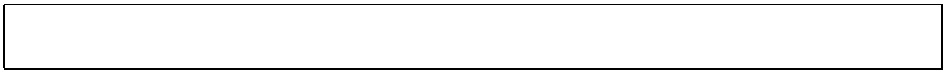
5. $for\ all\ t \in A : t < 45$ (1—4; pr. $\forall$)

Inference Rule Proving $for\ all$ statements: In order to prove a statement $for\ all\ x \in A : \mathcal{P}(x)$, let x be an arbitrarily chosen element of A, then show $\mathcal{P}(x)$ for that x. Abbreviation: "pr. $\forall$ ".

Format:

pr. $\forall$

1. Let $x \in A$ be arbitrary



k-1.$\mathcal{P}(x)$

k. $for\ all\ x \in A : \mathcal{P}(x)$ (1—k-1; pr. $\forall$)

Steps 1 and k-1 in the format above are dictated by the rule for proving $for\ all$ statements. The empty box represents additional steps that will be needed in order to show Step k-1.

Example 8:

Fill in the steps dictated by the rule for proving a $for\ all$ statement.

k. $for\ all\ x \in C : x < 12$ (_____; pr. $\forall$)

Solution:

1. Let $x \in C$ be arbitrary.

.

.

k-1. $x < 12$

k. $for\ all\ x \in C : x < 12$ (1— k-1; pr. $\forall$)

Example 9:

1. Let $t \in S$ be arbitrary.

.

7. $13 < t$

8. _____ (1—7; pr. $\forall$)

Solution:

1. Let $t \in S$ be arbitrary.

.

7. $13 < t$

8. $for\ all\ t \in S : 13 < t$ (1—7; pr. $\forall$)

We now get to the question of why it is sufficient to assume that A is not empty, in our rule for proving $for\ all$ statements. This can be explained in terms of the negations of $for\ all$ and $there\,exists$ statements.

Axiom $For\,all$ negation: $\neg(for\ all\ x \in A : \mathcal{P}(x))$ is equivalent to $there\,exists\ x \in A\ such\,that\ \neg\mathcal{P}(x)$.

Axiom $There\,exists$ negation: $\neg(there\,exists\ x \in A\ such\,that\ \mathcal{P}(x))$ is equivalent to $for\ all\ x \in A$: $\neg\mathcal{P}(x)$.

We don't get to using formal $there\,exists$ statements in proof steps until later. Informally, the statement $there\,exists\ x \in A\ such\,that\ \mathcal{P}(x)$ means exactly what it says. In order for this statement to be true there must be some element in A (that we can call x) for which $\mathcal{P}(x)$ is true.

Example 10:

Let $A = \{x \in \mathbb{N} \mid 8 < x\}$. Use the informal meanings of $for\ all$ and $there\,exists$ statements to determine whether each of the following statements is true or false. Label each statement accordingly.

$for\ all\ x \in A : x < 10$:_____

$there\,exists\ x \in A\ such\,that\ x < 10$:_____

$for\ all\ x \in A : x < 6$:_____

$there\,exists\ x \in A\ such\,that\ x < 6$:_____

$for\ all\ x \in A : 10 < x$:_____

$there\,exists\ x \in A\ such\,that\ 10 < x$:_____

$for\ all\ x \in A : 3 < x$:_____

$there\,exists\ x \in A\ such\,that\ 3 < x$:_____

Solution:

$for\ all\ x \in A : x < 10$: F

$there\,exists\ x \in A\ such\,that\ x < 10$: T

$for\ all\ x \in A : x < 6$: F

$there\,exists\ x \in A\ such\,that\ x < 6$: F

$for\ all\ x \in A : 10 < x$: F

$there\,exists\ x \in A\ such\,that\ 10 < x$: T

$for\ all\ x \in A : 3 < x$: T

$there\,exists\ x \in A\ such\,that\ 3 < x$: T

The only way for $for\ all\ x \in A : \mathcal{P}(x)$ to be false is for there to exist an element x in A for which $\mathcal{P}(x)$ is false. If A is empty, there can be no such element—so $for\ all\ x \in A : \mathcal{P}(x)$ must be true if A is empty. We say in this case that the statement is *vacuously* true. A complete, informal proof of the statement $for\ all\ x \in A : \mathcal{P}(x)$ would go as follows: if A is empty, then the statement is vacuously true, if A is not empty, then pick an arbitrary element from A and show that $\mathcal{P}$ is true for this element.

People don't focus on vacuously true statements and empty sets when doing proofs. They just assume that there is some element in A, because if there is not, then they are immediately

done. In this way our inference rule (which assumes that there is an element in A, and indents the block of steps based on this assumption) models customary informal practice.

EXERCISES

1. Let $A = \{x \in \mathbb{N} \mid x < 9\}$. Use the informal meanings of $for\ all$ and $there\ exists$ statements to determine whether each of the following statements is true (T) or false (F). Label each statement accordingly.

   (a) $for\ all\ x \in A : x < 10$:_____

   (b) $there\ exists\ x \in A\ such\ that\ x < 10$:_____

   (c) $for\ all\ x \in A : x < 6$:_____

   (d) $there\ exists\ x \in A\ such\ that\ x < 6$:_____

   (e) $for\ all\ x \in A : 10 < x$:_____

   (f) $there\ exists\ x \in A\ such\ that\ 10 < x$:_____

   (g) $for\ all\ x \in A : 3 < x$:_____

   (h) $there\ exists\ x \in A\ such\ that\ 3 < x$:_____

2. Fill in the underlined places.

   1. Let $x \in S$ be arbitrary.

   .

   7. $x < 7$

   8. _____ (_____; pr. $\forall$)

3. Fill in the steps dictated by the rule for proving a $for\ all$ statement

   (a)

   8. $for\ all\ x \in A : 5 < x$ (_____; pr. $\forall$)

   (b)

   6. $for\ all\ x \in A : x \in B$ (_____; pr. $\forall$)

REVIEW EXERCISES

4. For each set below with elements listed explicitly, write the set in terms of a rule that states which elements from the universal set $\mathbb{N}$ are in the given set.

   (a) $\{1, 2, 3\}$ = _____

   (b) $\{6, 7, 8, ...\}$ = _____

5. For each set below given by a defining rule, give the same set by listing the elements explicitly.

   (a) $\{y \in \mathbb{N} \mid y < 9\}$ = _____

   (b) $\{t \in \mathbb{N} \mid 3 < t\}$ = _____

6. Define $A = \{z \in \mathbb{N} \mid 7 < z\}$.

   (a) 4. $b \in A$

   5. _____(4; def. A)

   (b) 4. _____

   5. $c \in A$ (4; def. A).

7. Suppose we are given the following:

   5. $a \in B$
   6. $4 < a$ (5; def.B)
   7. $2 < 4$ (given)
   8. $2 < a$ (6, 7; Trans.<)
   9. $a \in C$ (8; def.C)

   What must the definitions of sets B and C be?

8. Let $B = \{x \in \mathbb{N} \mid x < 5\}$ and $C = \{x \in \mathbb{N} \mid x < 4\}$. Fill in the underlined steps or justifications below.

   1. $q \in C$
   2. _____ (1; def.C)
   3. $4 < 5$ _____
   4. $q < 5$ _____
   5. $q \in B$ _____

Discovering Proof Steps

Mathematics is a thing of the imagination. It is about an imaginative universe, a world of ideas. But the imagination is constrained by logic. This constraint allows mathematics its scope. It is thereby free to remove itself from the objects of immediate sense experience without becoming nonsense.

In mathematics, a thing is exactly what its definition says it is. A proof that something has a property is a demonstration that the property follows logically from the definition. In rigorous mathematics, a proof is not allowed to use attributes of our imaginative ideas that don't follow from the precise wording of the definition. Thus proof at its most basic level is proof that depends immediately on definitions. Our method of proof analysis discovers steps that follow from definitions.

The first step in the proof of some proposition is to determine the hypotheses and conclusion. The next step depends on the form of the top-level, formal statement of the conclusion. This top-level statement may contain pieces that are themselves formal statements, but is itself not contained in any larger statement.

Example 1:

The top-level statement in

(a) $for\,all\ x \in A : x \in B$

is a $for\,all$ statement. It contains the formal statements $x \in A$ and $x \in B$, but is itself not contained in a larger statement.

The top-level statement in

(b) $\{x \in \mathbb{N} \mid x < 10\} \subseteq \{x \in \mathbb{N} \mid x < 20\}$

is an assertion of set containment of the form $set \subseteq set$. It contains the formal statements $x < 10$, $x < 20$, and $x \in \mathbb{N}$.

The top-level form of a statement can be confirmed by the process of “diagramming the sentence”. In mathematics such diagramming can be done by inserting parentheses into the statement. Such parentheses will always surround lower-level statements and terms, but never the top-level relation. For example, in the statement $for\,all\ x \in A : x \in B$, parentheses can be put around the statements $x \in A$ and $x \in B$ to get: $for\,all\ (x \in A) : (x \in B)$. This confirms that the statement is a $for\,all$ statement, since the phrase $for\,all$ is not contained in parentheses. It would be obviously nonsensical to attempt to include the $for\,all$ phrase and exclude the set membership symbol “ $\in$ ” by a diagram such as: $(for\,all\ x \in A : x) \in (B)$. Thus the statement is not a statement about set membership at the top level.

Example 2:

Define $H = \{x \in \mathbb{N} \mid x < 10\}$ and $G = \{x \in \mathbb{N} \mid x < 20\}$. Prove that $H \subseteq G$.

To start the proof, we identify the hypotheses and conclusion.

Proof:

Assume: $H = \{x \in \mathbb{N} \mid x < 10\}$
$G = \{x \in \mathbb{N} \mid x < 20\}$

Show: $H \subseteq G$

The next step is to write the conclusion as the last step in the proof:

Proof:

Assume: $H = \{x \in \mathbb{N} \mid x < 10\}$
$G = \{x \in \mathbb{N} \mid x < 20\}$

Show: $H \subseteq G$

k. $H \subseteq G$.

Writing the conclusion as the last step in the proof creates a gap—which needs to be bridged by the steps leading to the conclusion. The next step in the process is to write down the justification for Step k. Since Step k is of the top-level form $set \subseteq set$, the justification for Step k must be the definition of $\subseteq$.

Proof:

Assume: $H = \{x \in \mathbb{N} \mid x < 10\}$
$G = \{x \in \mathbb{N} \mid x < 20\}$

Show: $H \subseteq G$

k. $H \subseteq G$ (; def. $\subseteq$)

The definition of *subset* makes the relation $H \subseteq G$ equivalent to its defining condition $for\ all\ x \in H : x \in G$. Since $H \subseteq G$ is to be shown in the last step, the defining condition $for\ all\ x \in H : x \in G$ must be the next-to-the-last step:

k-1. $for\ all\ x \in H : x \in G$
k. $H \subseteq G$ (k-1; def. $\subseteq$)

We next write down the justification for Step k-1. This will be determined by the top-level form of Step k-1. It is a $for\ all$ statement, so the rule for proving $for\ all$ statements must be the justification for Step k-1. The $for\ all$ rule tells us we need Steps 1 and k-2 below. Step 1 is put at the top of the gap, and Step k-2 is put at the bottom—making a new, smaller gap now between Steps 1 and k-2.

1. Let $x \in H$ be arbitrary.
.
k-2. $x \in G$
k-1. $for\,all\ x \in H : x \in G$ (1—k-2; pr. $\forall$)
k. $H \subseteq G$ (k-1; def. $\subseteq$)

The steps above are dictated by our analysis as we work backward from the conclusion. We now have to bridge the gap from Step 1 to Step k-2. What we mean by saying that x is chosen arbitrarily in H is that the only thing we know about x is the property it must have by virtue of being in H. Thus Step 2 must follow from Step 1 by using the definition of H. Similarly, to show $x \in G$ in Step k-2 we must use the definition of G.

1. Let $x \in H$ be arbitrary.
2. $x < 10$ (1; def. H)
.
k-3. $x < 20$
k-2. $x \in G$ (k-3; def. G)
k-1. $for\,all\ x \in H : x \in G$ (1—k-2; pr. $\forall$)
k. $H \subseteq G$ (k-1; def. $\subseteq$)

The steps above were dictated by our analytical method of discovering proof steps. You should also see why, logically, we had to get the steps above. There remains only to make the connection between Steps 2 and k-3, and this connection is clear: $x < 20$ follows from $x < 10$ (by the transitive property of $<$), if we supply Step 3, $10 < 20$, (which is justified by "given"). This gives a complete proof that $H \subseteq G$:

Proof:

Assume: $H = \{x \in \mathbb{N} \mid x < 10\}$
$G = \{x \in \mathbb{N} \mid x < 20\}$
Show: $H \subseteq G$

1. Let $x \in H$ be arbitrary.
2. $x < 10$ (1; def. H)
3. $10 < 20$ (given)
4. $x < 20$ (2, 3; Trans. $<$)
5. $x \in G$ (4; def. G)
6. $for\,all\ x \in H : x \in G$ (1—5; pr. $\forall$)
7. $H \subseteq G$ (6; def. $\subseteq$)

□

The equivalence of the relation "subset" and its $for\,all$ defining condition means that the rule for proving a $for\,all$ statement is used to prove that one set is a subset of another. The negation of the $for\,all$ statement is used to find counterexamples to assertions that one set is a subset of another.

By definition, the statement $A \subseteq B$ is equivalent to $for\,all\ x \in A : x \in B$. By the axiom on the negation of a $for\,all$ statement from the previous section, $\neg(A \subseteq B)$ is equivalent to $there\ exists\ x \in A\ such\,that\ x \notin B$. To find a counterexample to $A \subseteq B$, we informally show this $there\,exists$ statement; that is, we define some element in A, and show it is not in B. We will always take an informal approach to finding counterexamples. The reason for our formal approach to proofs is that it is the formal rules of inference that guide us in the step-discovery procedure.

Example 3:

Let $S = \{x \in \mathbb{N} \mid x < 12\}$ and $T = \{x \in \mathbb{N} \mid x < 10\}$. Find a counterexample that shows $S \subseteq T$ is false.

Solution:

$11 \in S$, but $11 \notin T$. Therefore $\neg(S \subseteq T)$.

In the paragraph preceding Example 3, we have used the fact that the statement $A \subseteq B$ and its defining condition are logically equivalent. We have also implicitly used the following axioms:

Axiom If $\mathcal{P}$ is equivalent to $\mathcal{Q}$, then $\neg\mathcal{P}$ is equivalent to $\neg\mathcal{Q}$.

Axiom The statements $\mathcal{P}$ and $\neg(\neg\mathcal{P})$ are logically equivalent.

These axioms will almost always be used implicitly.

Step-Discovery Outline

There are two different aspects to discovering proof steps: (1) In the *synthetic* aspect, you need to imagine how known information (steps already proven, for example) can be put together or used to obtain a desired result. (2) In the *analytic* aspect, you look at the desired result, and, from the intrinsic nature of this result, decide what steps are necessary to achieve it. It's best to write down all the steps that *analysis* dictates to be inevitable, before you work on the *synthesis*.

Analysis

1. Determine the hypotheses and conclusion.
2. Write the conclusion as the last line of the proof.

   The conclusion will be a formal statement. Thus far, the types we have are:

   basic logic statement forms

   $for\,all$

   undefined relations

   $element \in set$

   $number < number$

   $number = number$

   defined relations

   $set \subseteq set$
3. Write the justification for the conclusion.

   Don't copy proof steps from examples. Instead, analyze the conclusion yourself to see what is needed. Consider all the ways you might prove a statement having the form of the conclusion. Focus on what it means for the conclusion to be true. If the conclusion is a basic logic form, the rule for proving such a statement will always be available as the justification, and will dictate prior steps. If the conclusion is of the form $element \in set$, the only way of proving this (so far) is to show that the element satisfies the defining property for the set. Thus the justification will be the

definition of the set, and the defining condition will be the previous step. If the conclusion involves a defined relation at the top level, you can always use the definition of that relation as justification, in which case the preceding step must be the condition defining the relation. Thus the *form* of the conclusion indicates the justification, which, in turn, dictates the needed steps preceding the conclusion. Write these dictated steps down before going to 4 below.

4. Now, working from the bottom up, analyze the step immediately preceding the conclusion. From the form of this statement you will be able to write down the rule for its justification. This rule will dictate prior steps. Continue in this manner until you can go no further.

Synthesis

5. When you can no longer continue by analyzing steps from the bottom up, add new steps from the top down by again analyzing the form of the steps already known. If your bottom-up analysis leads to a step that can be proved in more than one way, and if you're not sure about the best way, work from the top down for a while. This might show the best approach to prove the needed step at the bottom.

6. You need to use information from the steps already proven, in order to add new steps. It is generally best to use first the information from the bottom-most of the known steps at the top. Then use the information from the steps toward the top. Finally, use the hypotheses to bridge the remaining gaps. Don't use the hypotheses until after you have exhausted the information from all the steps themselves.

At the end of this section is a copy of the step-discovery outline that you can tear out and use, as needed, when doing proofs for homework.

EXERCISES

1. Find a proof or a counterexample for each of the following statements:

   (a) Let $A = \{a \in \mathbb{N} \mid a < 10\}$ and $B = \{b \in \mathbb{N} \mid 5 < b\}$. Then $A \subseteq B$.

   (b) Let $A = \{a \in \mathbb{N} \mid 10 < a\}$ and $B = \{b \in \mathbb{N} \mid 5 < b\}$. Then $A \subseteq B$.

   (c) Let $A = \{a \in \mathbb{N} \mid 10 < a\}$ and $B = \{b \in \mathbb{N} \mid 5 < b\}$. Then $B \subseteq A$.

2. (a) Let S and T be arbitrary sets. Start to develop a proof that $S \subseteq T$ by the step-discovery procedure. Write down as many steps as you can with only the information available. (You don't know anything about the sets S and T.) Don't make up new information.

   (b) Give a counterexample to show that $S \subseteq T$ is not true for all sets S and T.

3. (a) Make a list of all definitions. Write each definition for future reference. This “definition sheet” can be used when you are following the step-discovery outline on homework.

   (b) The appendix lists the formats for the basic logic rules. Give an example of the use of each rule encountered so far. Use the appendix and your examples as a template when you follow the step discovery procedure on homework problems.

REVIEW EXERCISES

4. For each set below with elements listed explicitly, write the set in terms of a rule that states which elements from the universal set $\mathbb{N}$ are in the given set.

   (a) $\{5, 6, 7, 8, 9, \ldots\} =$ _____

   (b) $\{1, 2, 3, 4, 5, 6\} =$ _____

5. For each set below given by a defining rule, give the same set by listing the elements explicitly.

   (a) $\{t \in \mathbb{N} \mid t < 1\} =$ _____

   (b) $\{t \in \mathbb{N} \mid t < 4\} =$ _____

6. Define $X = \{t \in \mathbb{N} \mid 9 < t\}$.

   (a) 4. $b \in X$
   5. _____ (4; def. X)

   (b) 4. _____
   5. $b \in X$ (4; def. X)

7. Suppose we are given the following:

   5. $1 < a$
   6. $a \in X$ (5; def. X)
   7. $b \in X$
   8. _____ (7; def. X)

   What must the definition of X be? $X =$ _____ What must Step 8 be?

8. Fill in the underlined places in the following proof fragments.

   (g) 1. Let $x \in C$ be arbitrary.
   .
   7. $8 < x$
   8. _____ (_____; pr. $\forall$)

9. Fill in the steps dictated by the rule for proving a $for\ all$ statement.

   (a)

   8. $for\ all\ z \in X$: $z < 6$ (_____; pr. $\forall$)

   (b)

   6. $for\ all\ z \in X$: $z \in Y$ (_____; pr. $\forall$)

Step-Discovery Outline

There are two different aspects to discovering proof steps: (1) In the *synthetic* aspect, you need to imagine how known information (steps already proven, for example) can be put together or used to obtain a desired result. (2) In the *analytic* aspect, you look at the desired result, and, from the intrinsic nature of this result, decide what steps are necessary to achieve it. It's best to write down all the steps that *analysis* dictates to be inevitable, before you work on the *synthesis*.

Analysis

1. Determine the hypotheses and conclusion.
2. Write the conclusion as the last line of the proof.

   The conclusion will be a formal statement. Thus far, the types we have are:

   basic logic statement forms

   $$for\,all$$

   undefined relations

   $$element \in set$$
   $$number < number$$
   $$number = number$$

   defined relations

   $$set \subseteq set$$

3. Write the justification for the conclusion.

   Don't copy proof steps from examples. Instead, analyze the conclusion yourself to see what is needed. Consider all the ways you might prove a statement having the form of the conclusion. Focus on what it means for the conclusion to be true. If the conclusion is a basic logic form, the rule for proving such a statement will always be available as the justification, and will dictate prior steps. If the conclusion is of the form $element \in set$, the only way of proving this (so far) is to show that the element satisfies the defining property for the set. Thus the justification will be the definition of the set, and the defining condition will be the previous step. If the conclusion involves a defined relation at the top level, you can always use the definition of that relation as justification, in which case the preceding step must be the condition defining the relation. Thus the *form* of the conclusion indicates the justification, which, in turn, dictates the needed steps preceding the conclusion. Write these dictated steps down before going to 4 below.

4. Now, working from the bottom up, analyze the step immediately preceding the conclusion. From the form of this statement you will be able to write down the rule for its justification. This rule will dictate prior steps. Continue in this manner until you can go no further.

Synthesis

5. When you can no longer continue by analyzing steps from the bottom up, add new steps from the top down by again analyzing the form of the steps already known. If your bottom-up analysis leads to a step that can be proved in more than one way, and if you're not sure about the best way, work from the top down for a while. This might show the best approach to prove the needed step at the bottom.
6. You need to use information from the steps already proven, in order to add new steps. It is generally best to use first the information from the bottom-most of the known steps at the top. Then use the information from the steps toward the top. Finally, use the hypotheses to bridge the remaining gaps. Don't use the hypotheses until after you have exhausted the information from all the steps themselves.

Using $For\ All$ Statements

Examples 1 and 2 illustrate how to *use* a $for\,all$ statement that we know is true.

Example 1:

In the following steps, the known $for\ all$ statement in Step 2 is applied to the known information in Step 1 to infer Step 3.

1. $y \in A$
2. $for\ all\ x \in A : x < 7$
3. $y < 7$

The meaning of Step 2 is that every element in set A is less than 7. Since y is an element of A by Step 1, we can conclude that y must be less than 7.

Example 2:

In the following steps, the $for\ all$ statement in Step 1 is applied to the y in Step 2 (presumably already defined) to infer Step 3.

1. $for\ all\ x \in B : x < 10$
2. $y \in B$
3. _____

Solution:

1. $for\ all\ x \in B : x < 10$
2. $y \in B$
3. $y < 10$

Here is the general inference rule for using a $for\,all$ statement.

Inference Rule Using $for\ all$ statements: If $for\ all\ x \in A : \mathcal{P}(x)$ and $y \in A$ are steps in a proof, then $\mathcal{P}(y)$ can be inferred. Abbreviation: "us. $\forall$".

The format for using this rule is:

us. $\forall$

1. $for\,all\,x \in A : \mathcal{P}(x)$
2. $t \in A$
3. $\mathcal{P}(t)$ (1, 2; us. $\forall$)

Example 3:

1. $q \in B$
2. $for\ all\ x \in B : x < 12$
3. _____ (1, 2; us. $\forall$)

Solution:

1. $q \in B$
2. $for\ all\ x \in B : x < 12$
3. $q < 12$ (1, 2; us. $\forall$)

Since x is a local variable in $for\ all\ x \in \mathbb{N} : x < 12$, any other letter (except letters already in use for other things—such as q) would do as well. Thus the following two statements mean exactly the same thing.

$$for\ all\ x \in B : x < 12$$
$$for\ all\ t \in B : t < 12$$

Example 4:

1. $q \in B$
2. $for\ all\ t \in B : t < 12$
3. _____ (1, 2; us. $\forall$)

Solution:

1. $q \in B$
2. $for\ all\ t \in B : t < 12$
3. $q < 12$ (1, 2; us. $\forall$)

Example 5:

1. _____
2. $for\ all\ x \in A : 9 < x$
3. _____ (1, 2; us. $\forall$)

Solution:

1. $q \in A$
2. $for\ all\ x \in A : 9 < x$
3. $9 < q$ (1, 2; us. $\forall$)

Example 6:

1. $3 \in A$
2. $for\ all\ x \in A : x \in B$
3. _____ (1, 2; us. $\forall$)

Solution:

1. $3 \in A$
2. $for\ all\ x \in A : x \in B$
3. $3 \in B$ (1, 2; us. $\forall$)

Example 7:

1. $4 \in A$
2. _____
3. $4 \in B$ (1, 2; us. $\forall$)

Solution:

1. $4 \in A$
2. $for\ all\ x \in A : x \in B$
3. $4 \in B$ (1, 2; us. $\forall$)

Example 8:

1. $x \in A$
2. _____
3. $x \in B$ (1, 2; us. $\forall$)

Solution:

1. $x \in A$
2. $for\ all\ t \in A : t \in B$
3. $x \in B$ (1, 2; us. $\forall$)

The statement $for\ all\ x \in A : x \in B$, using the symbol "$x$", cannot be used as a solution in Example 8. The reason is that x must have been defined already, since it is used in Step 1. The statement $for\ all\ t \in A : t \in B$ means that t ranges over all the values in A, and for each of these it is also the case that $t \in B$. If x has already been defined, it represents a single thing, and can't range over the values of A.

The aim of the text material, from here to Section 16, is to develop your ability to find your own proof to any theorem you might discover in your investigation. Your ability to do this will depend on your mastery of the step-discovery procedure. It is necessary to abandon any reliance you might have on doing proofs by copying steps from other proofs that may be similar to the proof you need. As a significant step in this direction, you are to prove Theorem 5.1 at the end of this section.

In the previous section we defined the sets $H = \{x \in \mathbb{N} \mid x < 10\}$ and $G = \{x \in \mathbb{N} \mid x < 20\}$, and proved that $H \subseteq G$. The purpose in doing the proof was to illustrate the use of the method summarized at the end of that section, and to lead into your proof of Theorem 5.1. In the next example, we again illustrate the same method of discovering proof steps—one more stepping stone before Theorem 5.1. Review the proof of the next example, with a copy of the step-discovery outline from the previous section to look at as you do it. Try to anticipate each step and justification by following the outline. Use the proof in the text as confirmation.

Example 9:

Prove that if $K = \{x \in \mathbb{N} \mid x < 20\}$, and if $J \subseteq K$, then $for\ all\ a \in J$: $a < 20$.

Proof:

Assume: $K = \{x \in \mathbb{N} \mid x < 20\}$
$J \subseteq K$

Show: $for\ all\ a \in J\colon a < 20$

After deciding on hypotheses and conclusion, the next thing to do is to write the conclusion as the last step in the proof:

Proof:

Assume: $K = \{x \in \mathbb{N} \mid x < 20\}$
$J \subseteq K$

Show: $for\ all\ a \in J\colon a < 20$

k. $for\ all\ a \in J\colon a < 20$

The next thing to write down is the justification for Step k. This is determined by the top-level form of the statement of Step k—a $for\ all$ statement. Do we know that Step k is true, or are we trying to prove it? The rule for *using* a $for\ all$ statement only applies to $for\ all$ statements that have been already established. We're trying to *prove* Step k.

Proof:

Assume: $K = \{x \in \mathbb{N} \mid x < 20\}$
$J \subseteq K$

Show: $for\ all\ a \in J\colon a < 20$

k. $for\ all\ a \in J\colon a < 20$ (; pr. $\forall$)

In turn, the rule for proving $for\ all$ statements dictates Steps 1 and k-1:

Proof:

Assume: $K = \{x \in \mathbb{N} \mid x < 20\}$
$J \subseteq K$

Show: $for\ all\ a \in J\colon a < 20$

1. Let $a \in J$ be arbitrary.
.
.
k-1. $a < 20$
k. $for\ all\ a \in J\colon a < 20$ (1—k-1; pr. $\forall$)

The outline asks us next for justification for Step k-1. This normally would be the definition of $<$. Since the relation $<$ has not been defined, we stop adding steps from the bottom up and work from the top down. Step 1 is of the form $element \in set$. Since the set J has not been defined, we can't use the definition of J to get Step 2. There are no more steps that are indicated by the top-down, bottom-up analysis, so it is time to use the hypotheses. Which one: the definition of K, or the fact $J \subseteq K$? Since $a \in J$ from Step 1, we use $J \subseteq K$. What may be inferred from $J \subseteq K$? The statement is of the form $set \subseteq set$, so we use the definition of $\subseteq$ to write Step 2:

	1. Let $a \in J$ be arbitrary.	
	2. $for\ all\ x \in J$: $x \in K$	(hyp.; def. $\subseteq$)
	.	
	.	
	k-1. $a < 20$	
k.	$for\ all\ a \in J$: $a < 20$	(1— k-1; pr. $\forall$)

It is not legitimate to write $for\ all\ a \in J$**:** $a \in K$ as Step 2. We can't use a as a local variable in Step 2, since it is already in use from Step 1. Although a was chosen arbitrarily in Step 1, it has been chosen, and is now fixed. It is constant. It doesn't make any more sense to talk about all a's in Step 2, than it does to talk about all 3's. In Step 2, where we have x, you could have any other letter not already in use.

It is now possible to use the $for\ all$ statement of Step 2.

	1. Let $a \in J$ be arbitrary.	
	2. $for\ all\ x \in J$: $x \in K$	(hyp.; def. $\subseteq$)
	3. $a \in K$	(1, 2; us. $\forall$)
	.	
	.	
	k-1. $a < 20$	
k.	$for\ all\ a \in J$: $a < 20$	(1— k-1; pr. $\forall$)

Since we gave up working up from Step k at Step k-1, we're now working down. Step 3 is of the form $element \in set$. The definition of that set is the justification for Step 4:

	1. Let $a \in J$ be arbitrary.	
	2. $for\ all\ x \in J$: $x \in K$	(hyp.; def. $\subseteq$)
	3. $a \in K$	(1, 2; us. $\forall$)
	4. $a < 20$	(3; def. K)
	k-1. $a < 20$	
k.	$for\ all\ a \in J$: $a < 20$	(1— k-1; pr. $\forall$)

We see that Step 4 is Step k-1, so that we didn't have to work up from Step k-1 after all. It remains only to fill in the steps upon which Step k depends:

Proof:

Assume: $K = \{x \in \mathbb{N} \mid x < 20\}$
$J \subseteq K$

Show: $for\ all\ a \in J\colon a < 20$

1. Let $a \in J$ be arbitrary.
2. $for\ all\ x \in J\colon x \in K$ (hyp.; def. $\subseteq$)
3. $a \in K$ (1, 2; us. $\forall$)
4. $a < 20$ (3; def. K)
5. $for\ all\ a \in J\colon a < 20$ (1—4; pr. $\forall$)

□

Theorem 5.1 For sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

In order to prove this theorem, we first decide what we are given and what we need to show:

Proof:

Assume: A, B, C sets
1. $A \subseteq B$
2. $B \subseteq C$

Show: $A \subseteq C$

Before you continue the development of a formal proof as Exercise 1, let us illustrate the theorem with a Venn diagram. First we draw a circle for set C (Figure 5.1):

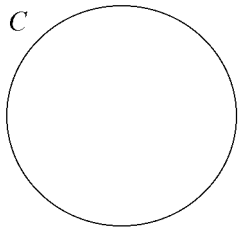


Figure 5.1

By the hypothesis $B \subseteq C$, we put the circle representing set B inside set C, as in Figure 5.2:

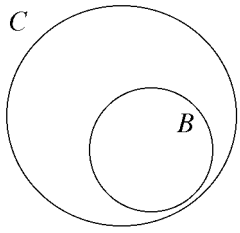


Figure 5.2

By hypothesis 2, $A \subseteq B$, we draw set A inside circle B, as in Figure 5.3. It is clear from the diagram, now, that A is inside C; that is, the conclusion $A \subseteq C$ is true.

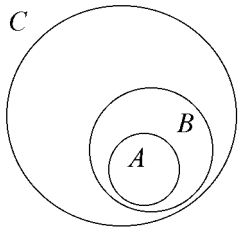


Figure 5.3

EXERCISES

1. Fill in the underlined places in the following proof fragments.

(a) 1. $y \in C$
2. $for\ all\ x \in C : x < 12$
3. _____ (_____;_____)

(b) 1. _____
2. $for\ all\ t \in B : t \in C$
3. _____ (1, 2; us. $\forall$)

(c) 1. $q \in B$
2. $for\ all\ t \in B : t \in C$
3. _____ (1, 2; us. $\forall$)

(d) 1. $5 \in S$
2. $for\ all\ x \in S : x \in T$
3. _____ (1, 2; us. $\forall$)

(e) 1. $4 \in S$
2. _____
3. $4 \in T$ (1, 2; us. $\forall$)

(f) 1. $x \in S$
2. _____
3. $x \in T$ (1, 2; us. $\forall$)

2. Prove Theorem 5.1. Stick exclusively to the step-discovery procedure.

REVIEW EXERCISES

3.

1. Let $x \in R$ be arbitrary.

.

7. $x < 8$

8. _____ (_____; pr. $\forall$)

4. Fill in the steps dictated by the rule for proving a $for\ all$ statement

(a)

8. $for\ all\ x \in A : 5 < x$ (_____; pr. $\forall$)

(b)

6. $for\ all\ x \in C : x \in D$ (_____; pr. $\forall$)

Using *Or* Statements

Definition For sets A and B, the *union* of A and B is the set $A \cup B$ defined by $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$.

The word "*or*" in mathematics is always taken in the inclusive sense, so that x is in $A \cup B$ if it is in A or in B or in both. From this informal meaning of the word "*or*" we can give examples of the union of a few sets:

Example 1:

(a) If $A = \{2, 3, 4\}$ and $B = \{3, 4, 5\}$, then $A \cup B = \{2, 3, 4, 5\}$.

(b) If $R = \{1, 2, 3\}$ and $S = \{2, 3\}$, then $R \cup S = \{1, 2, 3\}$.

(c) $\{2, 4, 6, 8, ...\} \cup \{1, 3, 5, 7, ...\} = \mathbb{N}$.

The shaded area in Figure 6.1 represents the set $A \cup B$:

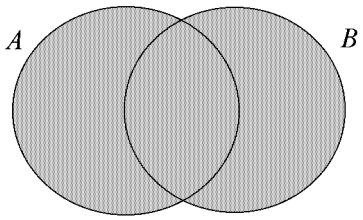


Figure 6.1

We are not allowed to use the informal idea of the word "*or*" in formal proofs, however. In order to use *or* statements in proofs, we need rules for proving and using statements of this form.

Inference Rule Using *or* statements (partial version): To use a statement $\mathcal{P}$ *or* $\mathcal{Q}$ that we know is true, in order to prove some statement $\mathcal{R}$, first assume that $\mathcal{P}$ is true and prove $\mathcal{R}$ in that case, then assume that $\mathcal{Q}$ is true and prove $\mathcal{R}$ in that case. Abbreviation: "us. *or*".

Format:

us. or

1. $\mathcal{P}$ *or* $\mathcal{Q}$

Case 1 2. $\mathcal{P}$

j. $\mathcal{R}$

Case 2 j+1. $\mathcal{Q}$

k-1. $\mathcal{R}$

k. $\mathcal{R}$ (1—k-1; us. *or*)

The reason for indenting is so we can keep track of the assumptions under which proof steps are true. Steps at the left-most level, such as the last step (conclusion) are true with only the hypotheses assumed. At the top of any indented block of steps we can see the additional assumption under which the steps are true.

Using a statement $\mathcal{P}$ *or* $\mathcal{Q}$ to prove $\mathcal{R}$ involves 2 cases, the first where we assume $\mathcal{P}$, and the second where we assume $\mathcal{Q}$. It is necessary that $\mathcal{R}$ be the last step in both cases. The steps needed to prove $\mathcal{R}$ in Case 1 are valid only in that case, and can't be used in Case 2, or anywhere else in the proof. Similarly, the steps in Case 2 can only be used in that case.

The empty boxes in the proof format above represent two remaining gaps that will each need to be bridged.

Example 2:

1. $x \in A$ *or* $x \in B$

Case 1 2. _____

.

5. _____

Case 2 6. _____

.

9. _____

10. $x < 8$ (1—9; us. *or*)

Solution:

1. $x \in A$ *or* $x \in B$

Case 1 2. $x \in A$

.

5. $x < 8$

Case 2 6. $x \in B$

.

9. $x < 8$

10. $x < 8$ (1—9; us. *or*)

Example 3:

Suppose that $A = \{t \in \mathbb{N} \mid t < 10\}$, $B = \{t \in \mathbb{N} \mid t < 20\}$, and $C = \{t \in \mathbb{N} \mid t < 30\}$. Prove that $A \cup B \subseteq C$.

Instead of merely reading the following proof asked for in Example 3, use the following procedure—which is suggested for reading all mathematics proofs: (1) cover the proof discussion below with a piece of paper, (2) follow the step-discovery outline by writing your own steps to anticipate the steps in the text, and (3) uncover the steps in the text to verify your work.

Proof:

Assume: $A = \{t \in \mathbb{N} \mid t < 10\}$
$B = \{t \in \mathbb{N} \mid t < 20\}$
$C = \{t \in \mathbb{N} \mid t < 30\}$

Show: $A \cup B \subseteq C$

k. $A \cup B \subseteq C$

The conclusion is of the form $set \subseteq set$. This top-level form regards $A \cup B$ as a single set. From the form of the conclusion, we get the justification for Step k.

Proof:

Assume: $A = \{t \in \mathbb{N} \mid t < 10\}$
$B = \{t \in \mathbb{N} \mid t < 20\}$
$C = \{t \in \mathbb{N} \mid t < 30\}$

Show: $A \cup B \subseteq C$

k. $A \cup B \subseteq C$ (; def. $\subseteq$)

By the definition of $\subseteq$, we get the following defining condition as Step k-1.

k-1. $for\,all\ x \in A \cup B : x \in C$
k. $A \cup B \subseteq C$ (k-1; def. $\subseteq$)

At the top level, statement k-1 is a $for\,all$ statement. Thus the rule for proving $for\,all$ statements is the justification for Step k-1. This rule dictates Steps 1 and k-2.

1. Let $x \in A \cup B$ be arbitrary.
.
k-2. $x \in C$
k-1. $for\,all\ x \in A \cup B : x \in C$ (1—k-2; pr. $\forall$)

k. $A \cup B \subseteq C$ (k-1; def. $\subseteq$)

At the top level, Statement k-2 is of the form $element \in set$. The justification for this step is therefore the definition of the set.

1. Let $x \in A \cup B$ be arbitrary.
.
k-2. $x \in C$ (; def. C)
k-1. $for\ all\ x \in A \cup B : x \in C$ (1—k-2; pr. $\forall$)
k. $A \cup B \subseteq C$ (k-1; def. $\subseteq$)

Getting $x \in C$ as Step k-2 from the definition of C, means that the condition defining C (applied to x) must be Step k-3.

1. Let $x \in A \cup B$ be arbitrary.
.
k-3. $x < 30$
k-2. $x \in C$ (k-3; def. C)
k-1. $for\ all\ x \in A \cup B : x \in C$ (1—k-2; pr. $\forall$)
k. $A \cup B \subseteq C$ (k-1; def. $\subseteq$)

Step k-3 is of the form $number < number$. Since the relation $<$ has not been defined, we are at the end of the bottom-up part of the analysis, and we now work from the top down. There is only one possibility for Step 2. Step 1 is of the form $element \in set$. The definition of that set gives us Step 2. Since x is in the set, x must satisfy the defining condition.

1. Let $x \in A \cup B$ be arbitrary.
2. $x \in A\ or\ x \in B$ (1; def. $\cup$)
.
k-3. $x < 30$
k-2. $x \in C$ (k-3; def. C)
k-1. $for\ all\ x \in A \cup B : x \in C$ (1—k-2; pr. $\forall$)
k. $A \cup B \subseteq C$ (k-1; def. $\subseteq$)

At the top level, Step 2 is an *or* statement. We are now in the position of wanting to use an *or* statement that we know is true (Step 2) to prove $x < 30$ (Step k-3). The rule for using *or* statements tells us just what to do.

	1. Let $x \in A \cup B$ be arbitrary.	
	2. $x \in A$ *or* $x \in B$	(1; def. $\cup$)
Case 1	3. $x \in A$	
	.	
	j-1. $x < 30$	
Case 2	j. $x \in B$	
	.	
	k-4. $x < 30$	
	k-3. $x < 30$	(2—k-4; us. *or*)
	k-2. $x \in C$	(k-3; def. C)
	k-1. $for\ all\ x \in A \cup B : x \in C$	(1—k-2; pr. $\forall$)
	k. $A \cup B \subseteq C$	(k-1; def. $\subseteq$)

Note that the statement $x < 30$ that we want to show occurs as the last step in each of the cases dictated by the rule for using *or* statements. We continue, from the top. Step 3 is of the form $element \in set$. The reason for Step 4 is therefore the definition of that set.

	1. Let $x \in A \cup B$ be arbitrary.	
	2. $x \in A$ *or* $x \in B$	(1; def. $\cup$)
Case 1	3. $x \in A$	
	4. $x < 10$	(3; def. A)
	.	
	j-1. $x < 30$	
Case 2	j. $x \in B$	
	.	
	k-4. $x < 30$	
	k-3. $x < 30$	(2—k-4; us. *or*)
	k-2. $x \in C$	(k-3; def. C)
	k-1. $for\ all\ x \in A \cup B : x \in C$	(1—k-2; pr. $\forall$)
	k. $A \cup B \subseteq C$	(k-1; def. $\subseteq$)

Connecting Step 4 and Step j-1 remains, but the way to do this is clear. We use the transitivity of $<$. Case 2 is done similarly, and this gives a complete proof.

Proof:

Assume: $A = \{t \in \mathbb{N} \mid t < 10\}$
$B = \{t \in \mathbb{N} \mid t < 20\}$
$C = \{t \in \mathbb{N} \mid t < 30\}$

Show: $A \cup B \subseteq C$

	1. Let $x \in A \cup B$ be arbitrary.	
	2. $x \in A$ *or* $x \in B$	(1; def. $\cup$)
Case 1	3. $x \in A$	
	4. $x < 10$	(3; def. A)
	5. $10 < 30$	(given)
	6. $x < 30$	(4, 5; Trans. $<$)
Case 2	7. $x \in B$	
	8. $x < 20$	(7; def. B)
	9. $20 < 30$	(given)
	10. $x < 30$	(8, 9; Trans.<)
	11. $x < 30$	(2—10; us. *or*)
	12. $x \in C$	(11; def. C)
13.	$for\ all\ x \in A \cup B : x \in C$	(1—12; pr. $\forall$)
14.	$A \cup B \subseteq C$	(13; def. $\subseteq$)

□

Note that it isn't necessary to provide justification for steps in which we make an assumption. They are true by assumption. The following theorem is a generalization of Example 3.

Theorem 6.1 For sets A, B and C, if $A \subseteq C$ and $B \subseteq C$, then $A \cup B \subseteq C$.

Proof:

Assume: A, B, C sets
1. $A \subseteq C$
2. $B \subseteq C$

Show: $A \cup B \subseteq C$

If we draw $A \subseteq C$ and $B \subseteq C$ in Figure 6.2, it is clear that $A \cup B$ must be a subset of C — as in Figure 6.3:

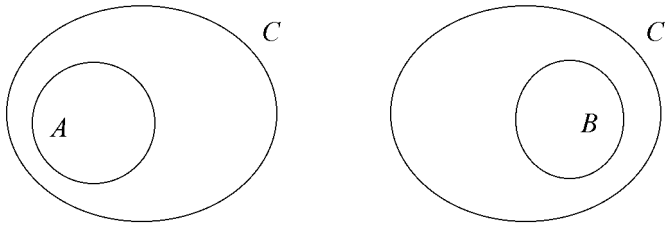


Figure 6.2

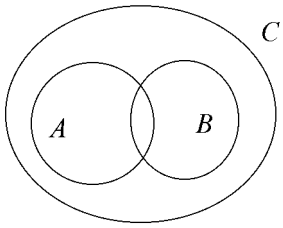


Figure 6.3

The proof of Theorem 6.1 is for you to do (Exercise 2). Follow the step-discovery outline.

The general rule for using *or* statements involves statements of the form $\mathcal{P}_1$ *or* $\mathcal{P}_2$ *or* ... *or* $\mathcal{P}_n$. Each of the n constituent statements $\mathcal{P}_1$ through $\mathcal{P}_n$ corresponds to a case in the proof, so there are n cases.

Inference Rule Using *or* statements: From the *or* statement $\mathcal{P}_1$ *or* $\mathcal{P}_2$ *or* ... *or* $\mathcal{P}_n$, we may infer any step that is true in all cases that don't lead to a contradiction. In particular, in order to use the statement $\mathcal{P}_1$ *or* $\mathcal{P}_2$ *or* ... *or* $\mathcal{P}_n$ to prove a statement $\mathcal{R}$, show that $\mathcal{R}$ holds in all cases that do not lead to a contradiction. (If all cases lead to a contradiction, then we may infer the negation of the assumption leading the block of steps containing the statement $\mathcal{P}_1$ *or* $\mathcal{P}_2$ *or* ... *or* $\mathcal{P}_n$. See Example 3 of Section 15, "Proof by Contradiction".)

By a *contradiction*, we mean a step in a proof that is the negation of a statement that we already know is true: some hypothesis, previously shown theorem, or more often, a previously established step in the proof. We use the symbol # to denote "contradiction".

Example 4:

6. $x \in A$

7. $x < 7$ *or* $x \in B$

Case 1 8. $x < 7$

.

10. $x \notin A$, # Step 6

Case 2 11. $x \in B$

.

13. _____

14. $x \in C$ (7—13; us. *or*)

Solution:

6. $x \in A$

7. $x < 7$ *or* $x \in B$

Case 1 8. $x < 7$

.

10. $x \notin A$, # Step 6

Case 2 11. $x \in B$

.

13. $x \in C$

14. $x \in C$ (7—13; us. *or*)

In Case 1 of Example 4, Step 10 is the statement $x \notin A$. This statement is the negation of Step 6, which we already know. Thus Step 10 contradicts Step 6. We have noted this fact after Step 10, with the phrase "# Step 6".

The justification for Step 14 says that we have obtained this step by the rule for using the *or* statement in Step 7. Thus we have concluded $x \in C$ by the rule. The rule states that we must have $x \in C$ as a step in each case that does not lead to a contradiction. Since Case 1 does lead to a contradiction, we need to have $x \in C$ as a step in Case 2.

The rule, in its general form, will be needed to prove Theorem 8.2.

EXERCISES

1. (a)

1. _____

Case 1
2. $x \in C$
3. ...
4. _____

Case 2
5. $x \in D$
6. ...
7. _____

8. $x < 7$ (1—7, us. *or*)

(b)

1. $x \in C$ *or* $y \in C$

Case 1
2. $x \in C$
3. ...
4. $y \in D$

Case 2
5. _____
6. ...
7. _____

8. _____ (1—7; us. *or*)

(c)

1. _____
2. $x \in A$ *or* $x \in B$ (1; def. $\cup$)

(d)

1. s $\in A \cup B$
2. _____ (1; def. $\cup$)

(e)

1. $x \in C$ *or* $x \in D$
2. _____ (1; def. _____)

(f)

1. $x \in A \cup B$
2. _____ (1; def. $\cup$)

Case 1 3. _____

4. ...
5. _____

Case 2 6. _____

7. ...
8. _____

9. $x \in C$ (2—8; us. *or*)

(g)

1. $x <$ 6 or y $<$ 5

Case 1 2. _____

3. ...
4. $y \in A$

Case 2 5. _____

6. ...
7. _____

8. _____ (1—7; us. *or*)

(h)

1. Let $x \in G$ be arbitrary

.

.

k. $x \in H \cup K$

k+1. _____ (1—k;_____)

2. Prove Theorem 6.1.

Implicit Defining Conditions

When we define a relation, we make the relation equivalent to its defining condition. The rule for using equivalence then lets us substitute the defining condition for the relation, and vice versa, in proof steps. For example, the relation $J \subseteq K$ between J and K is, by definition, equivalent to the logical statement $for\,all\ x \in J\mathbf{:}\ x \in K$. Thus, we might have either of the pairs of proof steps below.

1. $J \subseteq K$
2. $for\,all\ x \in J\mathbf{:}\ x \in K$ (1; def. $\subseteq$)

1. $for\,all\ x \in J\mathbf{:}\ x \in K$
2. $J \subseteq K$ (1; def. $\subseteq$)

According to the inference rules we have to date, this is the only way that we can use the definition of $\subseteq$ in a proof. We are now at the point of wanting to use defining conditions implicitly, without actually writing them down in proof steps. In our minds, we identify the relation $J \subseteq K$ with its defining condition $for\,all\ x \in J\mathbf{:}\ x \in K$. Thus to use a relation $J \subseteq K$ that we know is true, we use the equivalent $for\,all$ statement. However, we think of this not as using the $for\,all$ statement, but as using the relation $J \subseteq K$.

Suppose we have proof steps 1 and 2 below.

1. $a \in J$
2. $J \subseteq K$

To apply the information in Step 2 to Step 1, we apply the defining condition $for\,all\ x \in J\mathbf{:}\ x \in K$ to Step 1 to conclude $a \in K$. However, we think of this as applying the relation $J \subseteq K$ to Step 1 to conclude $a \in K$.

1. $a \in J$
2. $J \subseteq K$
3. $a \in K$ (1, 2; def. $\subseteq$)

The defining condition for $J \subseteq K$ becomes implicit. We use the defining condition, to write Step 3, but we don't write the defining condition down. Consider again the logic behind Steps 1 through 3 above: We know $a \in J$. We also know that everything in J is also in K. We therefore know that $a \in K$. This informal logic is perfectly clear, but there are things that are implicit in it. How do we know that everything in J is also in K? By the definition of $\subseteq$. The definition of $\subseteq$ has been used implicitly. We now state a rule that formally allows us to use definitions in this way.

Inference Rule Implicit definition rule: If the defining condition for some relation is a statement $\mathcal{P}$, then to prove the relation we prove $\mathcal{P}$, without writing $\mathcal{P}$ down. To use the relation, we use $\mathcal{P}$, without writing $\mathcal{P}$ down.

If we wish to call attention to the fact that we're using defining conditions implicitly, according to the rule above, we will write “imp.” after citing the appropriate definition. The notation “exp.” after the citation means that we are using the former rule.

Example 1:

In the exercise below, first fill in the underlined place using the implicit definition rule. Then in the second, explicit version of the same proof fragment, fill in the "missing " step with the explicit defining condition, and get the same conclusion as in the first steps.

1. $A \subseteq B$
2. $x \in A$
3. _____ (1, 2; def. $\subseteq$, imp.)

1. $A \subseteq B$
2. $x \in A$

$2\frac{1}{2}$. _____ (1; def. $\subseteq$, exp.)

3. _____ (2, 2 1/2;_____)

Solution:

1. $A \subseteq B$
2. $x \in A$
3. $x \in B$ (1, 2; def. $\subseteq$, imp.)

1. $A \subseteq B$
2. $x \in A$

$2\frac{1}{2}$. $for\ all\ t \in A: t \in B$ (1; def. $\subseteq$, exp.)

3. $x \in B$ (2, 2 1/2; us, $\forall$)

The effect of using the implicit definition rule is to remove from proofs some statements of a basic logic form, and to leave only more mathematical looking statements.

Example 2:

Recall the proof of Example 1 of Section 5:

Proof:

Assume: $K = \{x \in \mathbb{N} \mid x < 20\}$
$J \subseteq K$

Show: $for\ all\ a \in J: a < 20$

1. Let $a \in J$ be arbitrary.
2. $for\ all\ x \in J: x \in K$ (hyp.; def. $\subseteq$)
3. $a \in K$ (1, 2; us. $\forall$)
4. $a < 20$ (3; def. K)

5. $for\ all\ a \in J: a < 20$ (1— 4; pr. $\forall$)

□

Steps 1, 2, and 3 are needed—if we use the *explicit* form of the definition of $\subseteq$:

1. Let $a \in J$ be arbitrary.
2. $for\ all\ x \in J$: $x \in K$ (hyp.; def. $\subseteq$)
3. $a \in K$ (1, 2; us. $\forall$)

By using the *implicit* definition rule, however, we can use the hypothesis ($J \subseteq K$) and Step 1 ($a \in J$) to infer $a \in K$ immediately—which we now renumber as Step 2:

Proof:

Assume: $K = \{x \in \mathbb{N} \mid x < 20\}$
$J \subseteq K$

Show: $for\ all\ a \in J$: $a < 20$

1. Let $a \in J$ be arbitrary.
2. $a \in K$ (1, hyp.; def. $\subseteq$, imp.)
3. $a < 20$ (2; def. K)

4. $for\ all\ a \in J$: $a < 20$ (1—3; pr. $\forall$)

□

Using the implicit definition rule tends to focus our attention on the mathematical objects we're talking about, and not on the logical form of statements about them. Our logic should become increasingly implicit (but well understood). Note that our proof style begins with completely explicit use of definitions, inference rules, and formal statements. We move to implicit use of the rules after some practice with the explicit use. The correct approach from a pedagogical viewpoint is to move from the explicit to the implicit—not vice versa. In any area where understanding is paramount, shortcuts should not be learned before one gets the lay of the land.

Example 3:

Recall the proof of Example 4 of Section 4:

Proof:

Assume: $H = \{x \in \mathbb{N} \mid x < 10\}$
$G = \{x \in \mathbb{N} \mid x < 20\}$

Show: $H \subseteq G$

1. Let $x \in H$ be arbitrary.
2. $x < 10$ (1; def. H)
3. $10 < 20$ (given)
4. $x < 20$ (2, 3; Trans. $<$)
5. $x \in G$ (4; def. G)

6. $for\ all\ x \in H$: $x \in G$ (1—5; pr. $\forall$)
7. $H \subseteq G$ (6; def. $\subseteq$)

□

The defining condition for $H \subseteq G$ (Step 7) is explicitly written down as Step 6. If we were to use the implicit definition rule, we would not write the $for\ all$ statement of Step 6 down in the

proof. We would go through all the steps necessary to prove this $for\,all$ statement, but we would consider these steps as proving the equivalent statement $H \subseteq G$ instead of the $for\,all$ statement. The $for\,all$ statement becomes implicit:

Proof:

Assume: $H = \{x \in \mathbb{N} \mid x < 10\}$

$G = \{x \in \mathbb{N} \mid x < 20\}$

Show: $H \subseteq G$

1. Let $x \in H$ be arbitrary.
2. $x < 10$ (1; def. H)
3. $10 < 20$ (given)
4. $x < 20$ (2, 3; Trans. $<$)
5. $x \in G$ (4; def. G)
6. $H \subseteq G$ (1—5; def. $\subseteq$, imp.)

□

The implicit definition rule is involved when we provide counterexamples to statements about set containment. For example, consider the following statement, which we call a proposition, since, at this stage, we presumably don't know whether it is true or false.

Proposition If A and B are sets, then $A \cup B \subseteq B$.

The hypotheses and conclusion are:

Hypotheses: A, B sets

Conclusion: $A \cup B \subseteq B$

In order to exhibit a counterexample, we need to know what it means for $A \cup B \subseteq B$ to be false. By definition of containment, $A \cup B \subseteq B$ means $for\,all\ x \in A \cup B : x \in B$. The negation of this is $there\,exists\ x \in A \cup B\ such\,that\ x \notin B$. This tells us what it means for the $for\,all$ statement to be false. Finding such an x will show that the $for\,all$ statement is false. Since we mentally identify the statement $A \cup B \subseteq B$ with the $for\,all$ statement, we consider that to exhibit sets A and B and an element x that make the $for\ all$ statement false is to provide a counterexample to the assertion about set containment. For example:

Proposition If A and B are sets, then $A \cup B \subseteq B$.

Counterexample 4:

Hypotheses: A, B sets

Conclusion: $A \cup B \subseteq B$

Let $A = \{1\}$ and $B = \{2\}$. Then $A \cup B = \{1, 2\}$. Also $1 \in \{1, 2\}$ but $1 \notin \{2\}$, so that $\{1, 2\} \subseteq \{2\}$ is false.

EXERCISES

1. In each exercise below, first fill in the underlined place using the implicit definition rule. Then in the second, explicit version of the same proof fragment, fill in the "missing " step with the explicit defining condition, and get the same conclusion as in the first steps.

(a)

1. $C \subseteq D$
2. $x \in C$
3. _____ (1, 2; def. $\subseteq$, imp.)

1. $C \subseteq D$
2. $x \in C$

$2\frac{1}{2}$. _____ (1; def. $\subseteq$, exp.)

3. _____ (2, $2\frac{1}{2}$;_____)

(b)

1. X $\subseteq$ Y
2. _____
3. $t \in$ Y (1, 2; def. $\subseteq$, imp.)

1. X $\subseteq$ Y
2. _____

$2\frac{1}{2}$. _____ (1; def. $\subseteq$, exp.)

3. $t \in$ Y (2, $2\frac{1}{2}$;_____)

(c)

1. Let $x \in A$ be arb.
2. $x \in B$
3. _____ (1—2; def. $\subseteq$, imp.)

1. Let $x \in A$ be arb.
2. $x \in B$

$2\frac{1}{2}$. _____ (1—2; _____)

3. _____ ($2\frac{1}{2}$; def. $\subseteq$, exp.)

2. Rewrite the proof of Theorem 5.1, using the implicit definition rule in as many places as you can.

3. Rewrite the proof of Theorem 6.1, using the implicit definition rule in as many places as you can.

REVIEW EXERCISES

4. (a)

1. $x \in A$ *or* $y \in A$

Case 1 2. Assume $x \in A$

3. ...

4. $y \in B$

Case 2 5. _____

6. ...

7. _____

8. _____ (1—7; us. *or*)

(b)

1. s $\in C \cup D$

2. _____ (1; def. $\cup$, exp.)

(c)

1. $t \in C$ *or* $t \in D$

2. _____ (1; def. $\cup$, exp.)

(d)

1. $x \in G \cup H$

2. _____ (1; def. $\cup$, exp.)

Case 1 3. _____

4. ...

5. _____

Case 2 6. _____

7. ...

8. _____

9. $x < 9$ (2—8; us. *or*)

(e)

1. Let $x \in A$ be arbitrary

.

.

k. $x \in A \cup B$

k+1. _____ (1—k;_____)

Unions; Proving *Or* Statements

Inference Rule Proving *or* statements: In order to prove the statement $\mathcal{P}$ *or* $\mathcal{Q}$, either assume $\neg\mathcal{P}$ and show $\mathcal{Q}$, or assume $\neg\mathcal{Q}$ and show $\mathcal{P}$. Abbreviation: "pr. *or*".

There are two possible proof formats for using this rule:

pr. *or*

1. Assume $\neg\mathcal{P}$

k-1.$\mathcal{Q}$

k.. $\mathcal{P}$ *or* $\mathcal{Q}$ (1—k-1; pr. *or*)

pr. *or*

1. Assume $\neg\mathcal{Q}$

k-1.$\mathcal{P}$

k.. $\mathcal{P}$ *or* $\mathcal{Q}$ (1—k-1; pr. *or*)

Example 1:

In the gap indicated by the blank space, write all the steps dictated by the rule for proving *or* statements that justifies Step k.

k. $x \in G$ *or* $x \in H$ (_____; pr. *or*)

Solution 1:

1. Assume $x \notin G$

.

k-1. $x \in H$

k. $x \in G$ *or* $x \in H$ (1—k-1; pr. *or*)

Solution 2:

1. Assume $x \notin H$

.

k-1. $x \in G$

k. $x \in G$ *or* $x \in H$ (1— k-1; pr. *or*)

In any developing proof, the steps dictated by the rule for proving an *or* statement are put at the top and bottom of the gap above the statement.

Since there are two choices available, the rule doesn't dictate a unique pair of statements needed to prove the statement, as does the rule for proving $for\,all$ statements. In general, you will need to consider both possibilities, in order to choose the one that will most likely lead to success. You may even need to try both possible approaches, to see which works out the best.

Example 2:

1. Assume $t \notin A$

.

3. $t \in B$

4. _____ (1—3;_____)

Solution:

1. Assume $t \notin A$

.

3. $t \in B$

4. $t \in A$ *or* $t \in B$ (1—3; pr. *or*)

If x, for example, occurs in the *or* statement

k. $x \in A$ *or* $x \in B$

as a step in a proof, x would have had to have been already defined, either in the hypotheses, or in a previous proof step. The rule for proving *or* statements dictates that the Steps i—k-1 be inserted in the gap before Step k:

i. Assume $x \notin A$

.

k-1. $x \in B$

k. $x \in A$ *or* $x \in B$ (i—k-1; pr.*or*)

Step i does not define x. It makes an assumption about an element that must already be defined. We use the word "let" to define new symbols, and the word "assume" to make an assumption about something that has been defined already.

Example 3:

4. Assume $t \in G$

.

7. $t \in H$

8. _____ (4—7;_____)

Solution:

4. Assume $t \in G$

.

7. $t \in H$

8. t $\notin G$ *or* $t \in H$ (4—7; pr. or)

Example 4:

4. Let $t \in G$ be arbitrary

.

7. $t \in H$

8. _____ (4—7;_____)

Solution:

4. Let $t \in G$ be arbitrary

.

7. $t \in H$

8. $for\,all\ t \in G$: $t \in H$ (4—7; pr. $\forall$)

Suppose we have the following steps in a proof.

i. $x \in A$

.

k. $x \in A$ *or* $x \in B$

That is, suppose we know Step i, and seek to show Step k. The rule for proving or statements dictates steps such as

i. $x \in A$

i+1. Assume $x \notin B$

.

k-1. $x \in A$

k. $x \in A$ *or* $x \in B$ (i+1—k-1; pr.or)

Our job is now to show that Step k-1 is true. But here, Step k-1 is true since it is the same as Step i. Thus we get the following proof of Step k.

i. $x \in A$

i+1. Assume $x \notin B$

i+2. $x \in A$ (Step i)

i+3. $x \in A$ *or* $x \in B$ (i+1—i+2; pr.or)

In general, if we have $\mathcal{P}$ as a step in a proof, then we can prove $\mathcal{P}$ *or* $\mathcal{Q}$ in the manner above:

1. $\mathcal{P}$

2. Assume $\neg\mathcal{Q}$

3. $\mathcal{P}$ (Step 1)

4. $\mathcal{P}$ *or* $\mathcal{Q}$ (2—3; pr. or)

Thus if $\mathcal{P}$ is true then $\mathcal{P}$ *or* $\mathcal{Q}$ follows by the rule for proving *or* —without even using the assumption $\neg\mathcal{Q}$. Of course, in general it will be necessary to use $\neg\mathcal{Q}$ in order to show $\mathcal{P}$. But when $\mathcal{P}$ is known to be true, then $\mathcal{P}$ *or* $\mathcal{Q}$ must follow. We will interpret the rule for proving *or* statements so as to allow the following shortened (EZ) version of the steps above

pr. *or* EZ

1. $\mathcal{P}$
2. $\mathcal{P}$ *or* $\mathcal{Q}$ (1; pr. *or* EZ)

pr. *or* EZ

1. $\mathcal{Q}$
2. $\mathcal{P}$ *or* $\mathcal{Q}$ (1; pr. *or* EZ)

We consider the steps above an extension of the format for proving *or* statements.

If you need to show a statement $\mathcal{P}$ *or* $\mathcal{Q}$ in a proof, the first thing to do would be to see if you already know either of $\mathcal{P}$ or $\mathcal{Q}$. If so, then $\mathcal{P}$ *or* $\mathcal{Q}$ follows immediately by the EZ form of the rule for proving *or* statements. If not, then decide whether it would be better to assume $\neg\mathcal{P}$ and show $\mathcal{Q}$, or to assume $\neg\mathcal{Q}$ and show $\mathcal{P}$.

The shortened format for the rule for proving *or* statements makes the proof of Theorem 8.1 easy.

Theorem 8.1 For sets A and B:
(a) $A \subseteq A \cup B$
(b) $B \subseteq A \cup B$

Proof: Exercise 3

The EZ forms of the rules for proving *or* statements eliminate the need to make an obviously unnecessary assumption. The rules we have for using *or* statements sometimes lead to making an obviously false assumption. For example, suppose we have Steps 1 and 2, and wish to show $\mathcal{Q}$ in Step k below.

1. $\neg\mathcal{P}$
2. $\mathcal{P}$ *or* $\mathcal{Q}$
.
k. $\mathcal{Q}$

$\mathcal{Q}$ is shown by the rule for using the *or* statement in Step 2:

1. $\neg\mathcal{P}$
2. $\mathcal{P}$ *or* $\mathcal{Q}$

Case 1 3. $\mathcal{P}$ # Step 1
Case 2 4. $\mathcal{Q}$
5. $\mathcal{Q}$ (2—4; us. *or*)

Thus $\mathcal{Q}$ in Step 5 is formally established, since we have shown it in all cases that do not lead to a contradiction. The words “lead to” here are not quite appropriate, since the assumption in Case 1 is itself a contradiction. Also, in Case 2 we assume, in effect, the result we seek. We can avoid the unnecessary formalism, by the following EZ forms of the rule for using *or* statements.

us. *or* EZ

1. $\mathcal{P}$ *or* $\mathcal{Q}$
2. $\neg\mathcal{P}$
3. $\mathcal{Q}$ (1, 2; us. *or* EZ)

us. *or* EZ

1. $\mathcal{P}$ *or* $\mathcal{Q}$
2. $\neg\mathcal{Q}$
3. $\mathcal{P}$ (1, 2; us. *or* EZ)

Although the standard forms for the rules for proving and using *or* statements are called for in almost all situations, the EZ forms of the rules are useful in avoiding needless assumptions or assumptions that contradict known facts.

Theorem 8.2 For sets A, B and C, if $A \subseteq B$ *or* $A \subseteq C$ then $A \subseteq B \cup C$.

Proof:

Assume: A,B,C sets
$A \subseteq B$ *or* $A \subseteq C$

Show: $A \subseteq B \cup C$

The hypothesis for this theorem is the single *or* statement $A \subseteq B$ *or* $A \subseteq C$. The statement $A \subseteq B$ is only part of the *or* statement, and is not known to be true; that is, $A \subseteq B$ is not one of the hypotheses. In order to use the hypotheses of this theorem we need to employ the rule for using *or* statements. The step-discovery procedure first gives us the following steps:

1. Let $x \in A$ be arbitrary
.
.

k-3. $x \in B$ *or* $x \in C$ (; pr. *or*)
k-2. $x \in B \cup C$ (k-3; def. $\cup$, exp.)
k-1. $for\ all\ x \in A : x \in B \cup C$ (1—k-2; pr. $\forall$)
k. $A \subseteq B \cup C$ (k-1; def. $\subseteq$, exp.)

The first option in the rule for proving *or* statements dictates the following steps:

1. Let $x \in A$ be arbitrary
2. Assume $x \notin B$
.
.

k-4. $x \in C$
k-3. $x \in B$ *or* $x \in C$ (2—k-4; pr. *or*)

	k-2. $x \in B \cup C$	(k-3; def. $\cup$, exp.)
k-1.	$for\,all\ x \in A : x \in B \cup C$	(1—k-2; pr. $\forall$)
k.	$A \subseteq B \cup C$	(k-1; def. $\subseteq$, exp.)

We are now at the end of the bottom-up/top-down part of the step-discovery procedure, and need to use the hypotheses. As a matter of exposition, we write the hypothesis in the proof itself as Step 3—to precede the cases in the rule for using *or*.

1.	Let $x \in A$ be arbitrary	
	2. Assume $x \notin B$	
	3. $A \subseteq B\ or\ A \subseteq C$	(hyp.)
	.	
	.	
	k-4. $x \in C$	
k-3.	$x \in B\ or\ x \in C$	(2—k-4; pr. *or*)
k-2.	$x \in B \cup C$	(k-3; def. $\cup$, exp.)
k-1.	$for\,all\ x \in A : x \in B \cup C$	(1—k-2; pr. $\forall$)
k.	$A \subseteq B \cup C$	(k-1; def. $\subseteq$, exp.)

We now need to use the *or* statement of Step 3, which means that we have cases.

1.	Let $x \in A$ be arbitrary	
	2. Assume $x \notin B$	
	3. $A \subseteq B\ or\ A \subseteq C$	(hyp.)
Case 1	4. $A \subseteq B$	
	5. $x \in B$, # Step 2	(1, 4; def. $\subseteq$, imp.)
Case 2	6. $A \subseteq C$	
	7. $x \in C$	(1, 6; def. $\subseteq$, imp.)
	8. $x \in C$	(3—7; us. *or*)
9.	$x \in B\ or\ x \in C$	(2—8; pr. *or*)
10.	$x \in B \cup C$	(9; def. $\cup$, exp.)
11.	$for\,all\ x \in A : x \in B \cup C$	(1—10; pr. $\forall$)
12.	$A \subseteq B \cup C$	(11; def. $\subseteq$, exp.)

□

After Step 5, we have noted the fact that this step contradicts Step 2. The justification for Step 5 is the reason that it follows from previous steps, regardless of the fact that it is a contradiction. Step 5 follows from Steps 1 and 4, by the rule for using defining conditions implicitly. The fact that it contradicts Step 2 says that Case 1 in the proof really doesn't occur, under the assumptions preceding the *or* statement.

The use of an *or* statement that we know is true leads to cases. These cases can be used in an informal interpretation of Theorem 8.2 in terms of Venn diagrams. Figure 8.1 shows that the conclusion of the theorem holds in both cases indicated by the hypothesis:

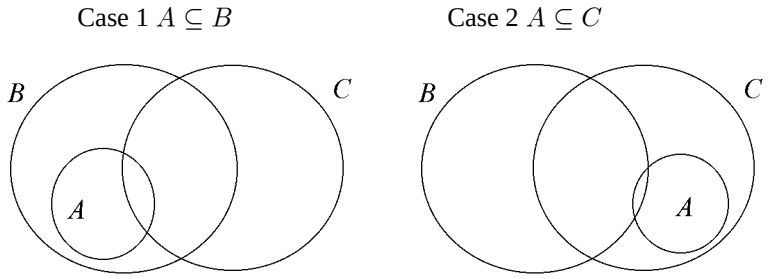


Figure 8.1

Example 5:

1. _____
2. $x \in A \cup B$ (1; def. $\cup$, exp.)

Solution:

1. $x \in A$ *or* $x \in B$
2. $x \in A \cup B$ (1; def. $\cup$, exp.)

Example 6:

1. _____
2. $x \in A \cup B$ (1; def. $\cup$, imp.)

Solution:

1. $x \in A$
2. $x \in A \cup B$ (1; def. $\cup$, imp.)

Example 6 illustrates the use of the implicit definition rule: By the definition of $\subseteq$, $x \in A \cup B$ means $x \in A$ *or* $x \in B$. The only way to prove this *or* statement with a single preceding step is to use the short (EZ) format; that is, either $x \in A$ or $x \in B$ must be the preceding step. Either of these statements would be satisfactory as Step 1. The intermediate step $x \in A$ *or* $x \in B$ in going from $x \in A$ to $x \in A \cup B$ is not written down.

In Example 7, we find a block of steps that proves the implicit *or* statement.

Example 7:

1. _____
.
j. _____
j+1. $x \in A \cup B$ (1—j; def. $\cup$, imp.)

Solution:

1. Assume $x \notin A$
.
j. $x \in B$
j+1. $x \in A \cup B$ (1—j; def. $\cup$, imp.)

Definition Given $a, b \in \mathbb{N}$, we say a is *less than or equal to* b (written $a \leq b$) iff $a < b$ *or* $a = b$.

Theorem 8.3 Transitivity of $\leq$: For $a,\ b,\ c \in \mathbb{N}$, if $a \leq b$ and $b \leq c$, then $a \leq c$.

Proof: Exercise 4.

The proof of Theorem 8.3 uses the following rule of inference:

Inference Rule Substitution: Any name or expression for a mathematical object can be replaced by another name or expression for the same object. It is necessary to avoid using the same name for different objects.

Example 8:

1. $a < b$
2. $b = c$
3. $a < c$ (1, 2; substitution)

In Example 8, b in Step 1 is replaced by c to get Step 3 — b and c being equal by Step 2. The equal sign in Step 2 means that b and c are two names for exactly the same number. Thus the statement in Step 3 is exactly the same statement as Step 1, except that another name for the number to the right of the " $<$ " sign is used. Thus the name "c" is substituted for the name "b" in this statement. The numbers remain the same. Only the names are changed.

EXERCISES

1. Write all the steps dictated by the rule for proving *or* statements that show Step k.

   k. $x \in A$ *or* $x \in B$ (_____; pr. *or*)

2. Fill in the underlined places in the following proof fragments.

   (a) 1. Assume $y \notin J$
   .
   3. $y \in K$
   4. _____ (1—3; _____)

   (b) 4. Assume $y \in J$
   .
   7. $y \in K$
   8. _____ (4—7;_____)

   (c) 4. Let $x \in A$ be arbitrary
   .
   7. $x \in B$
   8. _____ (4—7;_____)

   (d) 1. _____
   2. $x \in C \cup D$ (1; def. $\cup$, exp.)

(e) 1. _____
2. $x \in C \cup D$ (1; def. $\cup$, imp.)

(f) 1. _____
.
5. _____
6. $t \in X \cup Y$ (1—5; def. $\cup$, imp.)

3. (a) Write two proofs of Theorem 8.1a—one using the original, explicit definition rule, and one using the implicit definition rule.
(b) Same problem as in part (a)—applied to Theorem 8.1b.

4. Prove Theorem 8.3. First, fill in the steps dictated by the conclusion. Next, use one of the hypotheses. This will introduce cases into the proof. Label these Case 1 and Case 2. Use the second hypothesis in both Case 1 and Case 2. In Case 1, indent further for the new cases introduced by the second hypothesis. Call the new cases Case 1a and Case 1b. Similarly, in Case 2, call the new cases Case 2a and 2b.

In the following problems provide proofs for all true assertions. Provide counterexamples for those problems where you are asked to prove a false assertion.

5. Let A, B, and C be sets. Prove $A \cup B \subseteq A \cup C$.

6. Let $A \subseteq C$ and $B \subseteq D$ for sets A, B, C, and D. Prove $A \cup B \subseteq C \cup D$.

7. Let $A \cup B \subseteq A \cup C$ for sets A, B, and C. Prove $B \subseteq C$.

8. If $\mathcal{P}$ and $\mathcal{Q}$ are statements, the informal statement "if $\mathcal{P}$, then $\mathcal{Q}$" formed from them is called an *implication.* (Formal implications will be considered in Section 15.) The *converse* of the implication "if $\mathcal{P}$, then $\mathcal{Q}$" is formed by interchanging $\mathcal{P}$ and $\mathcal{Q}$ to obtain "if $\mathcal{Q}$, then $\mathcal{P}$". In Theorem 8.2 (For sets A, B and C, if $A \subseteq B$ *or* $A \subseteq C$ then $A \subseteq B \cup C$), if we replace the implication "if $A \subseteq B$ *or* $A \subseteq C$ then $A \subseteq B \cup C$" with its converse "if $A \subseteq B \cup C$, then $A \subseteq B$ *or* $A \subseteq C$" we get the statement "For sets A, B and C, if $A \subseteq B \cup C$, then $A \subseteq B$ *or* $A \subseteq C$". Prove this, or find a counterexample.

REVIEW EXERCISES

9. (a) 1. _____
Case 1 2. $t \in A$
3. . . .
4. _____
Case 2 5. $t \in B$
6. . . .
7. _____
8. $t < 9$ (1—7, us. *or*)

(b) 1. _____
2. $x \in C$ *or* $x \in D$ (1; def. $\cup$, exp.)

(c) 1. $t < 7$ *or* $4 <$ s

Case 1 2. _____

3. ...

4. s $\in T$

Case 2 5. _____

6. ...

7. _____

8. _____ (1—7; us. *or*)

10. In each exercise below, first fill in the underlined place using the implicit definition rule. Then in the second, explicit version of the same proof fragment, fill in the "missing " step with the explicit defining condition, and get the same conclusion as in the first steps.

(a) 1. $G \subseteq H$

2. $t \in G$

3. _____ (1, 2; def. $\subseteq$, imp.)

1. $G \subseteq H$

2. $t \in G$

$2\frac{1}{2}$. _____ (1; def. $\subseteq$, exp.)

3. _____ (2, $2\frac{1}{2}$;_____)

(b) 1. $G \subseteq H$

2. _____

3. $x \in H$ (1, 2; def. $\subseteq$, imp.)

1. $G \subseteq H$

2. _____

$2\frac{1}{2}$. _____ (1; def. $\subseteq$, exp.)

3. $x \in H$ (2, $2\frac{1}{2}$;_____)

(c) 1. Let $t \in G$ be arb.

2. $t \in H$

3. _____ (1—2; def. $\subseteq$, imp.)

1. Let $t \in G$ be arb.

2. $t \in H$

$2\frac{1}{2}$. _____ (1—2; _____)

3. _____ ($2\frac{1}{2}$; def. $\subseteq$, exp.)

Intersections; And Statements

Definition For any sets A and B, the *intersection* of A and B is the set $A \cap B$ defined by $A \cap B = \{x \mid x \in A \; and \; x \in B\}$.

The connective and in our formal language has an informal meaning which is identical to the word "and". Thus for sets A and B, an element is in the intersection $A \cap B$ if it is in both A and B. From this informal meaning of "and" we can give examples of the intersection of a few sets:

Example 1:

(a) If $A = \{2, 3, 4\}$ and $B = \{3, 4, 5\}$, then $A \cap B = \{3, 4\}$.

(b) If $R = \{1, 2, 3\}$ and $S = \{2, 3\}$, then $R \cap S = \{2, 3\}$.

(c) If $C = \{2, 4, 6, 8, ...\}$ and $D = \{1, 3, 5, 7, \; ...\}$, then $C \cap D = \emptyset$.

The set $A \cap B$ is represented by the shaded area in the Venn diagram of Figure 9.1:

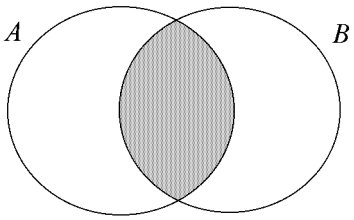


Figure 9.1

To deal with and statements in a proof, we have two rules—which determine the formal meaning. Notice that the rules are "logical" if the formal and agrees with our informal idea.

Inference Rule Using and statements: If $\mathcal{P} \; and \; \mathcal{Q}$ is a step in a proof, then $\mathcal{P}$ can be written as a step and $\mathcal{Q}$ can be written as a step. Abbreviation: "us. & ".

Formats:

us. &

1. $\mathcal{P} \; and \; \mathcal{Q}$
2. $\mathcal{Q}$ (1; us. &)

us. &

1. $\mathcal{P}$ *and* $\mathcal{Q}$
2. $\mathcal{P}$ (1; us. &)

Example 2:

1. $x < 1$ *and* $x \in A$
2. _____ (1; us. &)

Solution:

1. $x < 1$ *and* $x \in A$
2. $x < 1$ (or 2. $x \in A$) (1; us. &)

Inference Rule Proving *and* statements: In order to show $\mathcal{P}$ *and* $\mathcal{Q}$ in a proof, show $\mathcal{P}$ and also show $\mathcal{Q}$. Abbreviation: "pr. & ".

The proof format for using this rule for proving *and* statements is:

pr. &

j. $\mathcal{P}$

k-1. $\mathcal{Q}$

k. $\mathcal{P}$ *and* $\mathcal{Q}$ (j, k-1; pr. &)

Example 3:

1. _____
2. _____
3. $x \in$ M *and* $x \in$ N (1, 2; pr. &)

Solution:

1. $x \in$ M
2. $x \in$ N
3. $x \in$ M *and* $x \in$ N (1, 2; pr. &)

Theorem 9.1 For sets A and B:
(a) $A \cap B \subseteq A$
(b) $A \cap B \subseteq B$

Proof: Exercise 3.

Theorem 9.2 For sets A, B, and C, if $A \subseteq B$ and $A \subseteq C$, then $A \subseteq B \cap C$.

Proof: Exercise 4.

For sets A and B, we write $A = B$ to mean that A and B are two names for exactly the same set. We don't formally know what "same set" is, however, since "set" is undefined. If the idea of set were defined, then to prove $A = B$ we would show that A and B were exactly the same thing under the definition. Since "set" is undefined, in order to prove that two sets are equal, we must define what we mean by equal sets.

Definition A set A is $equal$ to a set B (written $A = B$) provided that $A \subseteq B \; and \; B \subseteq A$.

Example 4:

1. $A = B$
2. _____ (1; def. $=$, exp.)
3. _____ (2; us. &)
4. _____ (2; us. &)

Solution:

1. $A = B$
2. $A \subseteq B \; and \; B \subseteq A$ (1; def. $=$, exp.)
3. $A \subseteq B$ (2; us. &)
4. $B \subseteq A$ (2; us. &)

Example 5:

1. $A = B$
2. _____ (1; def. $=$, imp.)
3. _____ (1; def. $=$, imp.)

Solution:

1. $A = B$
2. $A \subseteq B$ (1; def. $=$, imp.)
3. $B \subseteq A$ (1; def. $=$, imp.)

Example 6:

1. _____
2. _____
3. $A = B$ (1, 2; def. $=$, imp.)

Solution:

1. $A \subseteq B$
2. $B \subseteq A$
3. $A = B$ (1, 2; def. $=$, imp.)

EXERCISES

1. (a) 1. $x \in C \; and \; x \leq 7$
   2. _____ (1; us. &)

   (b) 1. _____
   2. _____
   3. $t \in A \; and \; x \in A$ (1, 2; pr. &)

   (c) 1. $G = H$
   2. _____ (1; def. $=$, exp.)
   3. _____ (2; us. &)
   4. _____ (2; us. &)

   (d) 1. $G = H$
   2. _____ (1; def. $=$, imp.)
   3. _____ (1; def. $=$, imp.)

   (e) 1. _____
   2. _____
   3. $G = H$ (1, 2; def. $=$, imp.)

2. Use the step-discovery procedure to fill in all the proof steps you can leading up to a proof of a proposition with the following hypothesis and conclusion:

   Assume: G, H sets

   Show: $G = H$

   Give a counterexample to show that $G = H$ is not true for all sets G and H.

3. Prove Theorem 9.1.

4. Prove Theorem 9.2, and draw a Venn diagram that illustrates the theorem.

5. Let A, B, C, and D be sets. Prove or disprove the following propositions:

   (a) $A \subseteq A \cap B$.

   (b) If $A \subseteq B$ and $C \subseteq D$, then $A \cap C \subseteq B \cap D$.

REVIEW EXERCISES

6. Write all the steps dictated by the rule for proving *or* statements that show Step k.

k. $x \leq 9$ *or* $x \in C$ (_____; pr.*or*)

7. (a) 1. Assume $t \notin C$

.

3. $t \in D$

4. _____ (1—3; _____)

(b) 4. Let $t \in C$ be arbitrary

.

7. $t \in D$

8. _____ (4—7;_____)

(c) 1. _____

2. $t \in X \cup Y$ (1; def. $\cup$, imp.)

Symmetry

Theorem 10.1 For sets A and B,
(a) $A \cap B = B \cap A$
(b) $A \cup B = B \cup A$

We will use the proof of Theorem 10.1a as motivation for a new inference rule that will enable us to abbreviate proofs considerably. The final version of the proof will employ this rule. You are to employ the same rule to prove part (b). Note that the inference rule you will use to prove part (b) is stated after Theorem 10.1. In general, you are allowed to use any rule stated in a section to prove any theorem in the section—regardless of the order in which the rule and theorem are stated. This won't violate the principle of orderly, logical development, since the rules don't depend on theorems for their validity.

Proof:

Assume: A,B sets

Show: $A \cap B = B \cap A$

k-1.	$A \cap B \subseteq B \cap A$ *and* $B \cap A \subseteq A \cap B$	(; pr. &)
k.	$A \cap B = B \cap A$	(k-1; def. $=$, exp.)

We have written the conclusion as Step k. This step is of the form $set = set$, so we use the definition of equal sets to get Step k-1. Step k-1 is an *and* statement. The rule for proving *and* statements dictates two previous steps—which we write separately, since the two steps will have to be shown separately.

Proof:

Assume: A,B sets

Show: $A \cap B = B \cap A$

.		
j.	$A \cap B \subseteq B \cap A$	
.		
k-2.	$B \cap A \subseteq A \cap B$	
k-1.	$A \cap B \subseteq B \cap A$ *and* $B \cap A \subseteq A \cap B$	(j, k-2 ; pr. &)
k.	$A \cap B = B \cap A$	(k-1; def. $=$, exp.)

Note that the definition of intersection has not entered into the analysis yet. There are two steps (j and k-2) to establish. Further analysis leads to the following steps toward establishing Step j:

	1. Let $x \in A \cap B$ be arbitrary	
	.	
	j-2. $x \in B \cap A$	
j-1.	$for\ all\ x \in A \cap B : x \in B \cap A$	(1—j-2; pr. $\forall$)
j.	$A \cap B \subseteq B \cap A$	(j-1; def. $\subseteq$)

The definition of intersection and the rules for proving and using and statements provide the missing steps:

	1. Let $x \in A \cap B$ be arbitrary	
	2. $x \in A\ and\ x \in B$	(1; def. $\cap$, exp.)
	3. $x \in A$	(2; us. &)
	4. $x \in B$	(2; us. &)
	5. $x \in B\ and\ x \in A$	(3, 4; pr. &)
	6. $x \in B \cap A$	(5; def. $\cap$, exp.)
7.	$for\ all\ x \in A \cap B : x \in B \cap A$	(1—6; pr. $\forall$)
8.	$A \cap B \subseteq B \cap A$	(7; def. $\subseteq$, exp.)

We have established Step j (now Step 8), the first of the steps needed to prove the and statement in Step k-1. We now need to establish the second step, k-2: $B \cap A \subseteq A \cap B$. But notice that Step k-2 is just Step 8 with the roles of A and B reversed. Steps 9 through 16 are obtained by rewriting Steps 1 through 8 with the roles of A and B reversed:

	1. Let $x \in A \cap B$ be arbitrary	
	2. $x \in A\ and\ x \in B$	(1; def. $\cap$, exp.)
	3. $x \in A$	(2; us. &)
	4. $x \in B$	(2; us. &)
	5. $x \in B\ and\ x \in A$	(3, 4; pr. &)
	6. $x \in B \cap A$	(5; def. $\cap$, exp.)
7.	$for\ all\ x \in A \cap B : x \in B \cap A$	(1—6; pr. $\forall$)
8.	$A \cap B \subseteq B \cap A$	(7; def. $\subseteq$, exp.)
	9. Let $x \in B \cap A$ be arbitrary	
	10. $x \in B\ and\ x \in A$	(9; def. $\cap$, exp.)
	11. $x \in B$	(10; us. &)
	12. $x \in A$	(10; us. &)
	13. $x \in A\ and\ x \in B$	(11, 12; pr. &)
	14. $x \in A \cap B$	(13; def. $\cap$, exp.)

15. $for\ all\ x \in B \cap A : x \in A \cap B$ (9—14; pr. $\forall$)
16. $B \cap A \subseteq A \cap B$ (15; def. $\subseteq$, exp.)

The complete proof is therefore:

Proof of (a):

Assume: A,B sets

Show: $A \cap B = B \cap A$

1. Let $x \in A \cap B$ be arbitrary
2. $x \in A\ and\ x \in B$ (1; def. $\cap$, exp.)
3. $x \in A$ (2; us. &)
4. $x \in B$ (2; us. &)
5. $x \in B\ and\ x \in A$ (3, 4; pr. &)
6. $x \in B \cap A$ (5; def. $\cap$, exp.)

7. $for\ all\ x \in A \cap B : x \in B \cap A$ (1—6; pr. $\forall$)
8. $A \cap B \subseteq B \cap A$ (7; def. $\subseteq$, exp.)

9. Let $x \in B \cap A$ be arbitrary
10. $x \in B\ and\ x \in A$ (9; def. $\cap$, exp.)
11. $x \in B$ (10; us. &)
12. $x \in A$ (10; us. &)
13. $x \in A\ and\ x \in B$ (11, 12; pr. &)
14. $x \in A \cap B$ (13; def. $\cap$, exp.)

15. $for\ all\ x \in B \cap A : x \in A \cap B$ (9—14; pr. $\forall$)
16. $B \cap A \subseteq A \cap B$ (15; def. $\subseteq$, exp.)
17. $A \cap B \subseteq B \cap A\ and\ B \cap A \subseteq A \cap B$ (8, 16 ; pr. &)
18. $A \cap B = B \cap A$ (17; def. $=$, exp.)

□

Since Steps 9 through 16 are identical to Steps 1 through 8, except that the roles of A and B have been reversed, it is just a matter of uninformative busy work to write all the repetitive steps down. We will shortcut the process by replacing Steps 9 through 16 above with Step 9 below:

Proof of (a):

Assume: A,B sets

Show: $A \cap B = B \cap A$

1. Let $x \in A \cap B$ be arbitrary
2. $x \in A\ and\ x \in B$ (1; def. $\cap$, exp.)
3. $x \in A$ (2; us. &)
4. $x \in B$ (2; us. &)
5. $x \in B\ and\ x \in A$ (3, 4; pr. &)
6. $x \in B \cap A$ (5; def. $\cap$, exp.)

7. $for\ all\ x \in A \cap B : x \in B \cap A$ (1—6; pr. $\forall$)

8.	$A \cap B \subseteq B \cap A$	(7; def. $\subseteq$, exp.)
9.	$B \cap A \subseteq A \cap B$	(1—8; symmetry in A and B)
10.	$A \cap B \subseteq B \cap A$ *and* $B \cap A \subseteq A \cap B$	(8, 9 ; pr. &)
11.	$A \cap B = B \cap A$	(10; def. $=$, exp.)

□

The use of symmetry is formalized with the following rule, which we call an inference rule, although it would more properly be called a shortcut rule.

Inference Rule Using Symmetry: If a sequence of steps establishes the statement $\mathcal{Q}(A,B)$ in a proof, and if the sequence of the steps is valid with the roles of A and B reversed, then the statement $\mathcal{Q}(B,A)$ ($\mathcal{Q}$ with A and B reversed) may be written as a proof step. Abbreviation: "sym. A & B".

Note that in using symmetry in A and B in going from Step 8 to 9 in the proof above, we are doing this:

$$\begin{array}{c} A \cap B \subseteq B \cap A \\ \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \\ B \cap A \subseteq A \cap B \end{array}$$

not this:

$$\begin{array}{c} A \cap B \subseteq B \cap A \\ \searrow \quad \swarrow \\ B \cap A \subseteq A \cap B \end{array}$$

A statement $\mathcal{P}(A,B)$ that we accept as true for the sake of argument is called a *premise*. Thus the hypotheses that we get by interpreting theorem statements are premises. We also call assumptions made within a proof premises. Statements valid under the latter kind of premise are written at the same indentation level as the premise, or as further indentations within that level. The principle behind the use of symmetry is that if $\mathcal{Q}(A,B)$ follows from the premise $\mathcal{P}(A,B)$, then $\mathcal{Q}(B,A)$ follows from the premise $\mathcal{P}(B,A)$. The reason is that "A" and "B" are just names which could just as easily be interchanged.

In the proof above, the statement $\mathcal{Q}(A,B)$ ($A \cap B \subseteq B \cap A$) follows from an empty set of premises: the symbols "A" and "B" are named in the hypotheses, but there are no assumptions made about A and B. The empty set of premises is symmetric in A and B. The first set mentioned could be called "B" just as well as "A". The statement $\mathcal{Q}(B,A)$ ($B \cap A \subseteq A \cap B$) also follows from the hypotheses, and is at the same, highest indentation level—not dependent on any additional premises that are not symmetric in A and B.

When a step justified by symmetry depends on no premises (and is therefore at the highest indentation level) we list in the justification the symmetric step and the block of steps used to establish it. For example, the justification (1—8; sym. A & B) for Step 9 in the proof above means that Step 9 is symmetric with Step 8 and that Steps 1 through 7 establish Step 8. More examples of this situation are given in Section 14.

When a step justified by symmetry depends on symmetric premises, these premises are referred to in the justification. An example of this situation is given in the proof of Theorem 14.5. Note that in the proof above of Theorem 10.1a it would not be valid to use symmetry to interchange A and B in any of the indented steps 2 through 6, since these steps depend on the premise $x \in A \cap B$, which is not symmetric in A and B (unless the assertion of the theorem is known in advance).

Symmetry can safely be used as an effort saving rule, where you can see the validity of the steps that you are not writing down. You will never need to use symmetry to do proofs. In fact, if the use of symmetry is too handy, it should be suspect. Being symmetric with a true statement does not, in itself, make a statement true.

Using the implicit definition rule can further shorten the proof. Step 2 gives the defining condition that is equivalent to the statement of Step 1. Rather than writing this and statement down as a step, we use it, implicitly, to get Steps 3 and 4. Similarly, Step 6 follows immediately from Steps 3 and 4, by the implicit use of the condition defining intersection.

Also, if we use the definition of $\subseteq$ implicitly as justification for Step 8, the $for\ all$ statement of Step 7 need not be written as a step. If we use the definition of set equality implicitly as justification for Step 11, the and statement of Step 10 need not be written as a step. Thus we have the following, shortened proof:

Proof of (a):

Assume: A,B sets

Show: $A \cap B = B \cap A$

	1. Let $x \in A \cap B$ be arbitrary	
	2. $x \in A$	(1; def. $\cap$, imp.)
	3. $x \in B$	(1; def. $\cap$, imp.)
	4. $x \in B \cap A$	(2, 3; def. $\cap$, imp.)
5.	$A \cap B \subseteq B \cap A$	(1—4; def. $\subseteq$, imp.)
6.	$B \cap A \subseteq A \cap B$	(1—5; sym. A & B)
7.	$A \cap B = B \cap A$	(5, 6; def. $=$, imp.)

□

Step 1, $x \in A \cap B$, means $x \in A\ and\ x \in B$ to us, since we know the definition of intersection. Therefore, to use $x \in A \cap B$ we use the implicit and statement, to infer Steps 2 and 3, but we think of this as using Step 1. Similarly, from Steps 2 and 3, we can infer the statement $x \in B\ and\ x \in A$, but we think of this as inferring Step 4, $x \in B \cap A$.

The rule for implicit use of definitions allows us not only to contract what we write down, but to contract our thought processes. Thus we ignore the obvious, and are better able to focus on more fruitful things. In the next section, we take up informal, narrative-style proofs where logic is implicit. The rules for proving and using and statements disappear when we write in paragraph style. The statement "$x \in A$ and $x \in B$" in a paragraph proof could correspond to either the one step "k. $x \in A\ and\ x \in B$" or to the two steps "k. $x \in A$" and "k+1. $x \in B$". Our formal rules for proving and using and make these two possibilities logically equivalent. While the and rules fade away, the effects of other rules, although no longer explicit, can still be detected as they provide a basis for the form of the logical arguments.

EXERCISE

1. Prove Theorem 10.1b. Use symmetry.

REVIEW EXERCISES

2. (a) 1. Assume $t \in C$

.

4. $t \in D$

5. _____ (1—4;_____)

(b) 1. _____

2. _____

3. $C = D$ (1, 2; def. $=$, imp.)

(c) 1. _____

2. $t \in X \cup Y$ (1; def. $\cup$, exp.)

(d) 1. $C = D$

2. _____ (1; def. $=$, imp.)

3. _____ (1; def. $=$, imp.)

(e) 1. _____

.

5. _____

6. $t \in X \cup Y$ (1—5; def. $\cup$, imp.)

(f) 1. $C = D$

2. _____ (1; def. $=$, exp.)

3. _____ (2; us. &)

4. _____ (2; us. &)

(g) 1. _____

2. _____

3. $t < 8$ *and* $t \in C$ (1, 2; pr. &)

(h) 1. $t \in C$ *and* $t \leq 8$

2. _____ (1; us. &)

Narrative Proofs

Proofs in the mathematical literature don't follow the step-by-step form that our proofs have taken so far. Instead, they are written in narrative form using ordinary sentences and paragraphs. The primary function of such narrative proofs is to serve as a communication between writer and reader, whereas the step-by-step proofs we have considered so far are primarily logical verifications.

In a narrative proof, the writer takes for granted a certain level of sophistication in the reader. Thus certain details can be left out, since it is presumed that the reader can easily supply them if they are needed. Generally, the higher the level of the mathematics, the more detail left out. Our rule for the implicit use of defining conditions produces proofs that are intermediate between narrative proofs and the step-by-step proofs with explicit logic. Logic is always implicit in narrative proofs.

We will illustrate the formulation of narrative proofs as abbreviations of step-by-step proofs with implicit logic.

Example 1:

Consider the shortened version of the proof of Theorem 10.1a that used the implicit definition rule.

Theorem 10.1 For sets A and B,
(a) $A \cap B = B \cap A$
(b) $A \cup B = B \cup A$

Proof of (a):

Assume: A, B sets

Show: $A \cap B = B \cap A$

	1. Let $x \in A \cap B$ be arbitrary	
	2. $x \in A$	(1; def. $\cap$, imp.)
	3. $x \in B$	(1; def. $\cap$, imp.)
	4. $x \in B \cap A$	(2, 3; def. $\cap$, imp.)
5.	$A \cap B \subseteq B \cap A$	(1—4; def. $\subseteq$, imp.)
6.	$B \cap A \subseteq A \cap B$	(1—5; sym. A & B)
7.	$A \cap B = B \cap A$	(5, 6; def. $=$, imp.)

□

A narrative proof begins with a sentence or two that cover the hypotheses and conclusion. This is merely good writing style: first you tell your reader what you are assuming, and then what you will show:

Proof of (a):

We assume that A and B are any sets, and will show that $A \cap B = B \cap A$.

Next, we relate the steps that take us to the conclusion:

Proof of (a):

We assume that A and B are any sets, and will show that $A \cap B = B \cap A$. Let $x \in A \cap B$ be arbitrary. Then $x \in A$ and $x \in B$ by the definition of $\cap$. From this we get $x \in B \cap A$. Therefore $A \cap B \subseteq B \cap A$ by the definition of $\subseteq$. $B \cap A \subseteq A \cap B$ follows by symmetry, and from the last two assertions we get $A \cap B = B \cap A$, by the definition of set equality.

□

In a narrative proof, it isn't necessary to cite the justification for every step taken. Omit the justification when you think it will be clear to the reader. Don't be too repetitive. You should always, however, cite the hypotheses where these are used in the proof. The hypotheses are there because the theorem isn't true without them. It is a good idea therefore, to show where the hypotheses are needed in the proof.

Example 2:

Rewrite the proof of Theorem 8.2 as a narrative proof.

Theorem 8.2 For sets A, B and C, if $A \subseteq B$ *or* $A \subseteq C$ then $A \subseteq B \cup C$.

Proof:

Assume: A,B,C sets
$A \subseteq B$ *or* $A \subseteq C$

Show: $A \subseteq B \cup C$

	1. Let $x \in A$ be arbitrary	
	2. Assume $x \notin B$	
	3. $A \subseteq B$ *or* $A \subseteq C$	(hyp.)
Case 1	4. Assume $A \subseteq B$	
	5. $x \in B$, # Step 2	(1, 4; def. $\subseteq$, imp.)
Case 2	6. Assume $A \subseteq C$	
	7. $x \in C$	(1, 6; def. $\subseteq$, imp.)
	8. $x \in C$	(3—7; us. *or*)
	9. $x \in B$ *or* $x \in C$	(2—8; pr. *or*)
	10. $x \in B \cup C$	(9; def. $\cup$, exp.)
	11. $for\ all\ x \in A : x \in B \cup C$	(1—10; pr. $\forall$)
	12. $A \subseteq B \cup C$	(11; def. $\subseteq$, exp.)

□

Narrative proof:

Assume that A, B, and C are sets and that $A \subseteq B$ or $A \subseteq C$. We will show that $A \subseteq B \cup C$.

We have used the informal, English word "or" in the hypotheses of the narrative proof instead of the formal "or". The basic logic statement forms—such as and, or, $for\,all$, $there\,exists$—are not used in narrative proofs. They are used exclusively in connection with the formal rules of inference, and these rules are used to guide the step-discovery procedure. In writing a narrative proof, you are, so to speak, to put both the formal mathematics and the logic in your own words. With some words such as or and $there\,exists$, the informal equivalents "or" and "there exists" are used in exactly the same way as the formal words. An informal "for all", on the other hand, is not used at all. Instead, people talk about the arbitrarily chosen element used to prove the implicit $for\,all$ statement. As we said at the end of the preceding section, the formal and and the rules for proving and using and statements fade from sight in a narrative proof.

Narrative proof:

Assume that A, B, and C are sets and that $A \subseteq B$ or $A \subseteq C$. We will show that $A \subseteq B \cup C$. Let $x \in A$ be arbitrary and assume $x \notin B$. By hypothesis, $A \subseteq B$ or $A \subseteq C$. In the first case, we get $x \in B$ by the definition of subset, since $x \in A$. This contradicts our assumption. In the second case, we get $x \in C$. Therefore $x \in B \cup C$. This shows that[4] $A \subseteq B \cup C$.

□

The exercises at the end of this section ask you to provide narrative proofs for proofs you have previously done for homework. In future sections, when you are asked to prove a theorem, it is suggested that you first write a step-by-step proof, and then put this into your own words as a narrative proof. The criterion for a narrative proof to be valid is that there is a step-by-step proof for which it is an abbreviation. That is, it must be possible to establish any claim in a narrative proof by a step-by-step verification.

EXERCISES

Using your proofs done for previous homework as a guide, write paragraph proofs for the following theorems. In places where one of your proofs used a definition explicitly, you will need to first abbreviate the proof to use the definition implicitly.

1. Theorem 9. 1 (a) and (b).

2. Theorem 9.2.

3. Theorem 8.1a

[4] It would be helpful if there were many synonyms for the word "therefore", which tends to want to be over used in narrative proofs. Sports headlines repeatedly inform us that team A beat team B, and the essence of sport headline writing would seem to be to come up with colorful synonyms for "beat". While no one wants to go to that extreme in writing mathematical proofs, a little variety would be good.

Using Theorems

Recall Theorem 9.1.

Theorem 9.1 For sets A and B:
(a) $A \cap B \subseteq A$
(b) $A \cap B \subseteq B$

Assuming that you had already proved part (a), a proof of part (b) could proceed (synthetically—not using the step-discovery procedure) along the following lines:

Proof of (b):

Assume: A, B sets

Show: $A \cap B \subseteq B$

1.	$A \cap B \subseteq A$	(part (a) already shown)
2.	$B \cap A \subseteq B$	(1; sym. A & B)

Step 2 was obtained from Step 1 by reversing the roles of A and B—by symmetry. Step 2 is almost the conclusion we want, except that in Step 2 we have $B \cap A$ where we want $A \cap B$ in the conclusion. Theorem 10.1a, however, states that these two are exactly the same:

Theorem 10.1 For sets A and B,
(a) $A \cap B = B \cap A$
(b) $A \cup B = B \cup A$

The meaning of the equation in Theorem 10.1a is that $A \cap B$ and $B \cap A$ are two different expressions for exactly the same set, or two different ways the same set can be arrived at. An equation in mathematics always asserts that the left hand side and the right hand side are expressions for the same mathematical thing (such as the same number, or the same set). Recall the inference rule for using substitution:

Inference Rule Substitution: Any name or expression for a mathematical object can be replaced by another name or expression for the same object. It is necessary to avoid using the same name for different objects.

The proof of Theorem 9.1b can be completed by quoting Theorem 10.1a and using substitution:

Proof of (b):

Assume: A, B sets

Show: $A \cap B \subseteq B$

1.	$A \cap B \subseteq A$	(part (a) already shown)
2.	$B \cap A \subseteq B$	(1; sym. A & B)
3.	$A \cap B = B \cap A$	(Theorem 10.1a: For sets A, B: $A \cap B = B \cap A$)
4.	$A \cap B \subseteq B$	(2, 3; sub.)

The inference rule that allows us to use theorems in proofs is the following:

Inference Rule Using Theorems (partial version): If the hypotheses of a theorem are true for variables in a proof, then the conclusion is true and can be written as a proof step.

There are no hypotheses for Theorem 10.1. The theorem is true for any sets A and B whatever. Thus the hypotheses are vacuously satisfied, so by our inference rule the conclusion is true. The conclusion has been written as Step 3 in the proof. The same inference rule allows us to write the conclusion of part (a) (presumably already proved) as Step 1 in the proof.

Rather than writing out the conclusion of Theorem 10.1a as a proof step (Step 3), it is better to apply the statement of the conclusion to existing steps—thus using substitution implicitly. Since $A \cap B = B \cap A$, we can substitute $A \cap B$ for $B \cap A$ directly in Step 2, to give us Step 3 below:

1.	$A \cap B \subseteq A$	(Theorem 9.1a)
2.	$B \cap A \subseteq B$	(1; sym. A & B)
3.	$A \cap B \subseteq B$	(2; Theorem 10.1a: For sets A, B: $A \cap B = B \cap A$)

We have used Theorem 10.1a to make a *change* in Step 2 (obtaining Step 3 from Step 2 by substitution), and thus have abbreviated the longer process of writing out the conclusion as a proof step and then substituting in the next step. In the three-step proof above substitution has been used implicitly. Here is the final version of our inference rule:

Inference Rule Using Theorems: If the hypotheses of a theorem (or axiom) are true for variables in a proof, then the conclusion is true and can be written as a proof step, or applied, by substitution, to make changes in a proof step.

We can apply Theorem 10.1a to the sets we are working with in our new proof of Theorem 9.1b, since Theorem 10.1a is true for all sets A and B—including the sets A and B we're working with. Technically, we shouldn't use A and B to describe Theorem 10.1a, since A and B are already in use. They have been identified in the hypothesis of Theorem 9.1b, and are now fixed for the duration of the proof. They are constants, as far as the proof is concerned, so we should use different letters to describe Theorem 10.1a—as in the following:

1. $A \cap B \subseteq A$ (Theorem 9.1a)
2. $B \cap A \subseteq B$ (1; sym. A & B)
3. $A \cap B \subseteq B$ (2; Theorem 10.1a: For sets X, Y: $X \cap Y = Y \cap X$)

The situation is the same for Theorems (which are expressed informally) as it is for the formal $for\,all$ statements, where we can't use a variable already in use. Usually, even if the variables in the theorem being used are the same as the variables in the theorem being proved, the variables play different roles—so that changing to completely different variables can prevent confusion.

Axioms are informal mathematical statements that have exactly the same form as theorems. The only difference between a theorem and an axiom is that axioms are assumed true, and theorems need to be proven. Axioms and theorems are used in the same way in proofs. Recall the axiom that states the transitivity of the relation $<$:

Axiom Transitivity of $<$: For $a, b, c \in \mathbb{N}$, if $a < b$ and $b < c$, then $a < c$.

This axiom has the following hypotheses and conclusion:

Hypotheses: a, b, c natural numbers
1. $a < b$
2. $b < c$

Conclusion: $a < c$

The axiom was used in the proof in Example 2 of Section 4:

Example 3:

Define $H = \{x \in \mathbb{N} \mid x < 10\}$ and $G = \{x \in \mathbb{N} \mid x < 20\}$. Prove that $H \subseteq G$.

Proof:

Assume: $H = \{x \in \mathbb{N} \mid x < 10\}$
$G = \{x \in \mathbb{N} \mid x < 20\}$

Show: $H \subseteq G$

1. Let $x \in H$ be arbitrary.
2. $x < 10$ (1; def. H)
3. $10 < 20$ (given)
4. $x < 20$ (2, 3; Trans. $<$)
5. $x \in G$ (4; def. G)
6. $for\,all\ x \in H : x \in G$ (1—5; pr. $\forall$)
7. $H \subseteq G$ (6; def. $\subseteq$)

□

The variable x in the proof is defined in Step 1. We don't know what value x has, but it has some value that is fixed for the steps 1 through 4. If we assign the value of x to the variable a in the axiom, and if we assign 10 to b, then the hypothesis $a < b$ becomes $x < 10$. This statement is

true by Step 2 of the proof. If we assign 20 to c, the hypothesis $b < c$ becomes $10 < 20$. This statement is true, as Step 3 of the proof asserts. Thus both hypotheses of the axiom are true, so that we may infer that the conclusion is true and can be written as a proof step—by the inference rule for using theorems (or axioms). The conclusion, $a < c$, in the variables of the proof is $x < 20$, which is written as Step 4.

Theoretically, it isn't necessary to use theorems to do proofs—in any place where some theorem might be useful, one could "merely" put in all the steps needed to prove the theorem. Thus the use of theorems in proofs can be viewed as proof abbreviation. The point is that proofs that follow from definitions are more basic than proofs that use theorems.

EXERCISES

1. (a)
   1. $A \subseteq B \cup C$
   2. _____ (1; Theorem: For sets X, Y: $X \cup Y = Y \cup X$)

   (b)
   1. $A \subseteq B \cup C$
   2. $B \cup C \subseteq D$
   3. _____ (1,2; Theorem 5.1: For sets X, Y, Z: if $X \subseteq Y$ and $Y \subseteq Z$, then $X \subseteq Z$)

   (Note that the variables in which Theorem 5.1 is expressed on page 0 are A, B, and C, but these don't play the same role as the A, B, and C of the theorem.

2. Let A, B, and C be sets. Prove in two ways that if $A \subseteq B \cap C$, then $A \subseteq B$: (1) directly from definitions, without using theorems to justify proof steps, and (2) using Theorems 5.1 and 9.1.

Axioms for Addition and Multiplication

In mathematics, everything is just what its definition says it is. A proof that something has some property is a demonstration that the property follows logically from the definition. Not everything can be defined in terms of previously defined things, of course. There must be some undefined things that can be used as a starting point. Since the properties of these undefined things can't be shown by definition, we must assume these properties—which are called axioms.

The set $\mathbb{N} = \{1, 2, 3, 4, ...\}$ of natural numbers has been considered as a source for examples of sets. We assumed, as an axiom, that there was a relation $<$ on $\mathbb{N}$ that satisfied the transitive property. We are now going to dig a little deeper, and will assume, instead, that there are the two operations of addition and multiplication on $\mathbb{N}$. The relation $<$ will be defined later, and the transitive property will be proved as a theorem. Addition and multiplication are not defined, but are assumed to have axiomatic properties. The first axioms are the following:

Axiom Closure under addition: If $a, b \in \mathbb{N}$, then $a + b \in \mathbb{N}$.

Axiom Commutativity of addition: If $a, b \in \mathbb{N}$, then $a + b = b + a$.

Axiom Associativity of addition: If $a, b, c \in \mathbb{N}$, then $a + (b + c) = (a + b) + c$.

Axiom Closure under multiplication: If $a, b \in \mathbb{N}$, then $a \cdot b \in \mathbb{N}$.

Axiom Commutativity of multiplication: If $a, b \in \mathbb{N}$, then $a \cdot b = b \cdot a$.

Axiom Associativity of multiplication: If $a, b, c \in \mathbb{N}$, then $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Axiom Distributivity: If $a, b, c \in \mathbb{N}$, then $a \cdot (b + c) = a \cdot b + a \cdot c$.

Example 1:

Suppose $x \in \mathbb{N}$ and we have Step 1 below. Then Steps 2 and 3 follow.

1. $x + 10 = 32$
2. $x + 10 = 10 + x$ (Axiom: If $a, b \in \mathbb{N}$, then $a + b = b + a$)
3. $10 + x = 32$ (1,2; substitution)

The reasoning behind Example 1 is as follows: The equation in Step 1 means that $x + 10$ and 32 are two different expressions or names for exactly the same natural number. The axiom on commutativity states that if a and b are natural numbers, then $a + b = b + a$. Since $a + b = b + a$ is true for all natural numbers a and b, it is true for x and 10. Thus $x + 10 = 10 + x$. The equal sign here means that $x + 10$ and $10 + x$ are two different names for the same natural number. Step 3 comes from Step 1 by substituting $10 + x$ for $x + 10$—these being equal by Step 2.

Step 2 follows from our rule for using theorems—which also applies to using axioms. The rule states that if the hypotheses of the theorem (or axiom) hold for some variables in a proof, then the conclusion is true and can be written as a proof step, or applied by substitution to change existing proof steps. The hypotheses and conclusion of the axiom are:

Hypotheses: a, b natural numbers

Conclusion: $a + b = b + a$

Rather than writing out the commutative property itself as a proof step (as in Step 2), it is better to apply the property to existing steps (thus using substitution implicitly). Example 2 below does just this, in contracting the steps of Example 1.

Example 2:

Suppose $x \in \mathbb{N}$ and we have Step 1 below. Then Step 2 follows.

1. $x + 10 = 32$
2. $10 + x = 32$ (1; Axiom: For $a, b \in \mathbb{N},\ a + b = b + a$)

Thus we will almost always use the axioms above as reasons for making *changes to* steps in a proof—as in Example 2.

Example 3:

1. $x + 5 = a \cdot 7 + a \cdot 3$
2. _____ (1; Ax.: For $a, b, c \in \mathbb{N}$, $a \cdot (b + c) = a \cdot b + a \cdot c$)

Solution:

1. $x + 5 = a \cdot 7 + a \cdot 3$
2. $x + 5 = a \cdot (7 + 3)$ (1; Ax.: For $a, b, c \in \mathbb{N}$, $a \cdot (b + c) = a \cdot b + a \cdot c$)

Instead of writing out an axiom used as justification for a proof step, we may use the name of the property as an abbreviation. Using this abbreviation in Example 3 gives:

Example 3:

1. $x + 5 = a \cdot 7 + a \cdot 3$
2. $x + 5 = a \cdot (7 + 3)$ (1; Ax.: distributivity)

Example 4 below illustrates a form for exercises in this section.

Example 4:

In the exercise below, fill in Step 2 by making a change to Step 1 using the axiom indicated. Then get the same result the long way: (1) write the formal statement in the axiom, (2) assign the variables a, b, and c to variables in the steps, (3) write the formal statement in the axiom (with the variables in the proof) as Step $1\frac{1}{2}$, and (4) use substitution to get Step 2.

1. $x + y = 12 + (x + z)$
2. _____ (1; Ax.: Associativity of $+$)

formal statement: _____

assign variables in the axiom to variables in the steps:

$a =$ ____
$b =$ ____
$c =$ ____

1.	$x + y = 12 + (x + z)$	
$1\frac{1}{2}$.	_____	(Ax.: Associativity of $+$)
2.	_____	(1,1 $\frac{1}{2}$; sub.)

Solution:

1.	$x + y = 12 + (x + z)$	
2.	$x + y = (12 + x) + z$	(1; Ax.: Associativity of $+$)

formal statement: $a + (b + c) = (a + b) + c$
assign variables in the axiom to variables in the steps:

$a = 12$
$b = x$
$c = z$

1.	$x + y = 12 + (x + z)$	
$1\frac{1}{2}$.	$12 + (x + z) = (12 + x) + z$	(Ax.: Associativity of $+$)
2.	$x + y = (12 + x) + z$	(1,1$\frac{1}{2}$; sub.)

Example 4 illustrates two ways to think about using an axiom in proof steps: (1) implicitly, to make a change in a proof step, and (2) by writing the axiom itself explicitly as a proof step, and then using substitution—again, explicitly. It is almost always much clearer in mathematics to use substitution implicitly—taking a kind of mathematical shortcut. In future sections, we always use substitution implicitly when using one of the axioms above.

The axioms above for the natural numbers are all given informally, in terms of statements that have hypotheses and conclusions. They are applied to proof steps with our rule for using theorems or axioms. It is possible to give these axioms formally in terms of $for\,all$ statements involving two or three variables:

Axiom Closure under addition: $For\,all\ a, b \in \mathbb{N}:\ a + b \in \mathbb{N}$.

Axiom Commutativity of addition: $For\,all\ a, b \in \mathbb{N}:\ a + b = b + a$.

Axiom Associativity of addition: $For\,all\ a, b, c \in \mathbb{N}:\ a + (b + c) = (a + b) + c$.

Axiom Closure under multiplication: $For\,all\ a, b \in \mathbb{N}:\ a \cdot b \in \mathbb{N}$.

Axiom Commutativity of multiplication: $For\,all\ a, b \in \mathbb{N}:\ a \cdot b = b \cdot a$.

Axiom Associativity of multiplication: $For\,all\ a, b, c \in \mathbb{N}:\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Axiom Distributivity: $For\,all\ a, b, c \in \mathbb{N}:\ a \cdot (b + c) = a \cdot b + a \cdot c$.

The rules for using and proving $for\,all$ statements are extended to apply to more than one variable. For example, the following are the formats for proving and using $for\,all$ statements with two variables:

pr. $\forall$

1. Let $x \in A$ and $y \in B$ be arbitrary

k-1. $\mathcal{P}(x, y)$

k. $for\,all\, x \in A, y \in B : \mathcal{P}(x, y)$ (1—k-1; pr. $\forall$)

us. $\forall$

1. $for\,all\, x \in A,\ y \in B : \mathcal{P}(x, y)$
2. $t \in A$
3. $s \in B$
4. $\mathcal{P}(t, s)$ (1, 2, 3; us. $\forall$)

We won't proceed in this direction of formalizing things we can handle informally. In fact, we will always maintain our trend from the formal to the informal. Formality is used only to make things explicit. After things have been made explicit and understood, we proceed to informal, abbreviated expressions of the same ideas.

There is one thing that can be learned from the formal expression of the axioms, however. Recall, for example, that the variable x in the statement $for\,all\, x \in A : x \in B$ is called a *local variable*. The statement $for\,all\, x \in A : x \in B$ is not about x. It is about the sets A and B. In fact it is the defining condition for the relation $A \subseteq B$. From the statement $for\,all\, x \in A : x \in B$, we don't learn anything about x. We learn something about the sets A and B.

In the same way, the statement $for\,all\, a, b \in \mathbb{N} : a + b = b + a$ is not about the letters a and b. They are local variables. $For\,all\, a, b \in \mathbb{N} : a + b = b + a$ is a statement about the operation $+$ on the set $\mathbb{N}$. That is why the axiom is named the "commutativity of addition". Thus all the axioms are statements about the operations of addition and multiplication on the set of natural numbers—not about natural numbers themselves. This is true whether the axioms are given formally or informally.

EXERCISES

In the exercises below, fill in Step 2 by making a change to Step 1 using the axiom indicated. Then get the same result the long way: (1) write the formal statement in the axiom, (2) assign the variables a, b, (and perhaps c) to variables or constants (numbers) in the steps, (3) write the formal statement part of the axiom (with the variables in the proof) as Step $1\frac{1}{2}$, and (4) use substitution to get Step 2.

1.

1. $x + 9 = 12$
2. _____ (1; Ax.: Commutativity of $+$)

formal statement: _____
assign variables in the axiom to variables or constants in the steps:

$a =$ ____
$b =$ ____

1. $x + 9 = 12$
$1\frac{1}{2}$. _____ (Ax.: Commutativity of $+$)
2. _____ (1,$1\frac{1}{2}$; sub.)

2.

1. $x \cdot y = 12 \cdot (x \cdot z)$
2. _____ (1; Ax.: Associativity of $\cdot$)

formal statement: _____
assign variables in the axiom to variables or constants in the steps:

$a =$ ____
$b =$ ____
$c =$ ____

1. $x \cdot y = 12 \cdot (x \cdot z)$
$1\frac{1}{2}$. _____ (Ax.: Associativity of $\cdot$)
2. _____ (1,$1\frac{1}{2}$; sub.)

3.

1. $3 \cdot x = 2 \cdot (x + 10)$
2. _____ (1; Ax.: Distributivity)

formal statement: _____
assign variables in the axiom to variables or constants in the steps:

$a =$ ____
$b =$ ____
$c =$ ____

1. $3 \cdot x = 2 \cdot (x + 10)$
$1\frac{1}{2}$. _____ (Ax.: Distributivity)
2. _____ (1,$1\frac{1}{2}$; sub.)

4.

1. $x \cdot y = y + 10$
2. _____ (1; Ax.: Commutativity of $\cdot$)

formal statement: _____
assign variables in the axiom to variables or constants in the steps:

$a =$ ____
$b =$ ____

1. $x \cdot y = y + 10$
$1\frac{1}{2}$. _____ (Ax.: Commutativity of $\cdot$)
2. _____ (1,$1\frac{1}{2}$; sub.)

5.

1. $x \cdot y = y + 10$
2. _____ (1; Ax.: Commutativity of $+$)

formal statement: _____
assign variables in the axiom to variables or constants in the steps:

$a =$ ____
$b =$ ____

1. $x \cdot y = y + 10$
$1\frac{1}{2}$. _____ (Ax.: Commutativity of $+$)
2. _____ (1,$1\frac{1}{2}$; sub.)

6.

1. $(3 \cdot x + 12) + 25 = 1$
2. _____ (1; Ax.: Associativity of $+$)

formal statement: _____
assign variables in the axiom to variables or constants in the steps:

$a =$ ____
$b =$ ____
$c =$ ____

1. $(3 \cdot x + 12) + 25 = 1$
$1\frac{1}{2}$. _____ (Ax.: Associativity of $+$)
2. _____ (1,$1\frac{1}{2}$; sub.)

7. In the following problem provide the indicated justification:

1. $x + y = 42$
2. $y + x = 42$ (1; _____)

Implications; Equivalence

For statements $\mathcal{P}$ and $\mathcal{Q}$, the formal statement $if\ \mathcal{P}, then\ \mathcal{Q}$ is called an *implication* or if-$then$ statement . It is the next basic type we want to consider. For example, $if\ x \in A, then\ x < 7$ and $if\ A = B \cap C, then\ A \subseteq D$ are such if-$then$ statements. Informally, the statement $if\ \mathcal{P}, then\ \mathcal{Q}$ means that $\mathcal{Q}$ is true whenever $\mathcal{P}$ is true; that is, if $\mathcal{P}$ is true, then $\mathcal{Q}$ is also true.

The statement $\mathcal{P}$ in the implication $if\ \mathcal{P}, then\ \mathcal{Q}$ is called the *hypothesis* of the formal implication, and $\mathcal{Q}$ is called the *conclusion*. Our informal statements of theorems that have had hypotheses-conclusion interpretations have been proved by assuming the hypotheses to be true and showing the conclusion is therefore true. The same thing is done formally, in order to prove formal implications:

Inference Rule Proving if-$then$ statements: In order to prove the statement $if\ \mathcal{P}, then\ \mathcal{Q}$, assume $\mathcal{P}$ and show $\mathcal{Q}$. Abbreviation: "pr. $\Rightarrow$ ".

Format:

pr. $\Rightarrow$

1. Assume $\mathcal{P}$

k-1. $\mathcal{Q}$

k. $if\ \mathcal{P}, then\ \mathcal{Q}$ (1—k-1; pr. $\Rightarrow$)

Example 1:

1. _____

.

4. _____

5. $if\ x < 10, then\ x \in A$ (1—4; pr. $\Rightarrow$)

Solution:

1. Assume $x < 10$

.

4. $x \in A$

5. $if\ x < 10, then\ x \in A$ (1—4; pr. $\Rightarrow$)

Example 2:

1. _____

.

4. _____

5. $if\ x \in C, then\ x \in D$ (1—4; pr. $\Rightarrow$)

Solution:

1. Assume $x \in C$

.

4. $x \in D$

5. $if\ x \in C, then\ x \in D$ (1—4; pr. $\Rightarrow$)

Example 3:

1. _____

.

4. _____

5. $for\ all\ x \in C : x \in D$ (1—4; pr. $\forall$)

Solution:

1. Let $x \in C$ be arbitrary

.

4. $x \in D$

5. $for\ all\ x \in C : x \in D$ (1—4; pr. $\forall$)

In Step 1 of Example 2, we make an assumption about x, which would have had to have been already defined (say, in the hypotheses). In Step 1 of Example 3, we define the x, in order to prove the $for\ all$ statement of Step 5.

Example 4:

1. Assume $t \in$ P

.

4. $t \in$ Q

5. _____ (1—4; _____)

Solution:

1. Assume $t \in$ P

.

4. $t \in$ Q

5. $if\ t \in$ P, $then\ t \in$ Q (1—4; pr. $\Rightarrow$)

Example 5:

1. Let $t \in$ P be arbitrary

.

4. $t \in$ Q

5. _____ (1—4; _____)

Solution:

1. Let $t \in$ P be arbitrary

.

4. $t \in$ Q

5. $for\ all\ t \in$ P: $t \in$ Q (1—4; pr. $\forall$)

Our rule for using theorems in proofs states that if the hypotheses of a proven theorem have been shown to be true in the proof steps, then the conclusion is true and can be written as a proof step. The rule for using formal if-$then$ statements is analogous:

Inference Rule Using if-$then$ statements: If both $\mathcal{P}$ and $if\ \mathcal{P}, then\ \mathcal{Q}$ are established, then we may infer $\mathcal{Q}$. Abbreviation: "us. $\Rightarrow$ "

Format:

us. $\Rightarrow$

i. $if\ \mathcal{P}, then\ \mathcal{Q}$

j. $\mathcal{P}$

k. $\mathcal{Q}$ (i, j; us. $\Rightarrow$)

Example 6:

3. $a < 10$

.

5. $if\ a < 10, then\ a \in C$

6. _____ (3, 5; us. $\Rightarrow$)

Solution:

3. $a < 10$

.

5. $if\ a < 10, then\ a \in C$

6. $a \in C$ (3, 5; us. $\Rightarrow$)

Example 7:

2. $x \leq 5$

.

5. _____

6. $y \leq 5$ (3, 5; us. $\Rightarrow$)

Solution:

2. $x \leq 5$

.

5. $if\ x \leq 5, then\ y \leq 5$

6. $y \leq 5$ (3, 5; us. $\Rightarrow$)

The following theorem involves the equivalence of a formal if-$then$ statement and a formal *or* statement:

Theorem 14.1 The statement $\mathcal{P}\ or\ \mathcal{Q}$ is logically equivalent to $if\ \neg\mathcal{P}, then\ \mathcal{Q}$.

The rule for *using* equivalence, that a statement can be substituted for an equivalent one, has allowed us to make use of axioms involving equivalence, and has allowed us to infer a relationship from its defining condition, and vice versa. We now get to the rule for *proving* statements equivalent—which is needed to prove the theorem.

Inference Rule Proving equivalence: In order to prove that statements $\mathcal{P}$ and $\mathcal{Q}$ are equivalent, first assume $\mathcal{P}$ and show $\mathcal{Q}$, then assume $\mathcal{Q}$ and show $\mathcal{P}$ (or, the other way around). Abbreviation: "pr. eq."

If a proof that two statements are equivalent depends only on definitions, inference rules, and logical axioms, but no axioms of a particular mathematical system such as the natural numbers, we say that the two statements are "logically" equivalent.

An assertion, such as Theorem 14.1, that two statements are equivalent does not lend itself to interpretation by our informal hypotheses-conclusion model. In order to prove the assertion that the two statements $\mathcal{P}$ and $\mathcal{Q}$ are equivalent, there are two things to do: we need first to assume $\mathcal{P}$ and show $\mathcal{Q}$, and then to assume $\mathcal{Q}$ and show $\mathcal{P}$. Thus each of the two parts of the proof is interpreted by the hypotheses-conclusion model. We now add, to the hypotheses-conclusion format we have been using, a format for proving such two-part assertions. We introduce each part by a sentence that indicates hypotheses and conclusion, and conclude with a statement that the assertion follows since the two required parts have been shown.

The proof of Theorem 14.1 is written according to this new format. Notice that the first sentence identifies $if\ \neg\mathcal{P}, then\ \mathcal{Q}$ as the hypothesis, and $\mathcal{P}\ or\ \mathcal{Q}$ as the conclusion, for the first part of the proof. The assumption in Step 1 is dictated by the rule for proving *or* statements, used to justify Step 3.

Proof:

We first assume $if\ \neg\mathcal{P}, then\ \mathcal{Q}$ and show $\mathcal{P}\ or\ \mathcal{Q}$.

1. Assume $\neg\mathcal{P}$
2. $\mathcal{Q}$ (hyp., 1; us. $\Rightarrow$)

3. $\mathcal{P}\ or\ \mathcal{Q}$ (1—2; pr. *or*)

We now assume $\mathcal{P}$ *or* $\mathcal{Q}$ and show $if\ \neg\mathcal{P}, then\ \mathcal{Q}$.

1. Assume $\neg\mathcal{P}$
2. $\mathcal{P}$ *or* $\mathcal{Q}$ (hyp.)
5. $\mathcal{Q}$ (1, 2; us. *or*, EZ)

6. $if\ \neg\mathcal{P}, then\ \mathcal{Q}$ (1—5; pr. $\Rightarrow$)

By the two parts above, $\mathcal{P}$ *or* $\mathcal{Q}$ and $if\ \neg\mathcal{P}, then\ \mathcal{Q}$ are equivalent.

□

Note that steps are renumbered in each part of the proof.

Example 1:

1. Assume $\neg\mathcal{P}$

.

3. $\mathcal{Q}$

4. $if\ \neg\mathcal{P}, then\ \mathcal{Q}$ (1—3; pr. $\Rightarrow$)

Example 2:

1. Assume $\neg\mathcal{P}$

.

3. $\mathcal{Q}$

4. $\mathcal{P}$ *or* $\mathcal{Q}$ (1—3; pr. *or*)

In Examples 1 and 2, exactly the same steps (1 through 3) can establish either $if\ \neg\mathcal{P}, then\ \mathcal{Q}$ or $\mathcal{P}$ *or* $\mathcal{Q}$. This is reasonable, since the two statements are logically equivalent.

A proposition that follows readily from a theorem is called a *corollary* to the theorem. The next proposition is a corollary to Theorem 14.1.

Corollary 14.2 The statement $if\ \mathcal{P}, then\ \mathcal{Q}$ is logically equivalent to $\neg\mathcal{P}$ *or* $\mathcal{Q}$.

Proof: Exercise 2.

Theorem 14.3 The statements $\mathcal{P}$ *or* $\mathcal{Q}$ and $\mathcal{Q}$ *or* $\mathcal{P}$ are logically equivalent.

Proof:

We first assume $\mathcal{P}$ *or* $\mathcal{Q}$ and show $\mathcal{Q}$ *or* $\mathcal{P}$.

1. Assume $\neg\mathcal{P}$
2. $if\ \neg\mathcal{P}, then\ \mathcal{Q}$ (hyp.; Thm. 14.1: $\mathcal{P}$ *or* $\mathcal{Q}\ \Leftrightarrow\ if\ \neg\mathcal{P}, then\ \mathcal{Q}$).
3. $\mathcal{Q}$ (1,2; us. $\Rightarrow$)

4. $\mathcal{Q}$ *or* $\mathcal{P}$ (1—3; pr. *or*)

If we assume $\mathcal{Q}$ *or* $\mathcal{P}$, we show $\mathcal{P}$ *or* $\mathcal{Q}$ by an argument symmetric (in $\mathcal{P}$ and $\mathcal{Q}$) to the first part of the proof. Thus $\mathcal{P}$ *or* $\mathcal{Q}$ is equivalent to $\mathcal{Q}$ *or* $\mathcal{P}$.

□

Theorem 14.4 The statements $\mathcal{P}\ and\ \mathcal{Q}$ and $\mathcal{Q}\ and\ \mathcal{P}$ are logically equivalent.

Proof: Exercise 3.

The rule for using equivalence is used in the following examples.

Example 3:

1. $x \in C\ or\ x \in D$
2. $x \in C\ or\ x \in D$ is equivalent to $if\ x \notin C, then\ x \in D$ (Thm. 14.1: $\mathcal{P}\ or\ \mathcal{Q} \Leftrightarrow if\ \neg\mathcal{P}, then\ \mathcal{Q}$)
3. _____ (1, 2: us. eq.)

Solution:

1. $x \in C\ or\ x \in D$
2. $x \in C\ or\ x \in D$ is equivalent to $if\ x \notin C, then\ x \in D$ (Thm. 14.1: $\mathcal{P}\ or\ \mathcal{Q} \Leftrightarrow if\ \neg\mathcal{P}, then\ \mathcal{Q}$)
3. $if\ x \notin C, then\ x \in D$ (1, 2: us. eq.)

In example 3, first the assertion of Theorem 14.1 is given in Step 2, with $x \in C$ being $\mathcal{P}$, and $x \in D$ being $\mathcal{Q}$. (The symbol " $\Leftrightarrow$ " stands for equivalence in justifications.) Then Step 3 is obtained by replacing the statement of Step 1 with the equivalent statement, according to the rule for using equivalence.

We will not use the rule for using equivalence explicitly as in Example 3. Instead, the rule will be used implicitly to make a change, exactly as the substitution rule of inference has been used. Examples 3a through 5 show how this will be done.

Example 3a:

1. $x \in C\ or\ x \in D$
2. _____ (1; Thm. 14.1: $\mathcal{P}\ or\ \mathcal{Q}\ \Leftrightarrow\ if\ \neg\mathcal{P}, then\ \mathcal{Q}$)

Solution:

1. $x \in C\ or\ x \in D$
2. $if\ x \notin C, then\ x \in D$ (1; Thm. 14.1: $\mathcal{P}\ or\ \mathcal{Q}\ \Leftrightarrow\ if\ \neg\mathcal{P}, then\ \mathcal{Q}$)

Example 4:

1. $if\ x \in C, then\ x \in D$
2. _____ (1; Thm. 14.1: $\mathcal{P}\ or\ \mathcal{Q}\ \Leftrightarrow\ if\ \neg\mathcal{P}, then\ \mathcal{Q}$)

Solution:

1. $if\ x \in C, then\ x \in D$
2. $x \notin C\ or\ x \in D$ (1; Thm. 14.1: $\mathcal{P}\ or\ \mathcal{Q}\ \Leftrightarrow\ if\ \neg\mathcal{P}, then\ \mathcal{Q}$)

Example 5:

1. $for\ all\ x \in A : (x \in B\ or\ x < 9)$
2. _____ (1; Thm. 14.1: $\mathcal{P}\ or\ \mathcal{Q}\ \Leftrightarrow if\ \neg\mathcal{P}, then\ \mathcal{Q}$)

Solution:

1. $for\ all\ x \in A : (x \in B\ or\ x < 9)$
2. $for\ all\ x \in A : if\ x \notin B, then\ x < 9$ (1; Thm. 14.1: $\mathcal{P}\ or\ \mathcal{Q} \Leftrightarrow if\ \neg\mathcal{P}, then\ \mathcal{Q}$)

Theorem 14.4 can be used to write another proof of Theorem 10.1a:

Theorem 10.1 For sets A and B,
(a) $A \cap B = B \cap A$
(b) $A \cup B = B \cup A$

Proof of (b): Exercise 4.

Proof of (a):

We assume A and B are sets, and show $A \cap B = B \cap A$.

k. $A \cap B = B \cap A$ (; def. $=$, imp.)

The step-discovery procedure dictates Steps j and k-1:

Proof of (a):

We assume A and B are sets, and show $A \cap B = B \cap A$.

.
j. $A \cap B \subseteq B \cap A$
.
k-1. $B \cap A \subseteq A \cap B$
k. $A \cap B = B \cap A$ (j, k-1; def. $=$, imp.)

Analyzing Step j gives Steps 1 and j-1:

1. Let $x \in A \cap B$ be arbitrary
.
j-1. $x \in B \cap A$
j. $A \cap B \subseteq B \cap A$ (1—j-1; def. $\subseteq$, imp.)
.
k-1. $B \cap A \subseteq A \cap B$
k. $A \cap B = B \cap A$ (j, k-1; def. $=$, imp.)

Using the definition of $\cap$ (explicitly) gives us Steps 2 and j-2:

1. Let $x \in A \cap B$ be arbitrary
2. $x \in A\ and\ x \in B$ (1; def. $\cap$, imp.)

.
j-2. $x \in B \text{ and } x \in A$
j-1. $x \in B \cap A$ (j-2; def. $\cap$, imp.)
j. $A \cap B \subseteq B \cap A$ (1—j-1; def. $\subseteq$, imp.)
.
k-1. $B \cap A \subseteq A \cap B$
k. $A \cap B = B \cap A$ (j, k-1; def. $=$, imp.)

Step j-2 follows immediately from Step 2, by Theorem 14.4. We have a complete proof:

Proof of (a):
We assume A and B are sets, and show $A \cap B = B \cap A$.
1. Let $x \in A \cap B$ be arbitrary
2. $x \in A \text{ and } x \in B$ (1; def. $\cap$, imp.)
3. $x \in B \text{ and } x \in A$ (2; Thm. 14.4: $\mathcal{P} \text{ and } \mathcal{Q} \Leftrightarrow \mathcal{Q} \text{ and } \mathcal{P}$)
4. $x \in B \cap A$ (3; def. $\cap$, imp.)
5. $A \cap B \subseteq B \cap A$ (1—4; def. $\subseteq$, imp.)
6. $B \cap A \subseteq A \cap B$ (1—5: sym. A & B)
7. $A \cap B = B \cap A$ (5, 6; def. $=$, imp.)

□

The use of explicit definitions and theorems on logical equivalence makes proofs look more like logic exercises than mathematics. The proof above is no shorter than the proof in Section 10, and it does suffer from looking a little more like a logic exercise. However, it is certainly valid, and in some cases using theorems on logical equivalence can shorten a proof.

The next theorem is a technical necessity—which we now get out of the way.

Theorem 14.5 The statements $(\mathcal{P} \text{ or } \mathcal{Q}) \text{ or } \mathcal{R}$ and $\mathcal{P} \text{ or } (\mathcal{Q} \text{ or } \mathcal{R})$ are logically equivalent.

Proof:
First assume $(\mathcal{P} \text{ or } \mathcal{Q}) \text{ or } \mathcal{R}$ and show $\mathcal{P} \text{ or } (\mathcal{Q} \text{ or } \mathcal{R})$.
1. Assume $\neg\mathcal{P}$
.
j-1. $\mathcal{Q} \text{ or } \mathcal{R}$
j. $\mathcal{P} \text{ or } (\mathcal{Q} \text{ or } \mathcal{R})$ (1—j-1; pr. *or*)

Working back from Step j, the conclusion, we have the steps above. Now, working back from Step j-1 gives:

Proof:
First assume $(\mathcal{P}\ or\ \mathcal{Q})\ or\ \mathcal{R}$ and show $\mathcal{P}\ or\ (\mathcal{Q}\ or\ \mathcal{R})$.

1. Assume $\neg\mathcal{P}$
    2. Assume $\neg\mathcal{Q}$
    .
    j-2. $\mathcal{R}$
j-1. $\mathcal{Q}\ or\ \mathcal{R}$ (2—j-2; pr. *or*)
j. $\mathcal{P}\ or\ (\mathcal{Q}\ or\ \mathcal{R})$ (1—j-1; pr. *or*)

Since we get no more steps from analyzing the conclusion, it is time to use the hypothesis.

1. Assume $\neg\mathcal{P}$
    2. Assume $\neg\mathcal{Q}$
    3. $(\mathcal{P}\ or\ \mathcal{Q})\ or\ \mathcal{R}$ (hyp.)
Case 1 4. Assume $(\mathcal{P}\ or\ \mathcal{Q})$
    .
    j-4. $\mathcal{R}$
Case 2 j-3. Assume $\mathcal{R}$
    j-2. $\mathcal{R}$ (3—j-3; us. *or*)
j-1. $\mathcal{Q}\ or\ \mathcal{R}$ (2—j-2; pr. *or*)
j. $\mathcal{P}\ or\ (\mathcal{Q}\ or\ \mathcal{R})$ (1—j-1; pr. *or*)

The steps above are dictated, since we want to use Step 3 to get Step j-2. In order to use Step 4, we need more cases:

1. Assume $\neg\mathcal{P}$
    2. Assume $\neg\mathcal{Q}$
    3. $(\mathcal{P}\ or\ \mathcal{Q})\ or\ \mathcal{R}$ (hyp.)
Case 1 4. Assume $(\mathcal{P}\ or\ \mathcal{Q})$
    Case 1a 5. Assume $\mathcal{P}$ # Step 1
    Case 1b 6. Assume $\mathcal{Q}$ # Step 2
Case 2 7. Assume $\mathcal{R}$
    8. $\mathcal{R}$ (3—7; us. *or*)
9. $\mathcal{Q}\ or\ \mathcal{R}$ (2—8; pr. *or*)
10. $\mathcal{P}\ or\ (\mathcal{Q}\ or\ \mathcal{R})$ (1—9; pr. *or*)

Since Case 1a and 1b are both contradictions, Case 1 itself leads to a contradiction. Thus we get $\mathcal{R}$ from Case 2, as needed. This establishes the first part of the proof. In order to establish the second part, we seek to use symmetry.

Proof:

First assume $(\mathcal{P}\ or\ \mathcal{Q})\ or\ \mathcal{R}$ and show $\mathcal{P}\ or\ (\mathcal{Q}\ or\ \mathcal{R})$.

1. Assume $\neg\mathcal{P}$
   2. Assume $\neg\mathcal{Q}$
   3. $(\mathcal{P}\ or\ \mathcal{Q})\ or\ \mathcal{R}$ (hyp.)

Case 1 4. Assume $(\mathcal{P}\ or\ \mathcal{Q})$

Case 1a 5. Assume $\mathcal{P}$ # Step 1

Case 1b 6. Assume $\mathcal{Q}$ # Step 2

Case 2 7. Assume $\mathcal{R}$

8. $\mathcal{R}$ (3—7; us. *or*)

9. $\mathcal{Q}\ or\ \mathcal{R}$ (2—8; pr. *or*)

10. $\mathcal{P}\ or\ (\mathcal{Q}\ or\ \mathcal{R})$ (1—9; pr. *or*)

Next, we assume $\mathcal{P}\ or\ (\mathcal{Q}\ or\ \mathcal{R})$ and show $(\mathcal{P}\ or\ \mathcal{Q})\ or\ \mathcal{R}$

1. $\mathcal{P}\ or\ (\mathcal{Q}\ or\ \mathcal{R})$ (hyp.)
2. $(\mathcal{Q}\ or\ \mathcal{R})\ or\ \mathcal{P}$ (1; Thm. 14.3: $\mathcal{S}\ or\ \mathcal{T}\ \Leftrightarrow\ \mathcal{T}\ or\ \mathcal{S}$)
3. $(\mathcal{R}\ or\ \mathcal{Q})\ or\ \mathcal{P}$ (2; Thm. 14.3: $\mathcal{S}\ or\ \mathcal{T}\ \Leftrightarrow\ \mathcal{T}\ or\ \mathcal{S}$)
4. $\mathcal{R}\ or\ (\mathcal{Q}\ or\ \mathcal{P})$ (3, first part; sym. $\mathcal{P}\,\&\,\mathcal{R}$)
5. $(\mathcal{Q}\ or\ \mathcal{P})\ or\ \mathcal{R}$ (4; Thm. 14.3: $\mathcal{S}\ or\ \mathcal{T}\ \Leftrightarrow\ \mathcal{T}\ or\ \mathcal{S}$)
6. $(\mathcal{P}\ or\ \mathcal{Q})\ or\ \mathcal{R}$ (5; Thm. 14.3: $\mathcal{S}\ or\ \mathcal{T}\ \Leftrightarrow\ \mathcal{T}\ or\ \mathcal{S}$)

□

In the first part of the proof, Steps 1 through 10 conclude $\mathcal{P}\ or\ (\mathcal{Q}\ or\ \mathcal{R})$ from the premise $(\mathcal{P}\ or\ \mathcal{Q})\ or\ \mathcal{R}$. Also, Step 3 of the second part is symmetric (in $\mathcal{P}$ and $\mathcal{R}$) to the premise of the first part, so Step 3 acts as a premise under which we can conclude Step 4. To put it another way, we could insert the entire block of steps from part one, with $\mathcal{P}$ and $\mathcal{R}$ interchanged, between Steps 3 and 4 of the second part. This would prove Step 4 without using symmetry. The use of symmetry eliminates the need to repeat the block of steps.

If the proof of Theorem 14.5 seems excessively involved—to prove something that may be intuitively obvious, we can only respond that it is a price we need to pay, at the moment, for our formal approach. Everything has its price. The benefit of the formal approach is that the explicit rules of inference are able to guide in the step-discovery procedure. This benefit, for students beginning in deductive mathematics, outweighs all the disadvantages. To provide proofs only for statements that do not appear intuitively obvious is legitimate—once the intuition has become reliable.

The general rule for using *or* statements involved a statement of the form $\mathcal{P}_1\ or\ \mathcal{P}_2\ or\ ...\ or\ \mathcal{P}_n$. In order to be consistent, we need a rule for proving statements of the same form. We do this by defining $\mathcal{P}_1\ or\ \mathcal{P}_2\ or\ \mathcal{P}_3$ to be the same as $(\mathcal{P}_1\ or\ \mathcal{P}_2)\ or\ \mathcal{P}_3$ and repeating this as needed to define $\mathcal{P}_1\ or\ \mathcal{P}_2\ or\ ...\ or\ \mathcal{P}_n$. We want the meaning of $\mathcal{P}_1\ or\ \mathcal{P}_2\ or\ \mathcal{P}_3$ to be independent of the way the constituent statements are grouped. This follows from Theorem 14.5.

It follows that to prove $\mathcal{P}_1\ or\ \mathcal{P}_2\ or\ \mathcal{P}_3$, we can assume $\neg(\mathcal{P}_2\ or\ \mathcal{P}_3)$ and show $\mathcal{P}_1$, or assume $\neg\mathcal{P}_1$ and show $\mathcal{P}_2\ or\ \mathcal{P}_3$, or assume $\neg(\mathcal{P}_1\ or\ \mathcal{P}_2)$ and show $\mathcal{P}_3$, or assume $\neg\mathcal{P}_3$ and show $\mathcal{P}_1\ or\ \mathcal{P}_2$.

Corollary 14.6 For sets A, B, and C, $(A \cup B) \cup C = A \cup (B \cup C)$.

Proof: Exercise 4.

Theorem 14.7 The statements $(\mathcal{P}\ and\ \mathcal{Q})\ and\ \mathcal{R}$ and $\mathcal{P}\ and\ (\mathcal{Q}\ and\ \mathcal{R})$ are logically equivalent.

Proof: Exercise 5.

Corollary 14.8 For sets A, B, and C, $(A \cap B) \cap C = A \cap (B \cap C)$.

Proof: Exercise 6.

Theorem 14.9 The statements $if\ \mathcal{P},\ then\ \mathcal{Q}$ and $if\ \neg\mathcal{Q},\ then\ \neg\mathcal{P}$ are logically equivalent.

Proof:

We first assume $if\ \mathcal{P},\ then\ \mathcal{Q}$ and show $if \neg\mathcal{Q},\ then\ \neg\mathcal{P}$.

1. $if\ \mathcal{P},\ then\ \mathcal{Q}$	(hyp.)
2. $\neg\mathcal{P}\ or\ \mathcal{Q}$	(1; Cor. 14.2)
3. $\mathcal{Q}\ or \neg\mathcal{P}$	(2; Thm. 14.3)
4. $\neg(\neg\mathcal{Q})\ or \neg\mathcal{P}$	(3; Axiom: $\mathcal{R} \Leftrightarrow \neg(\neg\mathcal{R})$)
5. $if \neg\mathcal{Q},\ then \neg\mathcal{P}$	(4; Cor. 14.2)

We now assume $if \neg\mathcal{Q},\ then\ \neg\mathcal{P}$ and show $if\ \mathcal{P},\ then\ \mathcal{Q}$.

1. $if \neg\mathcal{Q},\ then \neg\mathcal{P}$	(hyp.)
2. $\neg(\neg\mathcal{Q})\ or \neg\mathcal{P}$	(1; Cor. 14.2)
3. $\mathcal{Q}\ or \neg\mathcal{P}$	(2; Axiom: $\mathcal{R} \Leftrightarrow \neg(\neg\mathcal{R})$)
4. $\neg\mathcal{P}\ or\ \mathcal{Q}$	(3; Thm. 14.3)
5. $if\ \mathcal{P},\ then\ \mathcal{Q}$	(1; Cor. 14.2)

□

The second set of steps in the proof above is merely the first set reversed. In both sets, each step was obtained from the previous step by substituting an equivalent statement—implicitly using the rule for using equivalence. Such a chain of equivalences is better written in the following format:

$\mathcal{P}_1$	
$\Leftrightarrow \mathcal{P}_2$	(reason that $\mathcal{P}_1 \Leftrightarrow \mathcal{P}_2$)
$\Leftrightarrow \mathcal{P}_3$	(reason that $\mathcal{P}_2 \Leftrightarrow \mathcal{P}_3$)
$\Leftrightarrow \mathcal{P}_4$	(reason that $\mathcal{P}_3 \Leftrightarrow \mathcal{P}_4$)
$\Leftrightarrow \mathcal{P}_5$	(reason that $\mathcal{P}_4 \Leftrightarrow \mathcal{P}_5$)

Thus $\mathcal{P}_1$ is equivalent to $\mathcal{P}_5$, since successive substitution in $\mathcal{P}_1 \Leftrightarrow \mathcal{P}_2$ produces $\mathcal{P}_1 \Leftrightarrow \mathcal{P}_5$. Substitution shows that equivalence is a transitive relation. Using this enables us to write a shorter proof of Theorem 14.9. Proofs that involve only substitution of equivalent statements should use this shorter style.

Proof:

$if\ \mathcal{P},\ then\ \mathcal{Q}$

$\Leftrightarrow \neg\mathcal{P}\ or\ \mathcal{Q}$ (Cor. 14.2)

$\Leftrightarrow \mathcal{Q}\ or\ \neg\mathcal{P}$ (Thm. 14.3)

$\Leftrightarrow \neg(\neg\mathcal{Q})\ or\ \neg\mathcal{P}$ (Axiom: $\mathcal{R} \Leftrightarrow \neg(\neg\mathcal{R})$)

$\Leftrightarrow if\ \neg\mathcal{Q},\ then\ \neg\mathcal{P}$ (Cor. 14.2)

□

The statement $if\ \neg\mathcal{Q},\ then\ \neg\mathcal{P}$ is called the *contrapositive* of the statement $if\ \mathcal{P},\ then\ \mathcal{Q}$. Theorem 14.9 asserts that an implication and its contrapositive are logically equivalent.

The statement $if\ \mathcal{Q},\ then\ \mathcal{P}$ is called the *converse* of the statement $if\ \mathcal{P},\ then\ \mathcal{Q}$. The converse of a true statement may be, but is not necessarily, true—so that a statement and its converse are not logically equivalent. Examples are given in the next section, where we consider in more detail what it means for an implication to be true or false.

EXERCISES

1. Fill in the underlined places

(a) 1. _____
.
4. _____
5. $if\ t < 6, then\ t \in$ P (1—4; pr. $\Rightarrow$)

(b) 1. _____
.
4. _____
5. $if\ t \in G, then\ t \in H$ (1—4; pr. $\Rightarrow$)

(c) 1. _____
.
4. _____
5. $for\ all\ t \in G$: $t \in H$ (1—4; pr. $\forall$)

(d) 1. Assume $t \in A$
.
4. $t \in B$
5. _____ (1—4; _____)

(e) 1. Let $t \in A$ be arbitrary
.
4. $t \in B$
5. _____ (1—4; _____)

(f) 3. $a < 6$
.
5. $if\ a < 6, then\ a \in B$
6. _____ (3, 5; us. $\Rightarrow$)

(g) 2. $a \leq 6$

.

5. _____

6. $b \leq 6$ (2, 5; us. $\Rightarrow$)

(h) 1. _____

2. $if\ t \in G, then\ t \in H$

3. $t \in H$ (1, 2; us. $\Rightarrow$)

(i) 1. $G \subseteq H$

2. _____

3. $H \subseteq J$ (1, 2; us. $\Rightarrow$)

(j) 1. _____

2. _____

3. $if\ A \subseteq B, then\ A \subseteq C$ (1, 2; pr. $\Rightarrow$)

(k) 1. $\mathcal{P}\ and\ \mathcal{Q}$

2. $if\ \mathcal{P}, then\ \mathcal{R}$

3. _____ (_____)

4. $\mathcal{R}$ (_____)

(l) 1. _____

2. _____ (1; pr. _____)

3. $if\ x \in B, then\ A \subseteq B$ (2; Thm. 14.1: $\mathcal{P}\ or\ \mathcal{Q} \Leftrightarrow if\ \neg\mathcal{P}, then\ \mathcal{Q}$)

(m) 1. _____

2. $x < 5\ or\ A \subseteq B$ (1; Thm. 14.1: $\mathcal{P}\ or\ \mathcal{Q} \Leftrightarrow if\ \neg\mathcal{P}, then\ \mathcal{Q}$) .

2. Prove Corollary 14.2

3. Prove Theorem 14.4.

4. Give a proof of Theorem 10.1b (For sets A and B, $A \cup B = B \cup A$) using Theorem 14.3, the rule for using equivalence (implicitly), and symmetry.

5. Prove Corollary 14.6.

6. Prove Theorem 14.7.

7. Prove Corollary 14.8.

8. Suppose that $\mathcal{P}$, $\mathcal{Q}$, $\mathcal{R}$, and $\mathcal{S}$ are formal language statements.

Assume: 1. $\mathcal{P}\ or\ \mathcal{Q}$

2. $if\ \mathcal{P}, then\ \mathcal{R}$

3. $if\ \mathcal{Q}, then\ \mathcal{S}$

Show: $\mathcal{R}\ or\ \mathcal{S}$

Proof by Contradiction

When mathematicians want to prove some statement $\mathcal{P}$, they frequently assume the negation of $\mathcal{P}$, and show that this leads to a contradiction. Such a proof by contradiction depends on the following axiom of logic, which formalizes the fact that a statement is either true or false—by definition.

Axiom For any statement $\mathcal{P}$, $\mathcal{P}$ *or* $\neg\mathcal{P}$ is true.

Suppose that we knew a sequence of steps that lead to a contradiction from the premise $\neg\mathcal{P}$. For example, suppose that we know that $x \in C$, and can show that $x \notin C$ follows from $\neg\mathcal{P}$. The statement $\mathcal{P}$ is then proved as follows:

1. $x \in C$
2. $\mathcal{P}$ *or* $\neg\mathcal{P}$ (Ax.: $\mathcal{P}$ *or* $\neg\mathcal{P}$)

Case 1 3. $\mathcal{P}$

Case 2 4. $\neg\mathcal{P}$

.

6. $x \notin C$ # Step 1

7. $\mathcal{P}$ (2—6; us. *or*)

The statement $\mathcal{P}$ follows, since it is true in all cases that don't lead to a contradiction. In practice, the *or* statement $\mathcal{P}$ *or* $\neg\mathcal{P}$ is used implicitly. The steps above are abbreviated as:

1. $x \in C$

2. Assume $\neg\mathcal{P}$ to get #

.

4. $x \notin C$ # Step 1

5. $\mathcal{P}$ (2—4; #)

A proof done according to this second format is called a "proof by contradiction". Such proofs are useful when dealing with top-level negations (*not* statements).

Example 1:

Prove that for sets C and D and an element x (of the universal set), if $x \notin C \cap D$, then $x \notin C$ *or* $x \notin D$.

Proof:

Assume: C, D sets
x element
$x \notin C \cap D$

Show: $x \notin C$ *or* $x \notin D$

The step-discovery procedure dictates:

Proof:

Assume: C, D sets
x element
$x \notin C \cap D$

Show: $x \notin C$ *or* $x \notin D$

1. Assume $x \in C$
.
k-1. $x \notin D$
k. $x \notin C$ *or* $x \notin D$ (1—k-1; pr.*or*)

The way to show Step k-1 $x \notin D$ is to assume the contrary, and get a contradiction. This will have the following form:

1. Assume $x \in C$
2. Assume $x \in D$ to get #

k-2. need # here
k-1. $x \notin D$ (2—k-2; #)
k. $x \notin C$ *or* $x \notin D$ (1—k-1; pr.*or*)

From Steps 1 and 2 we get $x \in C \cap D$, which contradicts the hypothesis:

Proof:

Assume: C, D sets
x element
$x \notin C \cap D$

Show: $x \notin C$ *or* $x \notin D$

1. Assume $x \in C$
2. Assume $x \in D$ to get #
3. $x \in C \cap D$, # hyp. (1, 2; def. $\cap$, imp.)
4. $x \notin D$ (2—3; #)
5. $x \notin C$ *or* $x \notin D$ (1—4; pr.*or*)

□

Notice that the justification for Step 3 shows why Step 3 is true (based, of course, on the assumptions). It does not say what Step 3 contradicts, or why it contradicts anything. The fact that Step 3 contradicts the hypothesis is given after the comma after Step 3.

Example 2:

Prove that for sets C and D and an element x, if $x \notin C \cup D$, then $x \notin C$.

Proof:

Assume: C, D sets
x element
$x \notin C \cup D$

Show: $x \notin C$

The step-discovery procedure dictates:

Proof:

Assume: C,D sets
x element
$x \notin C \cup D$

Show: $x \notin C$

k. $x \notin C$

The step-discovery procedure asks us to consider ways of proving the top-level *not* statement of Step k. (Recall that $x \notin C$ is just shorthand for $\neg(x \in C)$). If the set C were defined, then to show $x \notin C$, we could show x satisfies the negation of the defining property. Since C is just any set, and has not been defined, there is only one way to show this *not* statement—by contradiction.

1. Assume $x \in C$ to get #
.
k-1. need # here
k. $x \notin C$ (1—k-1; #)

From Step 1, we can conclude $x \in C \cup D$, which contradicts the hypothesis.

Proof:

Assume: C, D sets
x element
$x \notin C \cup D$

Show: $x \notin C$

1. Assume $x \in C$ to get #

2. $x \in C \cup D$, # hyp. (1; def. $\cup$, imp.)
3. $x \notin C$ (1—2; #)

□

Example 3:

Prove that for sets C and D and an element x, if $x \notin C$ *or* $x \notin D$, then $x \notin C \cap D$.

Proof:

Assume: C, D sets
x element
$x \notin C$ *or* $x \notin D$
Show: $x \notin C \cap D$

1. Assume $x \in C \cap D$ to get #
.
k-1. need # here
k. $x \notin C \cap D$ (1—k-1; #)

We introduce the hypothesis as Step 2. This introduces cases:

1. Assume $x \in C \cap$ D to get #
2. $x \notin C$ *or* $x \notin D$ (hyp.)
Case 1 3. $x \notin C$
4. $x \in C$, # Step 3 (1; def. $\cap$)
Case 2 5. $x \notin D$
6. $x \in D$, # Step 5 (1; def. $\cap$)
7. $x \notin C \cap D$ (1—6; #, us. *or*)

In using the *or* statement in Step 2, all cases lead to a contradiction. The inference rule on page 41 allows us to infer the negation of Step 1 (which leads the block of steps that includes the *or* statement in Step 2). To justify Step 7, we note both that this is a proof by contradiction, and that we are using the inference rule.

Theorem 15.1 The statements $\neg(\mathcal{P}\ and\ \mathcal{Q})$ and $\neg\mathcal{P}$ *or* $\neg\mathcal{Q}$ are equivalent.

Proof: Exercise 5.

Theorem 15.2 The statements $\neg(\mathcal{P}\ or\ \mathcal{Q})$ and $\neg\mathcal{P}\ and\ \neg\mathcal{Q}$ are equivalent.

Proof: Exercise 6.

Theorem 15.3 The statement $\neg(if\ \mathcal{P}, then\ \mathcal{Q})$ is equivalent to the statement $\mathcal{P}\ and\ \neg\mathcal{Q}$.

Proof:

$\neg(if\ \mathcal{P}, then\ \mathcal{Q})$	
$\Leftrightarrow\ \neg(\neg\mathcal{P}\ or\ \mathcal{Q})$	(Cor. 14.2: $if\ \mathcal{P}, then\ \mathcal{Q} \Leftrightarrow \neg\,\mathcal{P}\ or\ \mathcal{Q}$)
$\Leftrightarrow (\neg(\neg\,\mathcal{P}))\ and \neg\,\mathcal{Q}$	(Thm. 15.2: $\neg(\mathcal{R}\ or\ \mathcal{Q})\ \Leftrightarrow \neg\mathcal{R}\ and\ \neg\mathcal{Q}$)
$\Leftrightarrow \mathcal{P}\ and \neg\,\mathcal{Q}$	(Axiom: $\mathcal{P} \Leftrightarrow \neg(\neg\mathcal{P})$)

□

There is a situation where the inference rule for proving *if-then* statements may look strange. For example, suppose that $x \notin A$ has been established in a proof, and, further, that there is a need to establish $if\ x \in A, then\ x < 7$. The rule for proving *if-then* statements dictates Steps 2 through k-1 below.

1. $x \notin A$
   2. Assume $x \in A$
   .
   k-1. $x < 7$
k. $if\ x \in A, then\ x < 7$ (2—k-1; pr. $\Rightarrow$)

In this case, the rule dictates that we assume something ($x \in A$) contrary to a known fact. While the logic of this can be defended[5], it is probably bad public relations to assume something that is obviously false: "These mathematicians assume things that are contrary to known facts—and they think they are being logical." To avoid the appearance of being illogical, we can show that $if\ \mathcal{P}, then\ \mathcal{Q}$ follows logically from $\neg\mathcal{P}$ as follows:

1. $\neg\mathcal{P}$
2. $\neg\mathcal{P}\ or\ \mathcal{Q}$ (1; pr. or EZ)
3. $if\ \mathcal{P}, then\ \mathcal{Q}$ (2; Cor. 14.2: $if\ \mathcal{P}, then\ \mathcal{Q}\ \Leftrightarrow \neg\mathcal{P}\ or\ \mathcal{Q}$)

Similarly, $if\ \mathcal{P}, then\ \mathcal{Q}$ follows from $\mathcal{Q}$ as follows:

1. $\mathcal{Q}$
2. $\neg\mathcal{P}\ or\ \mathcal{Q}$ (1; pr. or EZ)
3. $if\ \mathcal{P}, then\ \mathcal{Q}$ (2; Cor. 14.2: $if\ \mathcal{P}, then\ \mathcal{Q}\ \Leftrightarrow \neg\mathcal{P}\ or\ \mathcal{Q}$)

By Theorem 15.3 ($\neg(if\ \mathcal{P}, then\ \mathcal{Q}) \Leftrightarrow \mathcal{P}\ and \neg\mathcal{Q}$) we see that the only way that $if\ \mathcal{P}, then\ \mathcal{Q}$ can be false is if $\mathcal{P}$ is true **and** $\mathcal{Q}$ is false. If $\neg\mathcal{P}$ is true, then this doesn't happen—so $if\ \mathcal{P}, then\ \mathcal{Q}$ is true. If $\mathcal{Q}$ is true, then this doesn't happen—so $if\ \mathcal{P}, then\ \mathcal{Q}$ is true. Thus the two short proofs above make sense. We will capture these as EZ forms of the rule for proving *if-then*:

Formats:

pr. $\Rightarrow$ EZ

1. $\neg\mathcal{P}$
k. $if\ \mathcal{P}, then\ \mathcal{Q}$ (1; pr. $\Rightarrow$ EZ)

[5] One can prove anything at all, including $x < 7$, under the assumption $x \in A$, since in a system [indented steps] with contradictions, anything can be shown to be true.

pr. $\Rightarrow$ EZ

1. $\mathcal{Q}$

k. $if\ \mathcal{P},\ then\ \mathcal{Q}$ (1; pr. $\Rightarrow$ EZ)

If when applying the step-discovery procedure, you need to prove a statement of the form $if\ \mathcal{P},\ then\ \mathcal{Q}$, the thing to do is to assume $\mathcal{P}$ and show $\mathcal{Q}$—unless $\neg\mathcal{P}$ or $\mathcal{Q}$ happens to be a previously known step. In that case, merely conclude $if\ \mathcal{P},\ then\ \mathcal{Q}$ by the EZ form of the rule. This will avoid the need to assume something contrary to a known step.

In mathematics, you may assume anything you like, without violating logic, since mathematics knows how to contain the results of such an assumption, without it infecting an entire argument. But this may make some people uncomfortable. In following the step-discovery procedure, you should only make those assumptions that are dictated by the analysis.

Example 4:

Let $\mathcal{P}$ be the statement $8 < 7$, and $\mathcal{Q}$ the statement $6 < 7$. Then $\neg\mathcal{P}$ is true, so by the EZ form of the rule for proving if-$then$ statements, $if\ \mathcal{P}, then\ \mathcal{Q}$ is true. The converse, $if\ \mathcal{Q},\ then\ \mathcal{P}$, is the statement $if\ 6 < 7,\ then\ 8 < 7$ — and this statement is evidently false. It illustrates the only way for an implication to be false: namely, for the hypothesis to be true, **and** the conclusion false (see Theorem 15.3). Such is not the case for the statement $if\ 8 < 7,\ then\ 6 < 7$ — which is therefore a true statement. Such implications, with a false hypothesis, are called *vacuously true.* Theorem 15.3 and the arguments leading to the EZ forms of the rule for proving implications show why mathematicians accept such statements. Some people are quite uncomfortable with vacuously true statements—probably because the precise, mathematical meaning of an if-$then$ statement does not exactly agree with their informal usage of "if-$then$".

Example 5:

Consider the statement $if\ \ x \in \{1,2\},\ then\ x \in \{1,2,3\}$. It is evidently true—with anyone's interpretation of if-$then$. The converse is the statement $if\ \ x \in \{1,2,3\},\ then\ x \in \{1,2\}$. Most users of informal mathematical language would consider this converse as false. What they mean by the statement is that "if x is an arbitrarily chosen element from the set $\{1,2,3\}$, then x is in the set $\{1,2\}$". In such a construction, x is called a *free variable*. We have not yet touched on free variables, and we would need to capture the same meaning with the formal statement $for\ all\ x \in \mathbb{N} : if\ x \in \{1,2,3\},\ then\ x \in \{1,2\}$ — and this formal statement is certainly false. For us, at this point, the statement $if\ x \in \{1,2,3\},\ then\ x \in \{1,2\}$ could not be made unless x were previously defined. And the truth of $if\ x \in \{1,2,3\},\ then\ x \in \{1,2\}$ would depend on the value of the previously defined x: if x were 3, the implication would be false; if x were any other number (say, 1, 2, or 17), the implication would be true.

Dealing with negations (*not* statements) when using the step-discovery procedure

There is no inference rule for either using or proving top-level negations. In order to deal with such statements we use either a proof by contradiction or axioms and theorems that involve equivalent statements.

Example 6:

Let A and B be any sets. Use the step-discovery procedure to find steps leading to a proof of $\neg(A \subseteq B)$.

Solution 1:

1. Assume $A \subseteq B$ to get #

2. $for\ all\ x \in A : x \in B$ (1; def. $\subseteq$)

.
k-1. get # here
k. $\neg(A \subseteq B)$ (1—k-1; #)

In Solution 1, it now remains necessary to use the $for\,all$ statement of Step 2 in order to obtain some contradiction.

Solution 2:

.
.
k-2. $there\,exists\,x \in A\,such\,that\,x \notin B$ (_____; pr. $\exists$)
k-1. $\neg(for\,all\,x \in A : x \in B)$ (k-2; Axiom: neg. $\forall$)
k. $\neg(A \subseteq B)$ (k-1; def. $\subseteq$)

By definition of $\subseteq$, $A \subseteq B$ is equivalent to $for\,all\,x \in A : x \in B$. By the axiom on page 22: if $\mathcal{P}$ is equivalent to $\mathcal{Q}$, then $\neg\mathcal{P}$ is equivalent to $\neg\mathcal{Q}$[6]. We therefore find Step k-1 by substituting $\neg(for\,all\,x \in A : x \in B)$ for $\neg(A \subseteq B)$. In the justification for Step k, we make explicit reference to the equivalence of the relation and its defining condition. The axiom stating the equivalence of the negations is used implicitly. We find Step k-2 by substituting a $there\,exists$ statement for the negation of a $for\,all$ statement—these being equivalent by the axiom on page 15. It now remains necessary to prove the formal $there\,exists$ statement of Step k-2. The rule for doing this is introduced in Section 18.

A proof by contradiction can be employed to use the negation of an element's being in a set. For example, suppose $B = \{x \in \mathbb{N} \mid x < 10\}$. If we knew $t \in \mathbb{N}$ and $t \notin B$, we would like to be able to infer that $t < 10$ was false.

One proof that from $t \in \mathbb{N}$ and $t \notin B$ we can infer $\neg(t < 10)$ is as follows:

1. $t \notin B$
    2. Assume $t < 10$ to get #
    3. $t \in B$, # Step 1 (2; def. B)
4. $\neg(t < 10)$ (2—3; #)

Equivalently, $t \notin B$ is equivalent to $\neg(t < 10)$, since $t \in B$ is equivalent to $t < 10$ — by substitution, or by the axiom on page 22.

Summary Using set definitions: Suppose $A = \{x \mid \mathcal{P}(x)\}$ and t is any element of the universal set. From $t \in A$ we may infer $\mathcal{P}(t)$, and, conversely, from $\mathcal{P}(t)$ we may infer $t \in A$. Also from $t \notin A$ we may infer $\neg(\mathcal{P}(t))$ and from $\neg(\mathcal{P}(t))$ we may infer $t \notin A$.

Example 7:

Define $D = \{x \in \mathbb{N} \mid x < 4\}$. The definition of D tells us why Step 2 below follows from Step 1, and why Step 4 follows from Step 3.

1. $a \notin D$
2. $\neg(a < 4)$ (1; def. D)
3. $\neg(b < 4)$
4. $b \notin D$ (3; def.D)

[6] At our present stage, we could establish this axiom as an easy theorem obtained by substitution and our rule for proving equivalence.

From our experience with the system of natural numbers, we know that $\neg(a < 4)$ is equivalent to $4 \leq a$. This fact depends on an axiom (trichotomy) for the natural numbers that we will consider later.

Solution 2 to Example 5 illustrates the following summarizing convention:

Summary Using the definition of a relation: Suppose some relation has been defined. Then, if the relation holds, the defining condition may be inferred. Conversely, if the defining condition holds, then the relation may be inferred. Also, if the negation of the relation holds, then the negation of the defining condition may be inferred, and conversely.

Example 8:

1. $\neg(S \subseteq T)$
2. $\neg\, for\, all\, x \in S : x \in T$ (1; def. $\subseteq$)

Example 9:

1. $x \notin A \cap B$
2. $\neg(x \in A\, and\, x \in B)$ (1; def. $\cap$)

EXERCISES

1. (a)
   1. $C = \{x \in \mathbb{N} \mid x < 7\}$
   2. $y \notin C$
   3. _____ (1, 2; def. C)

   (b)
   1. $D = \{x \mid \mathcal{P}(x)\}$
   2. $y \notin D$
   3. _____ (1, 2; _____)
   4. $z \in D$
   5. _____ (1, 4; _____)

   (c)
   1. $A \subseteq B$
   2. _____ (1; _____)

   (d)
   1. $\neg(A \subseteq B)$
   2. _____ (1; _____)

   (e)
   1. $x \notin A \cup B$
   2. _____ (1; _____)

2. Prove that for any sets A and B, and any element x, if $x \notin A$, then $x \notin A \cap B$.

3. Prove that for any sets A and B, and any element x, if $x \in A$ and $x \notin A \cap B$, then $x \notin B$.

4. Prove that for any sets A and B, and any element x, if $x \notin A$ *or* $x \notin B$, then $x \notin A \cap B$.

5. Prove Theorem 15.1.

6. Prove Theorem 15.2.

REVIEW EXERCISES

8. (a)

1. _____
.
4. _____
5. $if\ z \in A, then\ z \in B$ (1—4; pr. $\Rightarrow$)

(b)

1. Assume $z \in G$
.
4. $z \in H$
5. _____ (1—4; _____)

(c)

1. Let $z \in G$ be arbitrary
.
4. $z \in H$
5. _____ (1—4; _____)

(d)

2. $a > 6$
.
5. _____
6. $b > 6$ (2, 5; us. $\Rightarrow$)

(e)

1. $B \subseteq C$
2. _____
3. $C \subseteq D$ (1, 2; us. $\Rightarrow$)

Investigation: Discovering Set Identities

The axioms given in Section 13 presented the commutative and associative properties of addition and multiplication of the natural numbers. These properties also hold for the set operations of union and intersection—as was stated in Theorem 9.1 and Corollaries 14.6 and 14.8:

Theorem 9.1 For sets A and B,
(a) $A \cap B = B \cap A$
(b) $A \cup B = B \cup A$

Corollary 15.6 For sets A, B, and C, $(A \cup B) \cup C = A \cup (B \cup C)$.

Corollary 15.8 For sets A, B, and C, $(A \cap B) \cap C = A \cap (B \cap C)$.

The distributive property "if $a, b, c \in \mathbb{N}$, then $a \cdot (b + c) = a \cdot b + a \cdot c$" relates the two operations of addition and multiplication. It says in which way we can either multiply first and then add, or add first and then multiply. In this section we want to discover in what ways the set operations of intersection and union are related. In fact, we will also consider a third set operation, that of set *difference*.

Definition For sets A and B, the *complement* of B in A (also called the *difference*) is the set $A - B$ (read "A minus B") defined by: $A - B = \{x \mid x \in A \text{ and } x \notin B\}$.

Example 1:

(a) If $A = \{2, 3, 4, 5\}$ and $B = \{4, 5, 6, 7\}$, then $A - B = \{2, 3\}$.

(b) $\{x \in \mathbb{N} \mid x < 10\} - \{x \in \mathbb{N} \mid x < 6\} = \{6, 7, 8, 9\}$

The set $A - B$ is pictured as the shaded area in the Venn diagram of Figure 16.1.

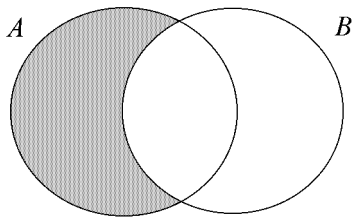


Figure 16.1

Before we seek relationships between set difference and the other set operations, union and intersection, we first ask if the commutative and associative properties hold for difference. In order

to answer this question, we first consider whether $A-(B-C)=(A-B)-C$ holds, for example, for the sets in the following Venn diagram:

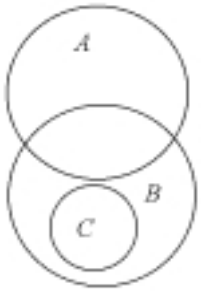
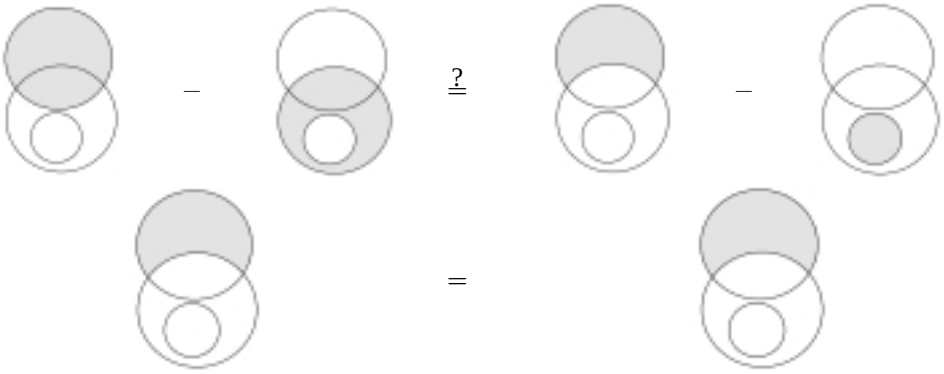


Figure 16.2

The validity of $A-(B-C)=(A-B)-C$ for the sets A, B, C above is checked as in the following example:

Example 2:

$A \quad - \quad (B-C) \quad \stackrel{?}{=} \quad (A-B) \quad - \quad C$



$-$ $\stackrel{?}{=}$ $-$

$=$

Since the shaded area representing $A-(B-C)$ is exactly the same as the shaded area representing $(A-B)-C$, we conclude that $A-(B-C)=(A-B)-C$ for the sets above. Notice, however, that there is a relationship that holds between the sets $A, B,$ and C in the Venn diagram, namely, that $C \subseteq B-A$.

Sets A and B such that $A \cap B=\emptyset$ are called *disjoint*. If also $A \cap C=\emptyset$ and $B \cap C=\emptyset$, then the three sets $A, B,$ and C are called *mutually disjoint*. Three mutually disjoint sets $A, B,$ and C are pictured in the following Venn diagram:

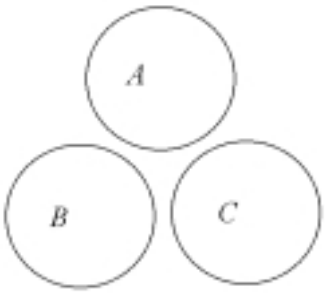
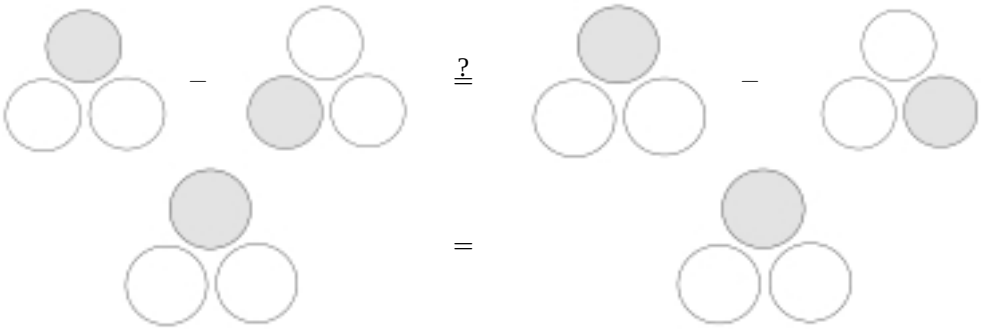


Figure 16.3

The validity of $A-(B-C)=(A-B)-C$ for the sets A, B, C above is checked in the following example.

Example 3:

$A \quad - \quad (B-C) \quad \stackrel{?}{=} \quad (A-B) \quad - \quad C$



Here again we see that $A-(B-C)=(A-B)-C$ — this time under the condition that the sets $A, B,$ and C are mutually disjoint. If we wish to see whether $A-(B-C)=(A-B)-C$ is true for *all* sets, then we need to consider a Venn diagram in which there are no relations between that sets $A, B,$ and C. In such a diagram, the sets are said to be in *general position.* The following diagram exhibits $A, B,$ and C in general position.

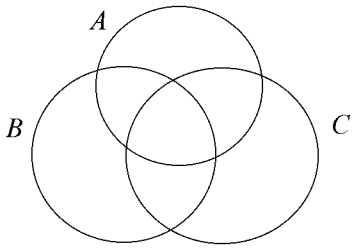
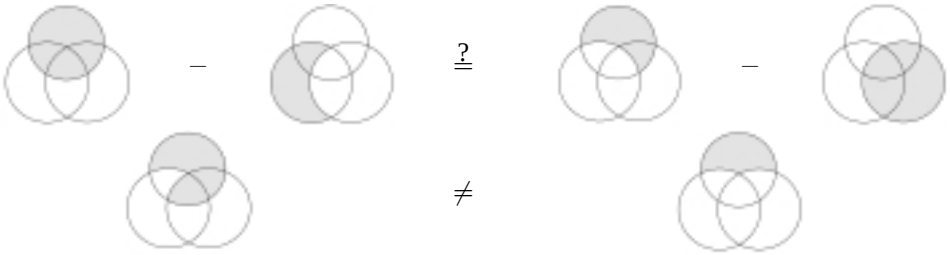


Figure 16.4

The validity of $A-(B-C)=(A-B)-C$ for the sets A, B, C above is checked in the following example.

Example 4:

$A \quad - \quad (B-C) \quad \stackrel{?}{=} \quad (A-B) \quad - \quad C$



From the diagrams above, we see that $A-(B-C)=(A-B)-C$ is *not* true for all sets $A, B,$ and C. In particular, it is not true for those sets pictured in Example 4 .Thus the sets in Example 4 serve as a counterexample to the assertion: "For all sets $A, B,$ and C, $A-(B-C)=(A-B)-C$." As an exercise, you can find sets of natural numbers that also serve as a counterexample. Example 2 leads us to believe that $A-(B-C)=(A-B)-C$ might be true for all sets that satisfy the hypothesis $A \subseteq B-C$. Thus we have the following conjecture: "For sets $A, B,$ and C, if $A \subseteq B-C$, then $A-(B-C)=(A-B)-C$." We also suspect the following conjecture: "For mutually disjoint sets $A, B,$ and C, $A-(B-C)=(A-B)-C$."

Investigation 1: Draw sets A and B in what you would consider to be general position. Using this diagram, show that $A-B=B-A$ is not true for all sets A and B. Thus, both the commutative and associative properties fail for the operation of set difference. Can you find some hypothesis under which $A-B=B-A$ is true? How many different conditions can you find that will insure that $A-B=B-A$ is true? (See the investigations in Section 20.)

The set equations $A \cup B=B \cup A$ and $(A \cap B) \cap C=A \cap (B \cap C)$, for example, are true for all sets $A, B,$ and C. Such equations, true for all values of the variables, are called *identities.* The purpose of this section is to discover (and prove) set identities that relate the set operations of union, intersection, and difference—just as the distributive property for multiplication over addition relates these two operations on the natural numbers. Identities that you find to be true as a result of your investigations in this section can be labeled Theorem 16.1, 16.2, and so on.

Investigation 2: By shading a diagram for sets $A, B,$ and C in general position (Figure 16.4), obtain the Venn diagrams that represent the following sets—sets that are unions, intersections, and differences.

UNIONS	INTERSECTIONS	DIFFERENCES
A	A	A
B	B	B
C	C	C
$A \cup B$	$A \cap B$	$A-B$
$A \cup C$	$A \cap C$	$A-C$
$B \cup C$	$B \cap C$	$B-C$
		$B-A$
		$C-A$
		$C-B$

Now find the sketches of the intersections of all the unions you have that involve all three sets $A, B,$ and C. (For example, sketch $A \cap (B \cup C)$, because it is an intersection of unions, and because it involves $A, B,$ and C). Don't repeat symmetric situations. (For example, having sketched $A \cap (B \cup C)$, don't bother to sketch $B \cap (A \cup C)$—which is merely symmetric in A and B). Label the diagrams with the sets that they represent. Use parentheses to remove ambiguities in your expressions. Then do the same thing to sketch the intersections of the differences. Then find the sketches of all the unions of the intersections and differences. Finally, sketch the differences of the intersections and unions.

Example 5:

You should have obtained the sketch shown in Figure 16.5 as an intersection of differences: $(A-B) \cap (A-C)$—or something symmetric to this expression.

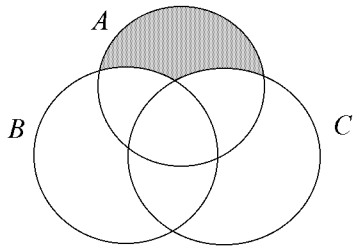


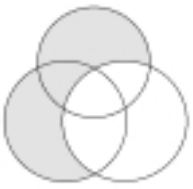
Figure 16.5

Investigation 3: Look through your sketches to find where the same shaded region is described by two or more set expressions. For each such region, make a list of the different ways the region can be described. In mathematics, to say $a = b$ always means that a and b are two names, or two representations, or two descriptions for exactly the same thing. If the same region of the Venn diagram can be described in two different ways, these two representations must be equal for the sets in the diagram. Set your two expressions for the shaded area equal to each other, to get a set equation. Since each of the two ways represents the same set in the Venn diagram, the equation must be true for the sets in the diagram. Conjecture that the equation is true for all sets A, B, and C. Prove this conjecture, or find a counterexample. Repeat the process for other regions. Proven conjectures can be called theorems. Some theorems that you can discover in this way are more important than the theorems in the text.

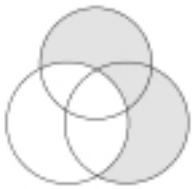
The point of these investigations is to discover relationships between the operations of set union, intersection, and difference. For example, to find a relationship between union and intersection, look for a region that can be described as a union at the top-level, and also as an intersection at the top level. To find other relationships between the same two operations, look for other regions that can be so described.

Example 6:

The Venn diagrams for the sets $(A \cup B) - C$ and $(A - B) \cup (C - B)$ are symmetric:

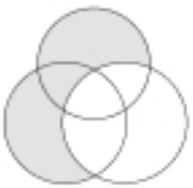


$(A \cup B) - C$

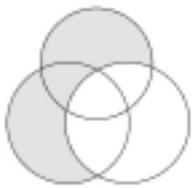


$(A - B) \cup (C - B)$

If we interchange the roles of B and C in the right-hand expression and Venn diagram we get a Venn diagram that is exactly the same as the left hand diagram:



$(A \cup B) - C$



$(A - C) \cup (B - C)$

We therefore conjecture that for all sets $A, B,$ and $C, (A \cup B) - C = (A - C) \cup (B - C)$.

Axiom for Existence; Uniqueness

The axioms of Section 13 don't give us any elements of $\mathbb{N}$, they merely assert what must be true about any elements that there may be in $\mathbb{N}$. The following axiom gives us an element in $\mathbb{N}$, in terms of which all the elements of $\mathbb{N}$ can be defined. It is called an identity for multiplication.

Axiom Existence of identity for multiplication: $There\,exists\,z \in \mathbb{N}\,such\,that\,(for\,all\,a \in \mathbb{N} : z \cdot a = a)$

The identity for multiplication is, of course, the number "one". Before we give it its usual name, however, we prove, *from the axioms*, that there can't be more than one such identity. It is very important in mathematics not to use a single symbol to represent two different things. We want to use the symbol "1" to stand for the identity for multiplication, so we must show there is only one such identity. In this case, we say that the identity is *unique*. We have the following formal rule for proving uniqueness:

Inference Rule Proving uniqueness: To prove that an element with property $\mathcal{P}$ is *unique*, assume two different names, say x_1 and x_2, for an element or elements with property $\mathcal{P}$, and then show $x_1 = x_2$. Abbreviation: "pr. ! "

Format:

pr. !

Assume: $\mathcal{P}(x_1)$ (read "x_1 has property $\mathcal{P}$" or "$\mathcal{P}$ holds for x_1")
$\mathcal{P}(x_2)$

Show: $x_1 = x_2$

In mathematics we always use the word "unique" in relation to some property: we say that an element is unique such that the property holds. By this we mean that there is only one element for which the property holds. For an identity z for multiplication, the property $\mathcal{P}(z)$ is:

$$for\,all\,a \in \mathbb{N}\text{: } z \cdot a = a$$

Theorem 17.1 There exists a unique $z \in \mathbb{N}$ such that $(for\,all\,a \in \mathbb{N}\text{: } z \cdot a = a)$

The phrase "there exists a unique" in Theorem 17.1 comprises two separate parts: existence and uniqueness. The statement of Theorem 17.1 is equivalent to the two assertions:

(1) $there\,exists\,z \in \mathbb{N}\,such\,that\,(for\,all\,a \in \mathbb{N}\text{: } z \cdot a = a)$

and (2) the element whose existence is given in (1) is unique.

In order to prove statements like the one in Theorem 17.1, we therefore need to do two things: (1) prove the existence statement, and (2) prove uniqueness. For Theorem 17.1, the existence part is an axiom, and doesn't need proof. The uniqueness part is proved using the rule for proving uniqueness.

Proof:

The existence part, there exists $z \in \mathbb{N}$ such that $(for\,all\ a \in \mathbb{N}\text{: } z \cdot a = a)$, is a restatement of the axiom we assume. To prove the uniqueness part we have:

Assume: z_1, z_2 integers

1. $for\,all\ a \in \mathbb{N}\text{: } z_1 \cdot a = a$
2. $for\,all\ a \in \mathbb{N}\text{: } z_2 \cdot a = a$

Show: $z_1 = z_2$

1.	$z_1 \cdot z_2 = z_2$	(hyp. 1; us. $\forall$)
2.	$z_2 \cdot z_1 = z_1$	(hyp. 2; us. $\forall$)
3.	$z_1 \cdot z_2 = z_1$	(2; comm. $\cdot$)
4.	$z_1 = z_2$	(1,3; sub.)

□

Step 3 comes from Step 2 by reversing z_1 and z_2 in the product $z_2 \cdot z_1$, by the axiom that gives the commutativity of multiplication.

The steps in the proof of Theorem 17.1 can be written in terms of a more natural (less formal) proof style that involves a chain of equalities: $a_1 = a_2 = a_3 = ... = a_n$, usually written vertically in proofs:

$$
\begin{aligned}
& a_1 \\
&= a_2 && \text{(reason that } a_1 = a_2 \text{)} \\
&= a_3 && \text{(reason that } a_2 = a_3 \text{)} \\
&. \\
&. \\
&= a_n && \text{(reason that } a_{n-1} = a_n \text{)}
\end{aligned}
$$

If we used such a chain, the steps in the preceding proof would be:

$$
\begin{aligned}
& z_1 \\
&= z_2 \cdot z_1 && (z_2 \text{ is } \cdot \text{ identity}) \\
&= z_1 \cdot z_2 && (\text{comm. } \cdot) \\
&= z_2 && (z_1 \text{ is } \cdot \text{ identity})
\end{aligned}
$$

□

We now know that there is only one multiplicative identity, and we give it its usual name "1". The property asserting existence of an identity can then be rewritten using the symbol "1" and the commutative property:

Axiom Property of $\cdot$ identity: $for\,all\ a \in \mathbb{N}:\ 1 \cdot a = a = a \cdot 1$

It is very important, at this point, to distinguish between our imaginative idea of addition and the properties of addition given by the axioms. Through experiences with counting — one, two, three, four, five, ... — we learn to use numbers as adjectives, and to come to conclusions involving this use. For example, we see that 2 apples plus 3 apples gives 5 apples, 2 pears plus 3 pears gives 5 pears, and so on. From this experience with using numbers as adjectives, we come to an abstract understanding of numbers as nouns. We realize that $2 + 3 = 5$ is a true statement about

numbers, that is, about the nouns. All civilizations with written languages have had symbols (called *numerals*) for the numbers one, two, three, four, and so on. This understanding of the natural numbers as nouns is the most basic idea in mathematics. It is even more basic than the idea of proof. Nevertheless, it is important to remain faithful also to the idea of proof—where everything must follow either from definitions or from axioms relating undefined terms.

We need to use statements such as $2 + 3 = 5$ in proof steps. Justification of such an equation must follow from the definitions of the terms involved and the axioms relating undefined terms. It is not legitimate, in a proof step, to bring in an appeal to some physical situation—to claim, for example, that two apples "plus" three apples gives five apples. To do this would be to import an imaginative idea of addition that is not completely captured in the axioms.

The natural numbers $2, 3, 4, 5$ and so on, are defined in terms of the identity of multiplication, 1, given by our axiom. Define the number 2 as $1 + 1$. The number 3 is defined as $2 + 1$. Similarly, define $4 = 3 + 1$, $5 = 4 + 1$, $6 = 5 + 1$, and so on. By the closure axiom, $2, 3, 4,$ and so on, are all natural numbers. The formal definitions agree exactly with our intuition.

From the definitions of the natural numbers, come all the facts about them. For example, the following facts, used to create multiplication and addition tables, derive from the definitions:

$2 + 2$
$= 2 + (1 + 1)$ (def.2)
$= (2 + 1) + 1$ (assoc. $+$)
$= 3 + 1$ (def. 3)
$= 4$ (def. 4)

$3 + 2$
$= 3 + (1 + 1)$ (def. 2)
$= (3 + 1) + 1$ (assoc. $+$)
$= 4 + 1$ (def. 4)
$= 5$ (def. 5)

$3 + 3$
$= 3 + (2 + 1)$ (def. 3)
$= (3 + 2) + 1)$ (assoc. $+$)
$= 5 + 1$ (previously shown add. fact: $3 + 2 = 5$)
$= 6$ (def. 6)

$2 \cdot 2$
$= 2 \cdot (1 + 1)$ (def. 2)
$= 2 \cdot 1 + 2 \cdot 1$ (distr.)
$= 2 + 2$ (mult. id.)
$= 4$ (previously shown add. fact: $2 + 2 = 4$)

$2 \cdot 3$
$= (1 + 1) \cdot 3$ (def. 2)
$= 1 \cdot 3 + 1 \cdot 3$ (dist.)
$= 3 + 3$ (mult. id.)
$= 6$ (previously shown add. fact: $3 + 3 = 6$)

We will allow such facts about the natural numbers, given in the addition and multiplication tables, (or more extensive computations for large numbers) to be used as proof steps. For example, the statement $7 + 3 = 10$ can be inserted in a proof with the justification "addition fact".

Example 1:

1. $x + 5 = a \cdot 7 + a \cdot 3$
2. $x + 5 = a \cdot (7 + 3)$ (1; Ax.: For $a, b, c \in \mathbb{Z},\ a \cdot (b + c) = a \cdot b + a \cdot c$)
3. $7 + 3 = 10$ (addition fact)
4. $x + 5 = a \cdot 10$ (2, 3; sub.)

Addition facts will frequently be used implicitly—as in the following example:

Example 2:

1. $x + 5 = a \cdot 7 + a \cdot 3$
2. $x + 5 = a \cdot (7 + 3)$ (1; Ax.: For $a, b, c \in \mathbb{Z},\ a \cdot (b + c) = a \cdot b + a \cdot c$)
3. $x + 5 = a \cdot 10$ (2; sub.)

EXERCISE

1. Define the numbers 6, 7, and 8.
   (a) Show that $3 + 4 = 7$.
   (b) Show that $2 \cdot 4 = 8$.

$There\ Exists$ Statements; Order

We now get to the formal inference rules for using and proving $there\,exists$ statements. These were introduced informally on page 15 to explain the logic behind vacuously true statements, and on page 22 to introduce counterexamples. Recall the axioms on page 15 giving the negations of $for\,all$ and $there\,exists$ statements:

Axiom $For\,all$ negation: $\neg(for\ \ all\ \ x \in A : \mathcal{P}(x))$ is equivalent to $there\,exists\ \ x \in A\ \ such\,that\ \neg\mathcal{P}(x)$.

Axiom $There\,exists$ negation: $\neg(there\,exists\ x \in A\ such\,that\ \mathcal{P}(x))$ is equivalent to $for\ all\ x \in A$: $\neg\mathcal{P}(x)$.

Example 1:

For sets A and B, the relation $A \subseteq B$ is equivalent to the statement $for\,all\,x \in A : x \in B$, by definition. Thus $\neg(A \subseteq B)$ is equivalent to $\neg(for\,all\,x \in A : x \in B)$ by the axiom on page 22. In turn, $\neg(for\,all\,x \in A : x \in B)$ is equivalent to $there\,exists\,x \in A\,such\,that\,x \notin B$ by the axiom above. Therefore, to find a counterexample to the assertion $A \subseteq B$, we informally showed this $there\,exists$ statement; that is, we defined an element x, showed that it was in A, and that it was not in B.

We now formalize this as the basis for proving $there\,exists$ statements in proofs.

Inference Rule Proving $there\,exists$ statements: In order to prove the statement $there\,exists\,x \in A\,such\,that\,\mathcal{P}(x)$, define x in the proof steps. Then prove both $x \in A$ and $\mathcal{P}(x)$ for your x. Abbreviation: "pr. $\exists$ ".

Format:

pr. $\exists$

i. <define x here>

j. $x \in A$

k-1. $\mathcal{P}(x)$

k. $there\,exists\,x \in A\,such\,that\,\mathcal{P}(x)$ (i, j, k-1; pr. $\exists$)

Inference Rule Using $there\,exists$ statements: From the statement $there\,exists\,x \in A\,such\,that\,\mathcal{P}(x)$ we may infer both $x \in A$ and $\mathcal{P}(x)$. Abbreviation: " us. $\exists$ ".

Format:

us. $\exists$

i. $there\ exists\ x \in A\ such\ that\ \mathcal{P}(x)$

.

j. $x \in A$ (i; us. $\exists$)

.

k. $\mathcal{P}(x)$ (i; us. $\exists$)

A $there\ exists$ statement (such as in Step i) is considered to define the symbol x, so that we may refer to it later in the proof (for example, in Steps j and k).

In the first sections, we considered an order relation $<$ on the set $\mathbb{N}$ as given, so that we could use it in numerical examples of sets. The transitive property of $<$ was taken as an axiom, which applied the examples, but not to any of the theoretical development. It wasn't used to prove any of the theorems about sets. We now give a formal definition of the relation $<$, and prove the transitive property from its definition and the axioms for addition and multiplication.

Definition For $a, b \in \mathbb{N}$, define a *is less than* b (written $a < b$) iff $there\ exists\ x \in \mathbb{N}\ such\ that\ b = a + x$.

The proof of the following theorem depends on the rules for proving and using $there\ exists$ statements:

Theorem 18.1 Transitivity of $<$: For natural numbers a, b, and c, if $a < b$ and $b < c$, then $a < c$.

Proof:

Assume: $a, b, c \in \mathbb{Z}$

1. $a < b$
2. $b < c$

Show: $a < c$

.

.

k-1. $there\ exists\ x \in \mathbb{N}\ such\ that\ c = a + x$

k. $a < c$ (k-1; def. $<$)

We now need to prove the $there\ exists$ statement of Step k-1. Steps i, j, and k-2 are dictated by the rule for proving such statements.

.

i. <define x here>

.

j. $x \in \mathbb{N}$

.

k-2. $c = a + x$

k-1. $there\ exists\ x \in \mathbb{N}\ such\ that\ c = a + x$

k. $a < c$ (k-1; def. $<$)

The bottom-up analysis of the step-discovery procedure has identified just what we need to do: define x, and show that $x \in \mathbb{N}$ and $c = a + x$ are true about the x we define. We can continue no further from the bottom up, so we use one of the hypotheses:

1.	$there\ exists\ x \in \mathbb{N}\ such\ that\ b = a + x$	(hyp. 1: $a < b$)
	.	
i.	<define x here>	
	.	
j.	$x \in \mathbb{N}$	
	.	
k-2.	$c = a + x$	
k-1.	$there\ exists\ x \in \mathbb{N}\ such\ that\ c = a + x$	
k.	$a < c$	(k-1; def. $<$)

The x that we are given in Step 1 might not be the same as the x we need to define in Step i, so we need to use another letter as the variable in Step 1. The steps we have above are all correct and logical, but if we continue from the development above, we can't define x in Step i, because it has already been defined by the $there\ exists$ statement of Step 1. So we use a letter other than x in Step 1.

1.	$there\ exists\ y \in \mathbb{N}\ such\ that\ b = a +$ y	(hyp. 1: $a < b$)
	.	
i.	<define x here>	
	.	
j.	$x \in \mathbb{N}$	
	.	
k-2.	$c = a + x$	
k-1.	$there\ exists\ x \in \mathbb{N}\ such\ that\ c = a + x$	
k.	$a < c$	(k-1; def. $<$)

The rule for using $there\ exists$ statements gives us Steps 2 and 3:

1.	$there\ exists\ y \in \mathbb{N}\ such\ that\ b = a +$ y	(hyp. 1: $a < b$)
2.	$y \in \mathbb{N}$	(1; us.$\exists$)
3.	$b = a +$ y	(1; us.$\exists$)
	.	
i.	<define x here>	
	.	
j.	$x \in \mathbb{N}$	
	.	
k-2.	$c = a + x$	
k-1.	$there\ exists\ x \in \mathbb{N}\ such\ that\ c = a + x$	
k.	$a < c$	(k-1; def. $<$)

From the second hypothesis we get Steps 4, 5, and 6:

1. $there\ exists\ y \in \mathbb{N}\ such\ that\ b = a + y$	(hyp. 1: $a < b$)
2. $y \in \mathbb{N}$	(1; us.$\exists$)
3. $b = a + y$	(1; us.$\exists$)
4. $there\ exists\ z \in \mathbb{N}\ such\ that\ c = b + z$	(hyp. 2: $b < c$)
5. $z \in \mathbb{N}$	(4; us.$\exists$)
6. $c = b + z$	(4; us.$\exists$)
.	
i. <define x here>	
.	
j. $x \in \mathbb{N}$	
.	
k-2. $c = a + x$	
k-1. $there\ exists\ x \in \mathbb{N}\ such\ that\ c = a + x$	
k. $a < c$	(k-1; def. $<$)

The step-discovery procedure has left us with (1) a clear definition of our task: define x and show $x \in \mathbb{N}$ and $c = a + x$ for our x, and (2) the things we have to work with to define x: a, b, and c from the hypotheses, and y and z, which have been defined in the proof steps.

Since $c = b + z$ and $b = a + y$, we can substitute $a + y$ for b in the first equation to get:

$$\begin{aligned} & c \\ & = b + z \\ & = (a + y) + z \\ & = a + (y + z) \end{aligned}$$

We can define x to be $y + z$. This is done with the statement "Let $x = y + z$". We will use the word "let" in formal proofs in only this way; that is, to define a new symbol in terms of previously defined symbols (analogous to an assignment statement in computer science).

1. $there\ exists\ y \in \mathbb{N}\ such\ that\ b = a + y$	(hyp. 1: $a < b$)
2. $y \in \mathbb{N}$	(1; us.$\exists$)
3. $b = a + y$	(1; us.$\exists$)
4. $there\ exists\ z \in \mathbb{N}\ such\ that\ c = b + z$	(hyp. 2: $b < c$)
5. $z \in \mathbb{N}$	(4; us.$\exists$)
6. $c = b + z$	(4; us.$\exists$)
7. Let $x = y + z$	
8. $x \in \mathbb{N}$	(2, 5, 7; ax.: If $p, q \in \mathbb{N}$, then $p + q \in \mathbb{N}$)
9. $c = (a + y) + z$	(3, 6; sub.)
10. $c = a + (y + z)$	(9; assoc. $+$)
11. $c = a + x$	(7, 10; sub.)
12. $there\ exists\ x \in \mathbb{N}\ such\ that\ c = a + x$	(7, 8, 11; pr.$\exists$)
13. $a < c$	(12; def. $<$)

□

The proof can be shortened with the following rule:

Inference Rule Using $there\ exists$ implicitly: We may refer to either of the statements $x \in A$ or $\mathcal{P}(x)$ within a proof statement $there\ exists\ x \in A\ such\ that\ \mathcal{P}(x)$ that is known to be true. That is, we need not rewrite these as proof steps.

Using this rule allows us to use the formal statements $y \in \mathbb{N}$ and $b = a + y$ within the $there\ exists$ statement of Step 1 — without rewriting these down as proof steps. Similarly, $z \in \mathbb{N}$ and $c = b + z$ can be used right from within Step 4. This allows us to contract the proof:

1. $there\ exists\ y \in \mathbb{N}\ such\ that\ b = a + y$	(hyp. 1: $a < b$)
2. $there\ exists\ z \in \mathbb{N}\ such\ that\ c = b + z$	(hyp. 2: $b < c$)
3. Let $x = y + z$	
4. $x \in \mathbb{N}$	(1, 2, 3; ax.: If $p, q \in \mathbb{N}$, then $p + q \in \mathbb{N}$)
5. $c = (a + y) + z$	(1, 2; sub.)
6. $c = a + (y + z)$	(5; assoc. $+$)
7. $c = a + x$	(3, 6; sub.)
8. $there\ exists\ x \in \mathbb{N}\ such\ that\ c = a + x$	(3, 4, 7; pr.$\exists$)
9. $a < c$	(8; def. $<$)

□

Note that the rule for implicit use of $there\ exists$ statements allows us to work from inside a $there\ exists$ statement, and not only at the top level. It is therefore an exception to the way we work with statements. In effect, we are able to interpret the $there\ exists$ statement informally.

The $there\ exists$ statement of Step 8 need not be written as a proof step, if we use the definition of $<$ implicitly:

1. $there\ exists\ y \in \mathbb{N}\ such\ that\ b = a + y$	(hyp. 1: $a < b$)
2. $there\ exists\ z \in \mathbb{N}\ such\ that\ c = b + z$	(hyp. 2: $b < c$)
3. Let $x = y + z$	
4. $x \in \mathbb{N}$	(1, 2, 3; ax.: $\mathbb{N}$ closed under $+$)
5. $c = (a + y) + z$	(1, 2; sub.)
6. $c = a + (y + z)$	(5; assoc. $+$)
7. $c = a + x$	(3, 6; sub.)
8. $a < c$	(3, 4, 7; def. $<$)

□

To justify Step 8, we need to refer to all the steps needed to prove the implicit $there\ exists$ statement: Step 3, where x is defined, and Steps 4 and 7 which state the needed properties of x. We can't use the definition of $<$ implicitly in using the hypotheses, since the $there\ exists$ statements of Steps 1 and 2 are needed to define the elements y and z for subsequent use in the proof. We can, however, abbreviate the proof further by writing it as a narrative proof:

Narrative proof:

Assume $a < b$ and $b < c$ for $a, b, c \in \mathbb{N}$. We will show $a < c$. Since $a < b$, there exists $y \in \mathbb{N}$ such that $b = a + y$, and since $b < c$, there exists $z \in \mathbb{N}$ such that $c = b + z$. Then $c = b + z = (a + y) + z = a + (y + z)$. Let $x = y + z$. Then $x \in \mathbb{N}$, since $\mathbb{N}$ is closed under $+$. Also $c = a + x$, so that $a < c$ by definition of $<$.

□

Definition For integers a and b, define $a \leq b$ (which is read "a is less than or equal to b") iff $a < b$ *or* $a = b$.

Theorem 18.2 Transitivity of $\leq$: For $a, b, c \in \mathbb{Z}$, if $a \leq b$ and $b \leq c$, then $a \leq c$.

Proof: Exercise 3.

Facts such as $3 < 6$ were considered as "given" for use in the first sections. Here these facts about the natural numbers and the relation $<$ can be shown from the definition of $<$ and previously shown addition facts, which follow from the definition of the elements in $\mathbb{N}$.

Example 1:

In order to show $3 < 6$, we need to prove $there\ exists\ x \in \mathbb{N}\ such\ that\ 6 = 3 + x$. Define $x = 3$. Then $6 = 3 + x = 3 + 3$, by one of the previously shown addition facts.

From now on, we will follow statements such as $3 < 6$ in proofs with the abbreviated justification "(def. $<$)". We will no longer assume that these are "given". They follow (easily) from the definition of $<$ — as in Example 1.

For natural numbers a and b, we define the relation $a > b$, read "a is greater than b", to mean the same as $b < a$. We use "a is greater than b" rather than "b is less than a" if we wish a rather than b to be the subject of our sentence. Mathematically, $a > b$ and $b < a$ mean exactly the same thing. In order that we need not refer to informal ideas in a formal proof, we need the following formal definition:

Definition For integers a and b, define $a > b$ iff $b < a$.

Theorem 18.3 Transitivity of $>$: For $x, y, z \in \mathbb{N}$, if $x > y$ and $y > z$, then $x > z$.

Proof: Exercises 4 and 5.

EXERCISES

1. Write all the steps dictated by the rule for proving $there\ exists$ statements.

   (a)

   k. $there\ exists\ t \in S\ such\ that\ t < 18$

   (b)

   k. $there\ exists\ x \in A \cap B$

2. The following proof fragments use the explicit version of the rule for using $there\ exists$ statements. Rewrite abbreviated versions of these proof fragments that use the inference rule for using $there\ exists$ statements implicitly.

   (a)

   1. $there\ exists\ x \in A\ such\ that\ x < 7$
   2. $x \in A$ (1; us. $\exists$)
   3. $A \subseteq C$ (hyp.)
   4. $x \in C$ (2, 3; def. $\subseteq$, imp.)

   (b)

   1. $there\ exists\ x \in A\ such\ that\ x \in B$
   2. $x \in A$ (1; us. $\exists$)
   3. $x \in B$ (1; us. $\exists$)
   4. $x \in A \cap B$ (2, 3; def. $\cap$, imp.)

3. Prove Theorem 18.2.

4. Follow the step-discovery procedure to prove Theorem 18.3.

5. Use Theorem 18.1 to prove Theorem 18.3. Note that using previously shown theorems in a proof abbreviates the proof, since it makes those steps unnecessary that were used to show the previous theorem. Note also that using previously shown theorems can do no more than this. Anything that can be proved using a theorem can be proved by a direct appeal to definitions and axioms—although the latter process may be so lengthy as to be impractical. By using theorems, it is also not necessary to repeat any creative processes use in the discovery of their proofs; that is, by using theorems, we need not reinvent the (perhaps centuries of) mathematics that led to their proofs.

Trichotomy

It might seem that the axioms we have so far would be enough to tell us everything we need to know about $\mathbb{N}$. This is not the case. In fact, we can't even prove that 1 is not equal to 2 from these axioms. The way that mathematicians show that such a proof is impossible is to find or invent a system in which all the axioms are true, but where $1 = 2$. The system need not be intuitive; it only needs to be logically consistent. (In fact, if $1 = 2$ in the system, it will probably be counter-intuitive to most people.)

Before we give an example in which $1 = 2$, we give a familiar example of a set on which we can define the operation of addition.

Example 1:

Suppose C is the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. Define addition on this set by the way you would add hours on the face of a clock. That is, 9 hours past 8 o'clock is 5 o'clock: we add 9 and 8 to get 17, and then subtract 12 to get 5. Thus $9 + 8 = 5$. In Exercise 6, you are asked to pick examples of numbers in C to illustrate the commutative and associative properties of addition.

Example 2:

Suppose N is the set $\{1\}$. Define addition and multiplication on this set by the rules

$$1 + 1 = 1$$
$$1 \cdot 1 = 1$$

The set $\{1\}$ together with the operations defined above satisfies all the axioms for $\mathbb{N}$ that we have so far; that is, if we replace $\mathbb{N}$ with N in all the axioms, the axioms can be shown to be true statements. The properties all reduce to the equation $1 = 1$ (Exercise 7).

If the number 2 were defined as $1 + 1 = 2$ for the system N of Example 2 (just as it is for $\mathbb{N}$), then since $1 + 1 = 1$ in N, we would have $1 = 2$. It similarly follows that $2 = 3 = 4$, and so on. Also, the equation $1 + 1 = 1$ shows that $there\, exists\, x \in N\, such\, that\, 1 = 1 + x$. This means that $1 < 1$. Of course $1 < 2$ also, because $2 = 1$.

The following axiom for the natural numbers prevents $1 < 2$ and $1 = 2$ from both being true in $\mathbb{N}$ — as they are in N of Example 2.

Axiom Trichotomy: For any $a, b \in \mathbb{N}$, exactly one of the following holds:

(a) $a < b$

(b) $a = b$

(c) $b < a$

The informal phrase "exactly one of the following holds" in the trichotomy axiom means:

(1) the formal statement $(a < b)\, or\, (a = b)\, or\, (b < a)$ holds, and

(2) if any of (a), (b), or (c) is taken as a hypothesis, then the negation of either of the others can be taken as a conclusion.

The equation $1 + 1 = 2$ in the natural numbers $\mathbb{N}$ shows that $there\,exists\,x \in \mathbb{N}\,such\,that$ $2 = 1 + x$. This means that $1 < 2$. By the trichotomy axiom above, then, we can't have $1 = 2$. Also, since $2 + 1 = 3$ in $\mathbb{N}, there\,exists\,x \in \mathbb{N}\,such\,that\ 3 = 2 + x$. This means that $2 < 3$. By trichotomy, then, $2 \neq 3$. From $1 < 2$ and $2 < 3$, we get $1 < 3$, by transitivity—and therefore $1 \neq 3$, by trichotomy.

Continuing in this manner, we see that each newly defined natural number is greater than and distinct from all the previously defined natural numbers. This gives us the well-known ordering of the natural numbers:

$$1 < 2 < 3 < 4 < 5 < ...$$

Further, no number in this list is equal to any other number in the list. You knew this by counting. We wanted to show that it follows from the axioms.

Not much can be done with equations in the natural numbers. Being able to work with and solve equations is the major reason for the creation of the larger number systems. There are a few operations with equations that can be illustrated in the natural numbers. One of these is the fact that we can add the same number to each side of an equation—as in the following example:

Example 3:

Suppose that $x \in \mathbb{N}$ and that we know that $3x + 2 = 17$ is a true statement (equation) about x. Then the fact that we can add 4 to each side of this equation is justified as in the following steps:

1. $3x + 2 = 17$	(hyp.)
2. $17 + 4 = 17 + 4$	(identity)
3. $(3x + 2) + 4 = 17 + 4$	(1, 2; sub.)

Step 2 is an identity and needs no real justification. It will be acceptable to merely note the fact. The net effect of these steps is to add the number 4 to each side of the equation in Step 1. We don't wish to go through this complex procedure and its logic—which involves writing down an identity—every time we want to add the same number to each side of an equation. Consequently, we'll make up a theorem that allows us to merely add the same number to each side of an equation. The proof of the theorem will be the same as the derivation of Step 3 from Steps 1 and 2 above. That is, the theorem will merely be a generalization of the steps above.

Theorem 19.1 If $a = b$ is an equation between natural numbers a and b, and c is any natural number, then

(a) $a + c = b + c$

(b) $a \cdot c = b \cdot c$

Proof of part (a):

Assume: $a, b, c \in \mathbb{N}$

$a = b$

Show: $a + c = b + c$

1. $a + c = a + c$	(identity)
2. $a + c = b + c$	(1, hyp.; sub.)

□

Proof of part (b): Exercise 1.

In applying this theorem, we don't quote the theorem or the theorem number. We merely state what number was added to each side of the equation:

Example 4:

6. $4 + x = 2 \cdot x$
7. $(4 + x) + 3 = (2 \cdot x) + 3$ (6; add 3)

Example 5:

6. $4 + x = 2 \cdot x$
7. $(4 + x) \cdot 5 = (2 \cdot x) \cdot 5$ (6; mult. by 5)

Theorem 19.2 If $x < y$ for $x, y \in \mathbb{N}$, and if $z \in \mathbb{N}$, then

(a) $x + z < y + z$

(b) $x \cdot z < y \cdot z$

Proof: Exercise 2.

Theorem 19.1 has a converse that can be proved using the trichotomy axiom:

Theorem 19.3 Suppose $a, b, c \in \mathbb{N}$.

(a) If $a + c = b + c$, then $a = b$.

(b) If $a \cdot c = b \cdot c$, then $a = b$.

Proof of part (a):

Assume: $a, b, c \in \mathbb{N}$
$a + c = b + c$

Show: $a = b$

	1. $(a < b)\ or\ (a = b)\ or\ (b < a)$	(axiom: trichotomy)
Case 1	2. $a < b$.	
	3. $a + c < b + c$	(2; Thm. 19.2a)
	4. $\neg(a + c = b + c)$ # hyp.	(3; trichotomy)
Case 2	5. $a = b$	
Case 3	6. $b < a$	
	7. $\neg(b + c = a + c)$ # hyp.	(2—4; sym.)
	8. $a = b$	(1—7; us. *or*)

□

Proof of part (b): Exercise 3.

Theorem 19.4 Suppose $a, b, c \in \mathbb{N}$.

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

(b) If $a \cdot c < b \cdot c$, then $a < b$.

Proof: Exercise 4.

Corollary 19.5 Suppose $a, b, c \in \mathbb{N}$.
(a) $a + c \leq b + c$ iff $a \leq b$
(b) $a \cdot c \leq b \cdot c$ iff $a \leq b$

Proof: Exercise 5.

Theorem 19.6 For $a, b \in \mathbb{N}$, if $b < a$, then there exists a unique $x \in \mathbb{N}$ such that $a = b + x$.

Proof:

The existence of $x \in \mathbb{N}$ such that $a = b + x$ follows from the definition of $<$. In order to show uniqueness, assume $a = b + x_1$ and $a = b + x_2$ for $x_1, x_2 \in \mathbb{N}$. Then $x_1 = x_2$ follows from $b + x_1 = b + x_2$ by Theorem 19.3a.

□

Definition Subtraction: For $a, b \in \mathbb{N}$ such that $b < a$, define $a \ minus \ b$ (written $a - b$) to be the unique integer x such that $a = b + x$. Thus $a = b + x$ iff $x = a - b$.

Example 6:

By the definition of subtraction, each addition fact about the natural numbers corresponds to a subtraction fact:

addition facts	corresponding subtraction facts
$2 + 3 = 3 + 2 = 5$	$5 - 2 = 3$ and $5 - 3 = 2$
$2 + 4 = 4 + 2 = 6$	$6 - 2 = 4$ and $6 - 4 = 2$
$1 + 2 = 2 + 1 = 3$	$3 - 1 = 2$ and $3 - 2 = 1$

Such subtraction facts may be used as justification for proof steps—as addition facts are used.

EXERCISES

1. Prove Theorem 191b.
2. Prove Theorem 19.2 parts (a) and (b). Don't try to copy the proof of theorem 19.1. Use the step-discovery procedure.
3. Prove Theorem 19.3b.
4. Prove Theorem 19.4.
5. Prove Corollary 19.5.
6. Pick examples of the numbers 1 through 12 to illustrate that the operation of clock addition of Example 1 satisfies the commutative and associative properties.
7. Show that all axioms we have so far for the operations $+$ and $\cdot$ on $\mathbb{N}$ are satisfied by the operations of $+$ and $\cdot$ defined on the set N of Example 2.

Divisibility; Formal *iff* statements

If a and b are natural numbers, then b is said to *divide* a if there is a natural number c such that $a = bc$.

Example 1:

3 divides 12 since $12 = 3 \cdot 4$.

We now give a formal definition of *divides*.

Definition For $a, b \in \mathbb{N}$, we say b *divides* a iff $there\,exists\ c \in \mathbb{N}\ such\ that\ a = bc$.

The customary notation for saying b divides a is $b \mid a$. The statement $b \mid a$ is also expressed by saying "b is a factor of a" or "a is a multiple of b". The formal statement

$$there\,exists\ c \in \mathbb{N}\ such\ that\ a = bc$$

of the definition above can also be phrased

$$a = bc\ for\ some\ c \in \mathbb{N}$$

Statements of either form may be called either $there\,exists$ statements or $for\,some$ statements.

Example 2:

1. $3 \mid a$
2. $a = 3c\ for\ some\ c \in \mathbb{N}$ (1; definition of "divides")

By the definition of divides, $3 \mid a$ is equivalent to $a = 3c\ for\ some\ c \in \mathbb{N}$. Thus the statement of the relationship $3 \mid a$ in Step 1 can be replaced by its defining condition $a = 3c\ for\ some\ c \in \mathbb{N}$, giving Step 2.

Example 3:

1. $a = 9c\ for\ some\ c \in \mathbb{N}$
2. $9 \mid a$ (1; definition of "divides")

By the definition of divides, $9 \mid a$ is equivalent to $a = 9c\ for\ some\ c \in \mathbb{N}$. Thus the statement of the defining condition $a = 9c\ for\ some\ c \in \mathbb{N}$ in Step 1 can be replaced by the defined relation $9 \mid a$, to get Step 2.

"Definition of *divides*" in justifications is abbreviated "def. $\mid$ ".

Example 4:

1. _____
2. $there\,exists\ z \in \mathbb{N}\ such\ that\ x = yz$ (1; def. $\mid$)

Solution:

1. $y \mid x$
2. $there\,exists\, z \in \mathbb{N}\; such\, that\; x = yz$ (1; def. $\mid$)

Theorem 20.1 Let a, b, $c \in \mathbb{N}$. If $b \mid a$ and $b \mid c$ then $b \mid (a + c)$.

Proof: Exercise 1.

Theorem 20.2 Let a, b, $c \in \mathbb{N}$. If $b \mid a$, then $b \mid ac$.

Proof: Exercise 2

Theorem 20.3 Let a, b, $c \in \mathbb{N}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: Exercise 3.

A $there\,exists$ statement can be used to give a formal definition of the empty set. Let $\mathbb{U}$ be the universal set; that is, all sets that we consider will have elements from $\mathbb{U}$. Then we have the following definition:

Definition A set S is *empty* (written $S = \emptyset$) iff $\neg(there\,exists\, x \in \mathbb{U}\; such\, that\; x \in S)$.

We have used the formal phrase $there\,exists\, x \in \mathbb{U}\; such\, that\; x \in S$ in this definition, since it is in the general form $there\,exists\, x \in A\; such\, that\; \mathcal{P}(x)$. From a statement $there\,exists\, x \in \mathbb{U}\; such\, that\; x \in S$ in some proof, we could infer both $x \in \mathbb{U}$ and $x \in S$, by the rule above. All elements must come from our universal set, however, so there is no need to clutter proof steps with assertions like $x \in \mathbb{U}$—or to worry about it at all. For this reason, we will use the abbreviated statement $there\,exists\, x \in S$,[7] instead of the statement $there\,exists\, x \in \mathbb{U}\; such\, that\; x \in S$. The rules for proving and using the abbreviated statement are exactly the same as the rules for proving and using the longer version, except that we omit explicitly mentioning that elements are in the universal set. With this convention we have the following restatement if the definition:

Definition A set S is *empty* (written $S = \emptyset$) iff $\neg(there\,exists\, x \in S)$.

A proof of the following theorem illustrates the rules or proving and using $there\,exists$ statements, as they apply to the shortened statements.

Theorem 20.4 For sets A, B, and C, if $A \subseteq B$, and $B \cap C = \emptyset$, then $A \cap C = \emptyset$

[7] The negation of the statement $there\,exists\, x \in S$ is the statement $for\,all\, x \in \mathbb{U} : x \notin S$. That is, when we form the negation of $there\,exists\, x \in S$, we must realize that it is an abbreviation of $there\,exists\, x \in \mathbb{U}\; such\, that\; x \in S$.

Proof:

Assume: A, B, C sets
$A \subseteq B$
$B \cap C = \emptyset$

Show: $A \cap C = \emptyset$

k-1. $\neg(there\ exists\ x \in A \cap C)$
k. $A \cap C = \emptyset$ (; def. $\emptyset$)

In order to establish Step k-1, we assume the contrary:

Proof:

Assume: A, B, C sets
$A \subseteq B$
$B \cap C = \emptyset$

Show: $A \cap C = \emptyset$

1. Assume $there\ exists\ x \in A \cap C$ to get #
2. $x \in A \cap C$ (1; us. $\exists$)
3. $x \in A$ (2; def. $\cap$)
4. $x \in B$ (3, hyp.; def. $\subseteq$)
5. $x \in C$ (2; def. $\cap$)
6. $x \in B \cap C$ (4, 5; def. $\cap$)
7. $there\ exists\ x \in B \cap C$ (1, 6; pr. $\exists$)
8. $\neg(there\ exists\ x \in B \cap C)$ # 7. (hyp.; def. $\emptyset$)
9. $\neg(there\ exists\ x \in A \cap C)$ (1—8; #)
10. $A \cap C = \emptyset$ (9; def. $\emptyset$)

□

The $there\ exists$ statement of Step 1 defines the symbol x, and the rule for using $there\ exists$ statements allows us to infer $x \in A \cap C$ about this x. We can omit Step 2 by using the rule implicitly.

In general, the rule for proving the statement $there\ exists\ x \in A\ such\ that\ \mathcal{P}(x)$ states that we must define x and show both that x is in A and that $\mathcal{P}(x)$ is true about x. Thus to prove Step 7, $there\ exists\ x \in B \cap C$, we need to define x and show $x \in B \cap C$. Step 7 is justified by (1,6; pr. $\exists$), since x is defined in Step 1 (by the $there\ exists$ statement) and shown to be in $B \cap C$ in Step 6.

If we use the definition of the empty set implicitly, we need not write down Step 9. That is, assuming (Step 1) that there is something in $A \cap C$, and then obtaining a contradiction proves that $A \cap C$ is empty—by the definition of the empty set:

1. Assume $there\,exists\,x \in A \cap C$ to get #	
2. $x \in A$	(1; def. $\cap$)
3. $x \in B$	(2, hyp.; def. $\subseteq$)
4. $x \in C$	(1; def. $\cap$)
5. $x \in B \cap C$	(3, 4; def. $\cap$)
6. $there\,exists\,x \in B \cap C$	(1, 5; pr. $\exists$)
7. $\neg(there\,exists\,x \in B \cap C)$, # 6.	(hyp.; def. $\emptyset$)
8. $A \cap C = \emptyset$	(1—7; def. $\emptyset$)

We can remove the step (6) with justification "pr. $\exists$" by considering the statement $there\,exists\,x \in B \cap C$ to be the defining condition for $B \cap C \neq \emptyset$—which is the negation of one hypothesis. That is, we know that a statement and its defining condition are equivalent, so by the axiom "If $\mathcal{P} \Leftrightarrow \mathcal{Q}$, then $\neg\mathcal{P} \Leftrightarrow \neg\mathcal{Q}$" we have that the negation of the statement is equivalent to the negation of the defining condition. By the extension of our implicit definition rule to apply to the negations of defining conditions, we can use the definition of the empty set implicitly to get a contradiction in the block of steps 1 through 7. That is, we think of $there\,exists\,x \in B \cap C$ as the condition defining $B \cap C \neq \emptyset$. To prove $B \cap C \neq \emptyset$, therefore, we prove its defining condition $there\,exists\,x \in B \cap C$, but we don't write the defining condition down:

1. Assume $there\,exists\,x \in A \cap C$ to get #	
2. $x \in A$	(1; def. $\cap$)
3. $x \in B$	(2, hyp.; def. $\subseteq$)
4. $x \in C$	(3; def. $\cap$)
5. $x \in B \cap C$	(3, 4; def. $\cap$)
6. $B \cap C \neq \emptyset$, # hyp.	(1, 5; def. $\emptyset$)
7. $A \cap C = \emptyset$	(1—6; def. $\emptyset$)

□

It's not possible to remove the formal $there\,exists$ statement of Step 1 from the proof, since this statement serves to define x.

The proof of Theorem 20.4 illustrates how to handle expressions involving the empty set. In general, the way to prove $X = \emptyset$ for some set X, is to show that X satisfies the property defining the empty set. Then $X = \emptyset$ by definition of the empty set. Similarly, in order to use the information from a known equation $Y = \emptyset$, use the fact that Y has the property defining the empty set; that is, Y is empty.

The equation $X = \emptyset$ has the form $set = set$, so, by definition of set equality, it is equivalent to $X \subseteq \emptyset\,and\,\emptyset \subseteq X$. Each of these expressions of set containment is equivalent to a $for\,all$ statement. The $for\,all$ statements will be *vacuously true*, and to prove such a statement we avoid using the rule for proving $for\,all$ statements, which involves the assumption of a set being nonempty. (See the discussion on page 15.) Our proofs will not be effective communications if they contain vacuously true statements and assumptions that are contrary to known facts. Consequently, we use the definition of the empty set, to prove or use equations of the type $X = \emptyset$.

The abbreviated proof, which uses implicit logic, can be rewritten as a narrative proof:

Narrative Proof:

Assume for sets $A, B,$ and C that $A \subseteq B$ and that $B \cap C = \emptyset$. We show that $A \cap C = \emptyset$. Thus assume there exists $x \in A \cap C$ in order to get a contradiction. Then $x \in A$ by the definition of intersection, so that by hypothesis $x \in B$. Also, $x \in C$ by the definition of intersection, from which we get $x \in B \cap C$—which contradicts the hypothesis. Consequently, $A \cap C = \emptyset$.

□

Consider The Venn diagram of Figure 20.1, which represents the hypotheses of Theorem 20.4.

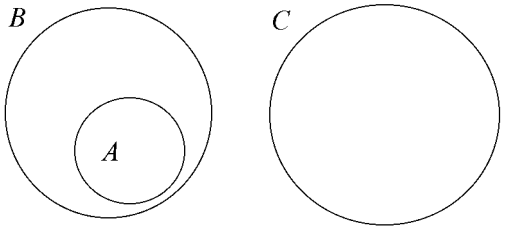


Figure 20.1

In the diagram, we have drawn $A \subseteq B$ and $B \cap C = \emptyset$. (Recall that such sets B and C are called *disjoint*.) It is easy to see from he diagram that A and C must also be disjoint. While it is safe to infer set relationships from appropriately drawn Venn diagrams, it is not *always* safe to draw inferences from diagrams. The rule is that a diagram can be considered as part of a proof, provided that inferences drawn from the diagram can be confirmed, if necessary, by a step-by-step verification. With this understanding about the validity of using diagrams, proofs that depend on diagrams can be considered as a further step in the process of writing increasingly informal proofs. We have seen the following four types of proof, in order of increasing sophistication: (1) step-by-step proofs with explicit logic (formal inference rules explicitly expressed), (2) step-by-step proofs with implicit logic, (3) narrative-style proofs, and (4) proofs using inferences drawn from diagrams.

Investigation 4: In Section 16, we conjectured that $A - (B - C) = (A - B) - C$ is true under either the hypothesis $A \subseteq B - C$ or the hypothesis that $A, B,$ and C are mutually disjoint. Verify both of these conjectures. In Section 16, you found conjectures about set identities by considering Venn diagrams for sets drawn in general position. Repeat Investigations 2 and 3 of Section 16—now, however, with some Venn diagrams for sets $A, B,$ and C that exhibit some relationship; that is, are not in general position. This will lead to conjectures about set relationships that hold under certain hypotheses.

The six types of basic, formal mathematical statements—$there\,exists$, $for\,all$, if-$then$, and, or, and not—make up the language in which mathematics is expressed. Formal "*iff*" statements are defined in terms of if-$then$ and and statements. *Iff* statements provide a formal analog to informal statements of equivalence. Recall that the informal idea of equivalence is used in definitions.

Example 5:

The relation of "subset" was defined as follows:

For sets A and B, $A \subseteq B$ iff $for\,all\ x \in A : x \in B$.

The relationship $A \subseteq B$ between A and B is equivalent, by definition, to the defining condition $for\,all\; x \in A : x \in B$.

Definition The statement $\mathcal{P}\ if\ and\ only\ if\ \mathcal{Q}$ is defined to be the same as $(if\ \mathcal{P}, then\ \mathcal{Q})\ and\ (if\ \mathcal{Q}, then\ \mathcal{P})$. "$If\ and\ only\ if$" is also written "*iff*".

In order to prove a statement $\mathcal{P}$ *iff* $\mathcal{Q}$ we would prove $(if\ \mathcal{P}, then\ \mathcal{Q})\ and\ (if\ \mathcal{Q}, then\ \mathcal{P})$. This top-level and statement is proved in two parts, first we prove $if\ \mathcal{P}, then\ \mathcal{Q}$, and then we prove $if\ \mathcal{Q}, then\ \mathcal{P}$. These two parts are exactly what we do to show that $\mathcal{P}$ is equivalent to $\mathcal{Q}$.

It is possible to speak informally about formal statements; that is, informal statements may contain formal statements. The reverse is not possible, however; that is, formal statements cannot contain informal ones. The formal *iff* is needed to get the idea of equivalence inside formal statements.

Theorem 20.5 For sets A and B, $A = B$ if and only if $for\,all\; x \in \mathbb{U}$: $x \in A$ *iff* $x \in B$.

Proof: Exercise 6.

Theorem 20.6 For sets A and B:
(a) $A \subseteq B$ *iff* $A \cap B = A$
(b) $A \subseteq B$ *iff* $A \cup B = B$

Proof: Exercise 7.

Investigation 5: The statement "if $\mathcal{P}$, then $\mathcal{Q}$" can be expressed by saying that $\mathcal{P}$ is a *sufficient* condition for $\mathcal{Q}$ — or that $\mathcal{Q}$ is a *necessary* condition for $\mathcal{P}$. The statement "$\mathcal{P}$ iff $\mathcal{Q}$" can be expressed by saying that $\mathcal{P}$ is a necessary and sufficient for $\mathcal{Q}$. In Investigation 1, you were asked if you could find some hypothesis under which $A - B = B - A$ was true—that is, could you find a sufficient condition on A and B for $A - B = B - A$ to be true? Is your sufficient condition also necessary? That is, have you found a necessary and sufficient condition for $A - B = B - A$? Which of your hypotheses (sufficient conditions) from Investigation 4 are also necessary?

EXERCISES

1. Prove Theorem 20.1.
2. Prove Theorem 20.2.
3. Prove Theorem 20.3.
4. Prove that the statements $there\,exists\, x \in A\, such\, that\, x \in B$ and $there\,exists\, x \in A \cap B$ are equivalent.
5. Suppose that A, B, and C are sets, that $A \subseteq B$, and that $A \cap C \neq \emptyset$. Prove that B $\cap\, C \neq \emptyset$.
6. Prove Theorem 20.5.
7. Prove Theorem 20.6.

The Integers

In order to provide instructive examples of the functions in the following sections, we need to extend the system $\mathbb{N}$ of natural numbers to include zero and negative numbers. The extended number system is called the set of *integers* and is denoted by $\mathbb{Z}$. The fact that $\mathbb{Z}$ contains all the natural numbers already defined is recorded as our first axiom for the integers:

Axiom $\mathbb{N} \subseteq \mathbb{Z}$.

The following axioms are the same as axioms that hold for $\mathbb{N}$. Since these axioms hold for all elements in $\mathbb{Z}$, they must hold for elements in the subset $\mathbb{N}$ of $\mathbb{Z}$. It is therefore no longer necessary to retain these separately as axioms for $\mathbb{N}$. We say that these properties of elements in $\mathbb{N}$ are now *inherited* from properties in $\mathbb{Z}$.

Axiom Commutativity of addition: If $a, b \in \mathbb{Z}$, then $a + b = b + a$.

Axiom Associativity of addition: If $a, b, c \in \mathbb{Z}$, then $a + (b + c) = (a + b) + c$.

Axiom Commutativity of multiplication: If $a, b \in \mathbb{Z}$, then $a \cdot b = b \cdot a$.

Axiom Associativity of multiplication: If $a, b, c \in \mathbb{Z}$, then $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Axiom Distributivity: If $a, b, c \in \mathbb{Z}$, then $a \cdot (b + c) = a \cdot b + a \cdot c$.

The following axioms for $\mathbb{Z}$ are analogous to those for $\mathbb{N}$:

Axiom Closure under addition: If $a, b \in \mathbb{Z}$, then $a + b \in \mathbb{Z}$.

Axiom Closure under multiplication: If $a, b \in \mathbb{Z}$, then $a \cdot b \in \mathbb{Z}$.

If we add two natural numbers, the result is another natural number. This fact doesn't follow from the axiom above, which tells us only that the sum will be some integer. That is, the fact that the natural numbers are closed under addition is not inherited from the axioms above for $\mathbb{Z}$. We must therefore list it in addition to the axioms above. Thus we need to carry forward the following axioms for $\mathbb{N}$:

Axiom Closure of the subset $\mathbb{N}$ under addition: If $a, b \in \mathbb{N}$, then $a + b \in \mathbb{N}$.

Axiom Closure of the subset $\mathbb{N}$ under multiplication: If $a, b \in \mathbb{N}$, then $a \cdot b \in \mathbb{N}$.

Since the element 1 that acts as an identity of multiplication for $\mathbb{N}$ is a member of the set $\mathbb{N}$, and since $\mathbb{N} \subseteq \mathbb{Z}$, we have that 1 is an integer. The next axiom asserts that 1 acts as an identity of multiplication for all of $\mathbb{Z}$—not only for the subset $\mathbb{N}$.

Axiom Identity for multiplication: $For\,all\ a \in \mathbb{Z} : 1 \cdot a = a \cdot 1 = a$.

The next axiom for $\mathbb{Z}$ asserts the existence of an identity for addition—something which $\mathbb{N}$ lacks, but which is included in the larger system $\mathbb{Z}$.

Axiom Identity for addition: $There\,exists\,z \in \mathbb{Z}\,such\,that\;\;(z + a = a + z = a\,for\,all\,a \in \mathbb{Z})$.

The identity for addition can be shown to be unique—exactly as the identity for multiplication was shown to be unique in Section 17. We can therefore give it its usual name 0, and reword the axiom above:

Axiom Identity for addition: $0 + a = a + 0 = a\,for\,all\;\;a \in \mathbb{Z}$.

Theorem 21.1 $0 \notin \mathbb{N}$.

Proof:

$0 + 0 = 0$, so if $0 \in \mathbb{N}$, then $0 < 0$ by definition of $<$ — which would contradict trichotomy in $\mathbb{N}$. Therefore $0 \notin \mathbb{N}$.

□

The point of enlarging $\mathbb{N}$ is to include additive inverses. For example, the additive inverse of 7 is denoted by -7. The integer -7 has the property that when we add it to 7 we get 0 (the additive identity). The next axiom asserts that every integer has an additive inverse:

Axiom Existence of an additive inverse: For each $a \in \mathbb{Z}$: $there\,exists\;\;b \in \mathbb{Z}\;\;such\,that$ $a + b = b + a = 0$.[8]

Theorem 21.2 For each $a \in \mathbb{Z}$, there exists a unique $b \in \mathbb{Z}$ such that $a + b = 0$.

Proof: Exercise 1.

The unique element b such that $a + b = 0$ (given by Theorem 21.2) is called "negative a" and is denoted by "-a". Thus a + -$a = 0$, and, by commutativity, -$a + a = 0$. The operation of subtraction can be defined for elements of $\mathbb{Z}$ in terms of additive inverses.

Definition For integers a and b, define the integer a *minus* b (written $a - b$) to be a plus the negative of b. That is, $a - b = a$ + -b.

The definition above defines subtraction for all integers, including the natural numbers. However, we already have a definition of subtraction for natural numbers, given on page 132. We must therefore show that the two definitions are equivalent. This follows from the next theorem.

Theorem 21.3 For any integers a and b, a + -$b = x$ iff $a = b + x$.

Proof: Exercise 2.

---

[8] The axiom is given informally—with hypotheses $a \in \mathbb{Z}$, and conclusion $there\,exists\;\;b \in \mathbb{Z}\;\;such\,that$ $a + b = b + a = 0$. There is nothing to be gained by giving this axiom formally as a top-level $for\,all$ statement. The reason for our formality is to guide in the step-discovery procedure, but an axiom doesn't need to be proved.

Investigation 6 Find theorems for the integers that are analogous to Theorems 19.1 and 19.3. If some statements that you get by replacing "natural number" with "integer" are not true, provide counterexamples. In the sequel, we will freely use these (true) theorems extended to the integers.

Part (a) of the next theorem asserts that for any integer a, the inverse of the inverse of a is a itself; that is, -(-a) $= a$. The proof uses Theorem 21.2, which asserts the uniqueness of an inverse, and the following inference rule for using uniqueness:

Inference Rule Using uniqueness: If we know that there is a unique element with property $\mathcal{P}$, then from the facts $\mathcal{P}(x_1)$ and $\mathcal{P}(x_2)$ we can infer $x_1 = x_2$. Abbreviation: " us. ! ".

Example 1:

1. $a + x = 0$
2. $a + y = 0$
3. there exists a unique $b \in \mathbb{Z}$ such that $a + b = 0$ (Thm. 21.2)
4. $x = y$ (1, 2, 3; us. !)

By using the rule above implicitly, we need not cite it as justification for a step. Instead, we cite the theorem that asserts uniqueness, as in Example 2:

Example 2:

1. $a + x = 0$
2. $a + y = 0$
3. $x = y$ (1, 2; Thm. 21.2: For each $a \in \mathbb{Z}$, there exists a unique $b \in \mathbb{Z}$ such that $a + b = 0$)

Theorem 21.4 For each $a, b \in \mathbb{Z}$:
(a) -(-a) $= a$.
(b) $0 \cdot a = 0$
(c) $(-1) \cdot a =$ -a
(d) -a + -b = -$(a + b)$

The proof of part (a) depends on the fact that -(-a) is (by definition) the inverse of -a, and a is also an inverse of -a:

Proof of (a):

Assume: a an integer

Show: -(-a) $= a$

1. $a +$ -$a = 0$ (def. inverse)
2. -$a + a = 0$ (1; comm. $+$)
3. -$a +$ -(-a) $= 0$ (def. inverse)
4. $a =$ -(-a) (2, 3; Thm. 21.2: For each $c \in \mathbb{Z}$, there exists a unique $b \in \mathbb{Z}$ such that $c + b = 0$)

□

Proof of (b):

Assume: a an integer

Show: $0 \cdot a = 0$

1. $0 \cdot a = 0 \cdot a$	(identity)
2. $(0 + 0) \cdot a = 0 \cdot a$	(1; sub. 0 is identity)
3. $0 \cdot a + 0 \cdot a = 0 \cdot a$	(2; dist.)
4. $[0 \cdot a + 0 \cdot a] + \text{-}(0 \cdot a) = 0 \cdot a + \text{-}(0 \cdot a)$	(3; add $\text{-}(0 \cdot a)$)
5. $0 \cdot a + [0 \cdot a + \text{-}(0 \cdot a)] = 0 \cdot a + \text{-}(0 \cdot a)$	(4; assoc. $+$)
6. $0 \cdot a + 0 = 0$	(5; $+$ inv.)
7. $0 \cdot a = 0$	(6; $+$ identity)

□

Proof of (c) and (d): Exercises 2 and 3.

It is a simple matter to extend the definition of order from $\mathbb{N}$ to all of $\mathbb{Z}$:

Definition For $a, b \in \mathbb{Z}$, a is said to be *less than* b (written $a < b$) iff $b = a + x \; for\, some\, x \in \mathbb{N}$.

Thus the integer a is less than the integer b iff we can add some natural number to b to obtain a. This definition clearly extends and does not conflict with the definition of order on $\mathbb{N}$ already given on page 122.

The condition $there\, exists\; x \in \mathbb{N}\; such\, that\; b = a + x$ is logically equivalent to the condition $b - a \in \mathbb{N}$, as the following steps show:

1. $there\, exists\, x \in \mathbb{N}\, such\, that\, b = a + x$	
2. $x \in \mathbb{N}$	(1; us.$\exists$)
3. $b = a + x$	(1: us.$\exists$)
4. $\text{-}a + b = \text{-}a + (a + x)$	(3; add $\text{-}a$)
5. $b + \text{-}a = (\text{-}a + a) + x$	(4; comm. & assoc. +)
6. $b - a = 0 + x$	(5; def. sub. & inv.)
7. $b - a = x$	(6; 0 is $+$ id.)
8. $b - a \in \mathbb{N}$	(2, 7; sub.)

By reversing Steps 1 through 8 above and adjusting the justifications somewhat, we can prove that if we assume $b - a \in \mathbb{N}$, then we can show $there\, exists\; x \in \mathbb{N}\; such\, that\; b = a + x$. The two conditions are therefore equivalent. This result is not important enough for us to call it a theorem, so we merely offer it as an alternate form for the definition of " $<$ ":

Definition For $a, b \in \mathbb{Z}$, define $a < b$ iff $b - a \in \mathbb{N}$.

Either form of the definition can be used to prove the parts of the following theorem.

Theorem 21.5 For all $a, b \in \mathbb{Z}$:

(a) $0 < a$ iff $a \in \mathbb{N}$

(b) $-a < 0$ iff $a \in \mathbb{N}$

(c) $a < 0$ iff $-a \in \mathbb{N}$

(d) $a < b$ iff $-b < -a$

Proof: Exercise 5.

Elements $z \in \mathbb{Z}$ such that $z > 0$ are called *positive* integers. By Theorem 21.5, a positive integer is just a natural number. Elements $z \in \mathbb{Z}$ such that $z < 0$ are called *negative* integers

Axiom Trichotomy for $\mathbb{Z}$: For any $a, b \in \mathbb{Z}$, exactly one of the following holds:

(a) $a < b$

(b) $a = b$

(c) $b < a$

The trichotomy axiom for $\mathbb{N}$, given on page 129, is clearly a consequence of this axiom. If we take b in the axiom to be zero, we see that every nonzero integer is either positive or negative and that no integer can be both positive and negative.

Theorem 21.5 is therefore the basis for the ordering of the integers:

$$\ldots -4 < -3 < -2 < -1 < 0 < 1 < 2 < 3 < 4 \ldots$$

Example 3:

$3 < 6$ (def. $<$), so $-6 < -3$ (Thm. 21.5d)

Theorem 21.6 For any $a \in \mathbb{Z}$, exactly one of the following holds:

(a) $a \in \mathbb{N}$

(b) $a = 0$

(c) $-a \in \mathbb{N}$

Proof: Exercise 6.

Rules for adding, subtracting, and multiplying negative integers are based on theorems that we now consider.

Theorem 21.7 For all $a, b \in \mathbb{Z}$:

(a) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$

(b) $(-a) \cdot (-b) = a \cdot b$

Consider the statement $(-a) \cdot b = -(a \cdot b)$ which is part of (a). $-(a \cdot b)$ is, by definition, the inverse of $a \cdot b$. In order to show $(-a) \cdot b = -(a \cdot b)$, we show that $(-a) \cdot b$ is also an inverse of $a \cdot b$, and then use the uniqueness of an additive inverse to conclude $(-a) \cdot b = -(a \cdot b)$. In order to simplify our notation, we will write the product $a \cdot b$ as ab, that is, either the dot " $\cdot$ " (with numerals) or juxtaposition (with letters) will be used to denote a product.

Proof of part of (a):

We assume a,$b \in \mathbb{Z}$ and show $(\text{-}a)b = \text{-}ab$.

1. $ab + (\text{-}a)b = (a + \text{-}a)b$	(dist.)
2. $ab + (\text{-}a)b = 0 \cdot b$	(1; + inv.)
3. $ab + (\text{-}a)b = 0$	(2; Thm. 21.4b: For each $c \in \mathbb{Z} : 0 \cdot c = 0$)
4. $(\text{-}a)b$ is an inverse of ab	(3; def. inv.)
5. $\text{-}ab$ is an inverse of ab	(notation for inv.)
6. $(\text{-}a)b = \text{-}ab$	(4,5; Thm. 21.0: uniqueness of + inverse)

□

The remaining part of (a), $a(\text{-}b) = \text{-}ab$, and part (b) are exercises.

Theorem 21.7 is true for any integers a and b, not necessarily positive integers. If we take a and b to be positive integers, however, then $\text{-}a$ and $\text{-}b$ are negative integers, and part (b) of the theorem states the fact, familiar from school computation, that a negative times a negative is positive: (neg.) · (neg.) = (pos.). It is difficult to justify the rule (neg.) · (neg.) = (pos.) to students acquainted only with descriptive mathematics and rules for computation. From our viewpoint, however, we see that the rule is a logical consequence of the axioms. If every integer has an additive inverse, and if the commutative, associative, and other axiomatic properties of the integers are to hold, then (neg.) · (neg.) = (pos.) must hold also. From part (a) of this theorem, we get the rules (pos.) · (neg.) = (neg.) and (neg.) · (pos.) = (neg.). Of course, the rule (pos.) · (pos.) = (pos.) comes from the closure of $\mathbb{N}$ under multiplication.

Example 1:

1. $(\text{-}5) \cdot (\text{-}4) =$ ____ (mult. fact)

Solution:

1. $(\text{-}5) \cdot (\text{-}4) = 20$ (mult. fact)

Theorem 21.7b and the previously accepted multiplication fact $5 \cdot 4 = 20$ give us the solution to Example 1. We will use Theorem 21.7b implicitly when justifying facts such as the one in Example 1—thus enlarging our multiplication facts to include multiplication by positive and negative integers.

Theorem 21.8 For all $a, b \in \mathbb{Z}$:

(a) $a + \text{-}b = \text{-}(b - a)$

(b) $b + \text{-}a = b - a$

Proof:

Part (b) is merely a restatement of the definition of subtraction. In order to prove part (a), assume that a and b are arbitrary integers. Then

$\text{-}(b - a)$	
$= \text{-}(b + \text{-}a)$	(def. subtr.)
$= (\text{-}1) \cdot (b + \ -a)$	(Thm. 21.4c)
$= (\text{-}1) \cdot b + (\text{-}1) \cdot (\ -a)$	(dist.)
$= \text{-}b + (\text{-}1) \cdot (\ -a)$	(Thm. 21.4c)

$= \text{-}b + 1 \cdot a$	(Thm. 21.7b)
$= \text{-}b + a$	(mult. id.)
$= a + \text{-}b$	(comm. $+$)

□

Theorem 21.8 applies to any integers a and b whatever—not only to natural numbers. If we apply the theorem to natural numbers a and b, however, with $a < b$, we get the following rule for adding integers of opposite sign. (Positive integers are said to have "positive sign", and negative integers to have "negative sign".)

> In order to add two integers of opposite sign, subtract the smaller from the larger, ignoring the signs of the integers. Then take the sign of the larger.

Example 2:

To add 7 and -10, ignore the signs of the numbers and observe $7 < 10$. Subtract the smaller from the larger: $10 - 7 = 3$, using the subtraction facts for the natural numbers. Then assign the remainder 3 a negative sign: $7 + \text{-}10 = \text{-}3$. Equivalently, by Theorem 21.8a: $7 + \text{-}10 = \text{-}(10 - 7)$.

Example 3:

To add 7 and -5, ignore the signs of the numbers and observe $5 < 7$. Subtract the smaller from the larger: $7 - 5 = 2$, using the subtraction facts for the natural numbers. Then assign the remainder 2 a positive sign: $7 + \text{-}5 = 2$. Equivalently, by Theorem 21.8b: $7 + \text{-}5 = (7 - 5)$.

Since a positive integer is just a natural number, to add two integers of positive sign, we use the addition facts (see page 119) for the natural numbers—which follow from the definitions of the numbers. To add two integers of negative sign, we use Theorem 21.4d: for $a, b \in \mathbb{Z}$: $\text{-}a + \text{-}b = \text{-}(a + b)$.

Example 4:

$\text{-}7 + \text{-}5 = \text{-}(7 + 5) = \text{-}12$.

Subtraction of integers reduces to some kind of addition, by the rule that subtracting an integer is equivalent to adding the inverse of the integer.

Example 5:

The expression $\text{-}7 - \text{-}5$ involves subtracting a negative 5 from a negative 7. This is equivalent to adding the inverse of -5 to the negative 7. Since, by Theorem 21.4a ($\text{-}(\text{-}a) = a$), the inverse of -5 is 5, we see that $\text{-}7 - \text{-}5$ is equivalent to $\text{-}7 + 5$, which by Theorem 21.8a is $\text{-}7 + 5 = \text{-}(7 - 5) = \text{-}2$. Symbolically: $\text{-}7 - \text{-}5 = \text{-}7 + \text{-}(\text{-}5) = \text{-}7 + 5 = \text{-}(7 - 5) = \text{-}2$.

The following theorems provide a basis for the operations of adding, subtracting, or multiplying both sides of an inequality by the same number—in order to solve the inequality.

Theorem 21.9 For all $a, b, c \in \mathbb{Z}$:

(a) if $a < b$, then $a + c < b + c$

(b) if $a < b$ and $c > 0$, then $ac < bc$

(c) if $a < b$ and $c < 0$, then $ac > bc$

Proof: Exercise 10.

Corollary 21.10 For all $a, b, c \in \mathbb{Z}$:

(a) if $a \leq b$, then $a + c \leq b + c$

(b) if $a \leq b$ and $c > 0$, then $ac \leq bc$

(c) if $a \leq b$ and $c < 0$, then $ac \geq bc$ (where $ac \geq bc$ is defined by $ac > bc \text{ or } ac = bc$)

Proof: Exercise 11.

EXERCISES

1. Prove Theorem 21.2.

2. Prove Theorem 21.3.

3. Prove Theorem 21.4c. Since -a is the inverse of a, the equation here asserts that $(\text{-}1) \cdot a$ is the inverse of a. This can be shown by adding $(\text{-}1) \cdot a$ to a to get 0, and then using the uniqueness of the additive inverse. By Theorem 21.4b and distributivity, we have

$$0 = 0 \cdot a = (1 + \text{-}1) \cdot a = 1 \cdot a + (\text{-}1) \cdot a = a + (\text{-}1) \cdot a.$$

Write this out as a formal step-by-step proof.

4. Prove Theorem 21.4d. Show that -a + -b is an inverse of $a + b$ by adding it to $a + b$ to get 0, and then use the uniqueness of the inverse.

5. Prove Theorem 21.5.

6. Prove Theorem 21.6.

7. Prove the following lemma: if $x + a = a$ or $a + x = a$ is true for any integers x and a, then $x = 0$. If $x + a = a$ is true for all $a \in \mathbb{Z}$, then x must be an identity for addition, and so must be zero by the uniqueness of such an identity. The content of the assertion you are to prove is that in order to have $x = 0$, we need not know $x + a = a$ for all $a \in \mathbb{Z}$ — only for one $a \in \mathbb{Z}$. This a may be x itself. Thus, by the lemma we may conclude $x = 0$ from $x + x = x$. Use this lemma to write a proof of Theorem 21.4b that is shorter than the proof in the text.

8. Prove for all integers a and b, $a(\text{-}b) =$ -ab (the remaining part of Theorem 21.7a).

9. Prove Theorem 21.7b.

10. Prove Theorem 21.9.

11. Prove Corollary 21.10.

Functions; Composition

We have considered the mathematical idea of a *set*. Although this term was not formally defined, a particular set could be defined by our giving a rule (itself an undefined term) for deciding which elements are in the particular set and which are not. Another fundamental idea in mathematics is the idea of a *function*. Informally, a function is a rule of correspondence between two sets: a function f from a nonempty set A to a set B is a rule that associates to each element x of A a uniquely determined element, denoted $f(x)$, of B. $f(x)$ is called the image of x under f. You can think of f as "sending" or "mapping" x in A to $f(x)$ in B. Thus to know a particular function f from A to B, you must know a rule for getting $f(x)$ in B given any x in A. The set A is called the *domain* of f, and B is called the *codomain* of f. The fact that f is a function from A to B is written $f: A \to B$.

Our format for defining a specific function will be to give (1) the function name together with the domain and codomain, (2) the rule that specifies what the function does to each element in the domain, and (3) a "for all elements in the domain" clause. A formal, set-theoretic definition of function is given in Section 25.

Example 1:

Define $f: \mathbb{Z} \to \mathbb{N}$ by $f(x) = x^2 + 3 \; for\, all \; x \in \mathbb{Z}$. Then, for example, $f(1) = 1^2 + 3 = 4$, $f(2) = 7$, $f(0) = 3$, f(-1) $= 4$, and so on.

Example 2:

Define $g: \mathbb{N} \to \mathbb{N}$ by $g(x) = 1 \; for\, all \; x \in \mathbb{N}$. Then, for example, $g(1) = 1, g(2) = 1$, and so on.

Example 3:

Define $h: \mathbb{N} \to \mathbb{N}$ by $h(x) = x + 1 \; for\, all \; x \in \mathbb{N}$. Then, for example, $h(1) = (2)$, $h(2) = 3$, $h(3) = 4$, and so on.

Example 4:

Define $k: \mathbb{N} \to \mathbb{N}$ by $k(x) = \begin{cases} 1 & \text{if } x \text{ is odd} \\ 2 & \text{if } x \text{ is even} \end{cases}$.

Then, for example, $k(1) = 1$, $k(2) = 2$, $k(3) = 1$, $k(4) = 2$, and so on.

Example 5:

Define $f: \mathbb{Z} \to \mathbb{Z}$ by $f(x) = x$. Then, for example, $f(1) = 1$, $f(2) = 2$, f(-1) = -1, and so on.

Note that the rules in Examples 1, 2, 3, and 5 for specifying the function are given by formulas but that the rule in Example 4 also specifies a function. Such a function is sometimes called *conditionally defined*. In all definitions, the $for\, all$ quantification is optional since it is implied when the domain is specified. To use information in the definition of a function, use the (perhaps implicit) $for\, all$ statement. The rule that defines a function is sometimes given by listing the images of the elements in the domain.

Example 6:

Let $A = \{a, b, c, d\}$ and $B = \{1, 2, 3\}$. Define $f: A \to B$ by $f(a) = 1$,$f(b) = 3$, $f(c) = 3$, and $f(d) = 1$. (Sometimes arrows are used to give the same information: $a \to 1$, $b \to 3$, $c \to 3$, $d \to 1$.)

It is sometimes helpful to diagram a function with its domain and codomain. For example, $f: A \to B$ is pictured as in Figure 1.

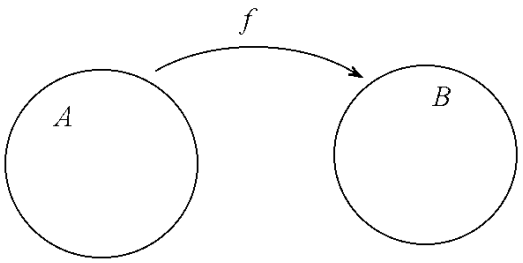


Figure 1

Definition Let $f: A \to B$. Define the set $f(A) = \{b \in B \mid b = f(x) \ for some \ x \in A\}$. $f(A)$ is called the *range* of f.

Example 7:

Let $f: \mathbb{N} \to \mathbb{N}$ be given by the rule $f(x) = 3x + 1$.

$f(1) = 4$

$f(2) = 7$

$f(\mathbb{N}) = \{4, 7, 10, 13, 16, ...\}$

The range of $f: A \to B$ is diagrammed in Figure 2.

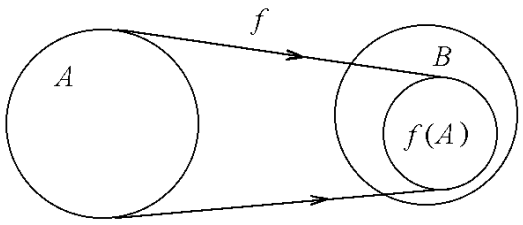


Figure 2

Definition Let $f: A \to B$, $g: B \to C$. Define $g \circ f: A \to C$ by $g \circ f(a) = g(f(a)) \ for all \ a \in A$.

$g \circ f$ is a new function, called the *composition* of g with f, that has the effect of first applying f to an element in A and then applying g to the result. Note that for this to make sense, the range of f must be contained in the domain of g. For simplicity, we take the codomain of f to be the domain of g.

Example 8:

Let $f: \mathbb{Z} \to \mathbb{Z}$ be given by $f(x) = x - 1$ and $g: \mathbb{Z} \to \mathbb{Z}$ be given by $g(y) = y^2 + 2$. Then $g \circ f: \mathbb{Z} \to \mathbb{Z}$ is given by $g \circ f(x) = g(f(x)) = g(x-1) = (x-1)^2 + 2$. Also $f \circ g: \mathbb{Z} \to \mathbb{Z}$ is given by $f \circ g(y) = f(g(y)) = f(y^2+2) = (y^2+2) - 1 = y^2 + 1$.

Composition of functions $f: A \to B$ and $g: B \to C$ is diagrammed in Figure 3.

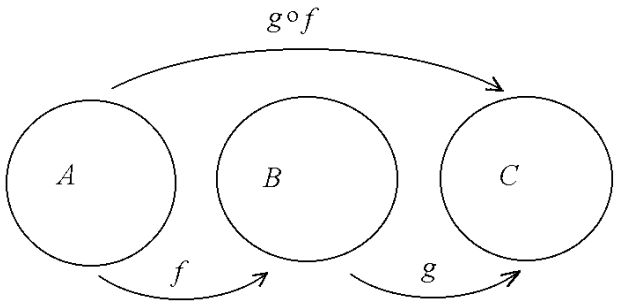


Figure 3

In Example 8 we used the variable x describing f to also describe $g \circ f$, since in $g \circ f$ we first apply f. Similarly, y describes both g and $f \circ g$. Although this was done to illustrate the way in which functions are composed, it is important to understand functions as rules. Composition of functions should therefore be viewed as a rule and not merely as the substitution of variables. The variables are only local variables needed to describe the rules. In the following example, doing without the aid of using different variables to describe f and g forces us to think of the functions as rules.

Example 9:

Let $f: \mathbb{Z} \to \mathbb{Z}$ be given by $f(x) = x^2 - 5 \; for\, all \; x \in \mathbb{Z}$ and $g: \mathbb{Z} \to \mathbb{Z}$ be given by $g(x) = 3x + 2 \; for\, all \; x \in \mathbb{Z}$.

(a) $g \circ f(x) =$

(b) $f \circ g(x) =$

Solution:

(a) $g \circ f(x) = 3(x^2 - 5) + 2 \; for\, all \; x \in \mathbb{Z}$

(b) $f \circ g(x) = (3x + 2)^2 - 5 \; for\, all \; x \in \mathbb{Z}$

Example 10:

Let $f: \{1, 2, 3, 4\} \to \{a, b, c\}$ be given by $1 \to a$, $2 \to b$, $3 \to b$, $4 \to c$.

Let $g: \{a, b, c\} \to \{x, y, z\}$ be defined by $a \to x$, $b \to y$, $c \to z$.

Then $g \circ f: \{1, 2, 3, 4\} \to \{x, y, z\}$ is defined by $1 \to x$, $2 \to y$, $3 \to y$, $4 \to z$.

There is no function $f \circ g$ defined, since the domain of f is not the codomain of g[9].

[9] In defining $g \circ f$ we have used the usual definition of composition, where the domain of g is equal to the codomain of f. This definition will keep notation simple in future theorems, with no real loss of generality. Alternate definitions sometimes require only that the range of f be a subset of the domain of g. The codomain of any such f can easily be redefined to be the domain of g.

Our next theorem asserts the associativity of composition, but first we need the idea of equal functions.

Definition Two functions $f: A \to B$ and $g: A \to B$ are said to be equal (written $f = g$) provided that $for\,all\ x \in A:\ f(x) = g(x)$.

Note that for f and g to be equal they must have the same domain and codomain (the context for definition). The definition just given states that functions are equal if the rules defining them yield the same value when applied to each element of their domain. The idea of equality asserts that the expressions on the left and right of the equal sign are just two names for exactly the same object. The reason we need definitions for equal sets and equal functions is that the ideas of set and function are themselves undefined. Therefore "sameness" needs to be defined in these cases.

Theorem 22.1: Let $f: A \to B$, $g: B \to C$, and $h: C \to D$. Then $(h \circ g) \circ f = h \circ (g \circ f)$.

Note that at the top level, the conclusion is the statement that two functions are equal: $(h \circ g) \circ f = h \circ (g \circ f)$. By the definition of equality, we need to show two things in order to prove the theorem:

(1) $(h \circ g) \circ f$ and $h \circ (g \circ f)$ have the same domain & codomain
(2) $[(h \circ g) \circ f](x) = [h \circ (g \circ f)](x)\ for\,all\ x \in A$

These two things give us the points of the two paragraphs of the proof.

Proof:

First observe that $h \circ g: B \to D$ so that $(h \circ g) \circ f: A \to D$. Also, $g \circ f: A \to C$, so that $h \circ (g \circ f): A \to D$. Therefore $(h \circ g) \circ f$ and $h \circ (g \circ f)$ both have domain A and codomain D by definition of composition.

We now show that $[(h \circ g) \circ f](x) = [h \circ (g \circ f)](x)\ for\,all\ x \in A$:

1. Let $x \in A$.
.
.
k. $(h \circ g) \circ f(x) = h \circ (g \circ f)(x)$
k+1. $(h \circ g) \circ f(x) = h \circ (g \circ f)(x)\ for\,all\ x \in A$ (1—k; pr. $\forall$)

Therefore $(h \circ g) \circ f = h \circ (g \circ f)$ by definition of equal functions.

Step k states that $(h \circ g) \circ f$ and $h \circ (g \circ f)$ do exactly the same thing to x. What these functions do to x is given by their definition. By definition, $[(h \circ g) \circ f](x)$ is $(h \circ g)(f(x))$ and $[h \circ (g \circ f)](x)$ is $h(g \circ f(x))$. Applying the definition again, $(h \circ g)(f(x))$ is $h(g(f(x)))$ and $h(g \circ f(x))$ is $h(g(f(x)))$. The left and right sides of Step k are therefore the same. In order to establish Step k, we therefore start with this same thing as a step in our proof:

2. $h(g(f(x))) = h(g(f(x)))$ (identity)

Such steps (obvious identities) need no justification in parentheses. We now have the following proof:

Proof:

First observe that $h \circ g: B \to D$ so that $(h \circ g) \circ f: A \to D$. Also, $g \circ f: A \to C$, so that $h \circ (g \circ f): A \to D$. Therefore $(h \circ g) \circ f$ and $h \circ (g \circ f)$ both have domain A and codomain D by definition of composition.

We next show that $[(h \circ g) \circ f](x) = [h \circ (g \circ f)](x)$ $for\, all\ x \in A$:

1. Let $x \in A$.
2. $h(g(f(x))) = h(g(f(x)))$ (identity)
3. $h \circ g(f(x)) = h(g \circ f(x))$ (2; def. $\circ$)
4. $(h \circ g) \circ f(x) = h \circ (g \circ f)(x)$ (3; def. $\circ$)

k+1. $(h \circ g) \circ f(x) = h \circ (g \circ f)(x)$ $for\, all\ x \in A$ (1—4; pr. $\forall$)

Therefore $(h \circ g) \circ f = h \circ (g \circ f)$ by definition of equal functions.

□

The fact that the domain and codomain of $h \circ (g \circ f)$ and $(h \circ g) \circ f$ are the same is needed for equality. It is the context in which the definition is made. We "observed" this fact in the first few lines of our proof. In general, we will use the word "observe" in asserting, in a proof, the appropriate context for a theorem or definition. It is customary to omit such observations in proofs if they are obvious.

Steps like Step 2 above, which appear in proofs seemingly out of a clear blue sky, are almost always determined by thinking backward from a desired result. They seem mysterious only to those who imagine steps are discovered in the same order in which they appear in the proof. People who memorize proofs (a wholly worthless activity) may memorize steps in this order. People who *think about* proofs never think in this order. This is why, when reading a mathematics text, it is not informative to merely see why each step follows logically from the preceding steps. Instead, try analyzing the proofs yourself and use the text only if you get stuck. Such a do-it-yourself approach will reveal not only that the theorems are true (false theorems are rarely printed in texts) but *why* they are true.

The form of the preceding proof, with Step 2 appearing out of the blue and with different but simultaneous manipulations of each side of the equations, is awkward. A chain of equalities (page 118) is more natural:

Let $x \in A$.

$(h \circ g) \circ f(x)$

$= (h \circ g)(f(x))$ (def. $\circ$)

$= h(g(f(x)))$ (def. $\circ$)

$= h((g \circ f(x)))$ (def. $\circ$)

$= h \circ (g \circ f)(x)$ (def. $\circ$)

$(h \circ g) \circ f = h \circ (g \circ f)$ (def. $=$ fcns., imp.)

Definition For any set A, define the function $i_A: A \to A$ by $i_A(a) = a$ for each $a \in A$. i_A is called the $identity\, function$ on A.

Example 11:

$i_{\mathbb{N}}: \mathbb{N} \to \mathbb{N}$ is given by $i_{\mathbb{N}}(a) = a$ for all $a \in \mathbb{N}$, so, for example, $i_{\mathbb{N}}(1) = 1$, $i_{\mathbb{N}}(2) = 2$, and so on.

Theorem 22.2 For any $f: A \to B$:
(a) $f \circ i_A = f$
(b) $i_B \circ f = f$

Proof of (a):

Observe first that $f \circ i_A$ and f both have domain A and codomain B.

1. Let $x \in A$ be arbitrary.	
2. $f \circ i_A(x) = f(i_A(x))$	(def. $\circ$)
3. $i_A(x) = x$	(def. i_A)
4. $f \circ i_A(x) = f(x)$	(2,3; sub.)
5. $f \circ i_A(x) = f(x)\ for\ all\ x \in A$	(1—4; pr. $\forall$)
6. $f \circ i_A = f$	(5; def. $=$ fcns.)

□

Proof of (b): Exercise 5.

In the proof of Theorem 22.2a, we used the substitution rule of inference. The definition of composition asserts that the element to which $f \circ i_A$ maps x is the element $f(i_A(x))$. Thus $f \circ i_A(x)$ and $f(i_A(x))$ are the same thing by definition. In Step 2 the equal sign denotes that we have two different names or representations for the same thing, and the same is true in Step 3. Step 4 was obtained by replacing $i_A(x)$ with x in Step 2, these things being equal by Step 3. It is better to use substitution implicitly. The following steps do this for Theorem 22.2a:

1. Let $x \in A$.	
2. $f \circ i_A(x) = f(i_A(x))$	(def. $\circ$)
3. $f \circ i_A(x) = f(x)$	(2; def. i_A)
4. $f \circ i_A(x) = f(x)\ for\ all\ x \in A$	(1—3; pr. $\forall$)

In these steps the definition of i_A was used as a reason for changing Step 2 to Step 3. In doing this, substitution need not be stated explicitly.

In the first proof of Theorem 22.2a, information from the appropriate definitions was put down first. (Note that in this proof, Steps 2 and 3 do not depend on previous steps.) Then this information was organized in Step 4. It is generally better to organize your thoughts on scrap paper (analyzing and changing steps by definition) than to put the contents of definitions down as steps in a proof and then organize things in later proof steps. A proof step with the following justification would be indicative of a poorly organized proof that was difficult to read (see also Exercise 9):

22. ...	(Steps 2,4,7,18,21; sub.)

The most natural proof of Theorem 22.2a, and the easiest to read, involves a chain of equalities.

Let $x \in A$.
$f \circ i_A(x)$
$= f(i_A(x))$ (def. $\circ$)
$= f(x)$ (def. i_A)
$f \circ i_A = f$ (def. $=$ fcns., imp.)

□

Example 12:
Let $f: \mathbb{N} \to \mathbb{N}$ and $g: \mathbb{N} \to \mathbb{N}$ be functions. Define the function $f+g: \mathbb{N} \to \mathbb{N}$ by the rule $f+g(x) = f(x) + g(x)$ for all $x \in \mathbb{N}$. Prove or find a counterexample to

(a) For all functions $h: \mathbb{N} \to \mathbb{N}$: $(f+g) \circ h = (f \circ h)+(g \circ h)$.

(b) For all functions $h: \mathbb{N} \to \mathbb{N}$: $h \circ (f+g) = (h \circ f)+(h \circ g)$.

Proof of (a):

Let $x \in \mathbb{N}$ be arbitrary.
$(f+g) \circ h(x)$
$= (f+g)(h(x))$ (def. $\circ$)
$= f(h(x)) + g(h(x))$ (def. $+$ of fcns.)
$= f \circ h(x) + g \circ h(x)$ (def. $\circ$)
$= [f \circ h + g \circ h](x)$ (def. $+$ of fcns.)
Therefore $(f+g) \circ h = f \circ h + g \circ h$. (def. $=$ fcns.)

□

Counterexample to (b):

Let $h(x) = x^2$, $f(x) = x$, and $g(x) = x$.
Then
$h \circ (f+g)(x) = h(f+g(x)) = h(f(x) + g(x)) = h(x + x) = h(2x) = (2x)^2 = 4x^2$.
But
$h \circ f + h \circ g(x) = h \circ f(x) + h \circ g(x) = h(f(x)) + h(g(x)) = h(x) + h(x) = x^2 + x^2 = 2x^2$

EXERCISES

1. Define a function $f: A \to B$ where
   (a) A has two elements and B has four.
   (b) B has two elements and A has four.

2. Let $f: \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = x^2$. Find
   (a) $f(0)$
   (b) $f(3)$
   (c) $f(-3)$

3. Let $h: \mathbb{N} \to \mathbb{N}$ be defined by $h(z) = z^3 + z$ and $k: \mathbb{N} \to \mathbb{N}$ be defined by $k(z) = z^2 + 2$. Define:
   (a) $h \circ k$
   (b) $k \circ h$

4. Let $f: \{1, 2, 3, 4, 5\} \to \{a, b, c, d, e\}$ be defined by $1 \to a,\ 2 \to a,\ 3 \to b,\ 4 \to b,\ 5 \to c$. Let g: $\{a,b,c,d,e\} \to \{1,2,3,4,5\}$ be defined by $a \to 5$, $b \to 4$, $c \to 4$, $d \to 3$, $e \to 2$. Define
   (a) $f \circ g$
   (b) $g \circ f$

5. Prove Theorem 22.2b.

6. Prove or find a counterexample to the following "cancellation laws" for function composition:
   (a) Let $f: A \to B$, $g: A \to B$, and $h: B \to C$.
   If $h \circ f = h \circ g$, then $f = g$.
   (b) Let $f: A \to B$, $g: A \to B$, and $h: C \to A$.
   If $f \circ h = g \circ h$, then $f = g$.

7. Let $f: \mathbb{N} \to \mathbb{N}$ and $g: \mathbb{N} \to \mathbb{N}$ be functions. Define the function $f \cdot g: \mathbb{N} \to \mathbb{N}$ by the rule $f \cdot g(x) = f(x) \cdot g(x)$ for all $x \in \mathbb{N}$. Prove or find a counterexample to:
   (a) For all functions $h : \mathbb{N} \to \mathbb{N}$: $(f \cdot g) \circ h = (f \circ h) \cdot (g \circ h)$.
   (b) For all functions $h : \mathbb{N} \to \mathbb{N}$: $h \circ (f \cdot g) = (h \circ f) \cdot (h \circ g)$.

8. Prove or find a counterexample to the following:
   (a) For all functions $f: \mathbb{N} \to \mathbb{N}$, $g: \mathbb{N} \to \mathbb{N}$, and $h : \mathbb{N} \to \mathbb{N}$: $(f+g) \cdot h = (f \cdot h) + (g \cdot h)$.
   (b) For all functions $f: \mathbb{N} \to \mathbb{N}$, $g: \mathbb{N} \to \mathbb{N}$, and $h : \mathbb{N} \to \mathbb{N}$: $(f \cdot g) + h = (f + h) \cdot (g + h)$.

9. Comment on the following universal proof scheme. Suppose we are given a theorem $\mathcal{P}$. To prove $\mathcal{P}$, write down all the definitions (as steps) of the terms in $\mathcal{P}$ plus the definitions of the terms in those definitions, and so on until only undefined terms (such as set and function) remain. Call these definitions Steps 1 through Step k. For Step k+1, write down $\mathcal{P}$ and give "substitution" as a reason. (Regardless of what your opinion may be as to the validity of this, you should avoid making your proofs look like this.)

One-to-One Functions

The function $f: \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2$ has the property that $f(2) = 4$, and $f(-2) = 4$. Such a function is called *many-to-one* since there is an element, 4, in the range of f with at least two different elements mapping to it. Functions with only one element in their domain mapping to each element in the range are called *one-to-one* (abbreviated "1-1"). We seek a wording for a definition. This wording should be in terms of our standard phrases: $for\,all$; if ..., $then$ ...; and; or; and so on. Think for a minute of what you could give for a condition on a function $f: A \to B$ that would ensure that f was one-to-one. Here is how we will do it:

Definition A function $f: A \to B$ is called *one-to-one* iff $for\,all\ a_1,\ a_2 \in A\ : if\ f(a_1) = f(a_2),\ then\ a_1 = a_2$.

The idea in the definition is that we pick two different names a_1 and a_2, for objects in A. The condition $f(a_1) = f(a_2)$ states that f sends the object named by a_1 to the same place it sends the object named by a_2. Under these conditions, if f is to be a one-to-one function, it must be the case that a_1 and a_2 are two different names for the same object. Hence $a_1 = a_2$.

One-to-one functions have the property that, for each element in their range there is a unique element in their domain mapping to it. The approach above is generally used to prove uniqueness: pick two different names for an object or objects with a property, then show both names are names for the same object. There is therefore only one object with the property.

Suppose we wish to prove that a function f: $A \to B$ is one-to-one. Our inference rules dictate the following:

1. Let $a_1, a_2 \in A$.
    2. Assume $f(a_1) = f(a_2)$
    .
    .
    k. $a_1 = a_2$

k+1. $if\ f(a_1) = f(a_2), then\ a_1 = a_2$	(2—k; pr. $\Rightarrow$)
k+2. $for\,all\ a_1, a_2 \in A:\ if\ f(a_1) = f(a_2), then\ a_1 = a_2$	(1—k+1; pr.$\forall$)
k+3. f is one-to-one.	(k+2; def. 1-1)

By our implicit definition rule, we may omit Step k+2 since the property $\mathcal{P}$, which establishes that f is one-to-one, is just that given in Step k+2. Our implicit definition rule does not completely remove the strictly logical assertions from the proof, however, since Step k+1 serves to express a part of the defining condition $\mathcal{P}$. It seems inappropriate that we would need to state a part of $\mathcal{P}$ but not $\mathcal{P}$ itself.

Our next step in proof abbreviation will involve combining Steps 1 and 2 above and eliminating Step k+1. That is, we give a single rule for proving statements of the form $for\,all\ x, y \in A:\ if\ \mathcal{P}(x,y), then\ \mathcal{Q}(x,y)$. Note that in the proof fragment above, we prove Step k+2 by first choosing arbitrary a_1 and a_2, then assuming $f(a_1) = f(a_2)$ for these, and finally proving $a_1 = a_2$.

Inference Rule Proving $for\text{-}all\text{-}if\text{-}then$ statements: In order to prove a statement of the form $for\,all\ x \in A:\ if\ \mathcal{P}(x),\ then\ \mathcal{Q}(x)$, choose an arbitrary x in A and assume $\mathcal{P}(x)$ is true for this x. (Either of $x \in A$ or $\mathcal{P}(x)$ may then be used in future steps.) Then prove that $\mathcal{Q}(x)$ is true. Analogous rules hold for more than one variable. (Abbreviation: pr.$\forall \Rightarrow$)

Format:

pr.$\forall \Rightarrow$

i. Let $x \in A$ and $\mathcal{P}(x)$
(or "Let $x \in A$ and assume $\mathcal{P}(x)$"
or "Suppose $x \in A$ and $\mathcal{P}(x)$"
or "Assume $\mathcal{P}(x)$ for $x \in A$").[10]

j. $\mathcal{Q}(x)$

j+1. $for\,all\ x \in A:\ if\ \mathcal{P}(x),\ then\ \mathcal{Q}(x)$ (i—j; pr.$\forall \Rightarrow$)

The extension of the preceding rule to two variables is used in the following example:

Example 1:

Let $f: \mathbb{N} \to \mathbb{N}$ be defined by $f(x) = 2x + 4$ for all $x \in \mathbb{N}$. Prove that f is one-to-one.

Proof:

1. Let $x, y \in \mathbb{N}$ and $f(x) = f(y)$	
2. $2x + 4 = 2y + 4$	(1; def f)
3. $2x = 2y$	(2; Thm. 19.3)
4. $x = y$	(3; Thm. 19.3)
5. $for\,all\ x, y \in \mathbb{N}:\ if\ f(x) = f(y),\ then\ x = y$	(1—4; pr. $\forall \Rightarrow$)
6. f is one-to-one	(5; def. 1-1, exp.)

□

Step 5 could be omitted by using the definition of one-to-one implicitly in Step 6.

Example 2:

The proof of Example 1 in paragraph form might be:

Proof:

Let x,$y \in \mathbb{N}$ and $f(x) = f(y)$. Then $2x + 4 = 2y + 4$ by definition of f. Hence $x = y$, so that f is one-to-one by definition.

□

[10] You will see many other wordings that mean the same thing. It is not the words that count. Readers who know the conclusion you are after will automatically interpret any reasonable words so that their meaning is consistent with obtaining this conclusion. This is the way it is with informal language; the ideas carry us through what would otherwise be ambiguous wordings. Words and phrases are interpreted in context.

Theorem 23.1 Let $f: A \to B$ and $g: B \to C$ be one-to-one functions. Then $g \circ f$ is one-to-one.

Proof: Exercise 3.

Conjecture 23.2 Let $f: A \to B$ and $g: B \to C$ be functions.
(a) If $g \circ f$ is one-to-one, then f is one-to-one.
(b) If $g \circ f$ is one-to-one, then g is one-to-one.

Attempted Proof of (a):

Assume: $g \circ f$ is 1-1

Show: f is 1-1

1. Let $a_1, a_2 \in A$ and $f(a_1) = f(a_2)$
.
.
k. $a_1 = a_2$

k+1. f is one-to-one. (1—k; def. 1-1, imp.)

Further analysis at this time yields nothing: if we ask what it means for $a_1 = a_2$, we learn nothing. It means only that a_1 and a_2 name the same thing. There is no way to break this down further by definition. So, as usual, it is time to invoke the hypothesis. We are starting to get away from proofs that follow immediately from definitions. Generally, we need to be a little bit clever in the way we apply the hypothesis to the problem at hand. Here, of course, we need not be too clever. We know $f(a_1) = f(a_2)$ and that this element is in B—the domain of g, so we apply g. That is, $f(a_1)$ and $f(a_2)$ are two names for the same element of B. Since g is a function, it must send this single element to a single element of C—regardless of whether that element of B is called $f(a_1)$ or $f(a_2)$. Thus, $g(f(a_1)) = g(f(a_2))$. We justify this step by saying "apply g"—which is more natural than the formalism of substituting $f(a_1)$ for $f(a_2)$ in the identity $g(f(a_2)) = g(f(a_2))$

1. Let $a_1, a_2 \in A$ and $f(a_1) = f(a_2)$
2. $g(f(a_1)) = g(f(a_2))$ (1; apply g)
3. $(g \circ f)(a_1) = (g \circ f)(a_2)$ (2; def. $\circ$)
4. $a_1 = a_2$ (3, hyp.; def. 1-1, imp.[11])
5. f is 1-1 (1—4; def. 1-1, imp.)

□

In going from Step 3 to Step 4 we are using the fact that $g \circ f$ is one- to-one. The expanded step-by-step procedure would be this:

3. $g \circ f(a_1) = g \circ f(a_2)$ (2; def.$\circ$)
4. $for\,all\ x,y \in A:\ if\ g \circ f(x) = g \circ f(y),\ then\ x = y$ (hyp.; def. 1-1, exp.)

[11] Here the rule for *using* $for\text{-}all\text{-}if\text{-}then$ statements, given below, is used implicitly.

5. $if\ g\circ f(a_1) = g\circ f(a_2), then\ a_1 = a_2$	(1,4; us.$\forall$)
6. $a_1 = a_2$	(3,5; us $\Rightarrow$)

Steps 5 and 6 can be combined if we introduce a rule for using $for\text{-}all\text{-}if\text{-}\ then$ statements:

Inference Rule Using $for\text{-}all\text{-}if\text{-}then$ statements: If $for\,all\ x \in A:\ if\ \mathcal{P}(x), then\ \mathcal{Q}(x)$ is true, and $a \in A$ and $\mathcal{P}(a)$ are true, then we may infer $\mathcal{Q}(a)$.

1. Let $a_1, a_2 \in A$ and $f(a_1) = f(a_2)$	
2. $g(f(a_1)) = g(f(a_2))$	(1; apply g)
3. $g\circ f(a_1) = g\circ f(a_2)$	(2; def.$\circ$)
4. $for\,all\ x, y \in A:\ if\ g\circ f(x) = g\circ f(y), then\ x = y$	(hyp.; def. 1-1, exp.)
5. $a_1 = a_2$	(1,3,4; us $\forall \Rightarrow$)

Step 4 can be omitted, if we use the definition of 1-1 implicitly—which gives the proof on page 157.

The rule for using $for\text{-}all\text{-}if\text{-}then$ statements is the formal analogue of the rule for using theorems, where the $for\,all$ and if parts correspond to the hypotheses and the $then$ part corresponds to the conclusion. The rule for proving $for\text{-}all\text{-}if\text{-}then$ statements is the formal analog of our informal procedure of assuming the hypotheses and showing the conclusion.

Attempted Proof of (b):

Assume: $g\circ f$ is 1-1

Show: g is 1-1

1. Let $b_1, b_2 \in B$ and $g(b_1) = g(b_2)$.

.

.

k. $b_1 = b_2$

k+1. $for\,all\ b_1, b_2 \in B:\ if\ g(b_1) = g(b_2), then\ b_1 = b_2$	(1—k; pr.$\forall \Rightarrow$)
k+2. g is one-to-one.	(k+1; def. 1-1)

If there were some $a_1,\ a_2\ \in A$ such that $f(a_1) = b_1$ and $f(a_2) = b_2$, then the b_1 and b_2 would be related to the composition $g\circ f$ and we could perhaps proceed. If there are no such a_1 and a_2, then there does not seem to be any way the hypotheses will help us proceed. We therefore will try to construct a counterexample. Here we need to construct functions g and f such that g is not one-to-one but $g\circ f$ is one-to-one. In doing this, we will make some $b \in B$ have the property that f sends no $a \in A$ to this b.

Counterexample 3:

Define $A = \{1\}$, $B = \{2, 3\}$, $C = \{4\}$.

Define f: $A \to B$ by $f(1) = 2$.

Define g: $B \to C$ by $g(2) = 4$, $g(3) = 4$.

Check that g is not one-to-one: $g(2) = g(3)$ but $2 \neq 3$.
Check that $g \circ f$ is one-to-one:

1. Let $a_1, a_2 \in A$ and $g \circ f(a_1) = g \circ f(a_2)$.
2. $a_1 = 1$ (def. A)
3. $a_2 = 1$ (def. A)
4. $a_1 = a_2$ (2,3; sub.)
5. $g \circ f$ is one-to-one. (1—4; def. 1-1, imp.)

□

We can now rewrite as a theorem the part of the conjecture we were able to prove.

Theorem 23.3 Let $f: A \to B$ and $g: B \to$ C be functions. If $g \circ f$ is one-to-one, then f is one-to-one.

In order that a function $f: A \to B$ not be one-to-one, it must satisfy the negation of the defining condition for one-to-one.

Condition: $for\ all\ a_1, a_2 \in A\ :\ if\ f(a_1) = f(a_2), then\ a_1 = a_2$

Negation: $for\ some\ a_1, a_2 \in A:\ \neg(if\ f(a_1) = f(a_2), then\ a_1 = a_2)$

By Theorem 15.3 this can be written:

Negation: $for\ some\ a_1, a_2 \in A:\ f(a_1) = f(a_2)\ and\ a_1 \neq a_2$

In order to prove that some $f: A \to B$ is not one-to-one, then, we need to establish the existence statement above—that is, define a_1 and a_2 and show that they have the required property. See the check that g is not one- to-one in Counterexample 3.

Example 4:

Show that $f: \mathbb{N} \to \mathbb{N}$ defined by $f(x) = 7$ is not one-to-one.

Proof:
$f(1) = 7 = f(2)$ and $1 \neq 2$.

□

Recall that for a statement $if\ \mathcal{P}\ then\ \mathcal{Q}$, the statement $if\ \neg\mathcal{Q}, then\ \neg\mathcal{P}$ is called the contrapositive of the first. Theorem 14.9 asserts that a statement and its contrapositive are equivalent. The statement $if\ a_1 \neq a_2, then\ f(a_1) \neq f(a_2)$ is the contrapositive of the statement $if\ f(a_1) = f(a_2), then\ a_1 = a_2$ that appears in the definition of one-to-one. We can get an alternative formulation for a function's being one-to-one by substituting $if\ a_1 \neq a_2, then\ f(a_1) \neq f(a_2)$ for its contrapositive $if\ f(a_1) = f(a_2), then\ a_1 = a_2$ in the definition of one-to-one. This gives the following theorem:

Theorem 23.4 A function $f: A \to B$ is one-to-one iff $for\ all\ a_1, a_2 \in A:\ if\ a_1 \neq a_2, then\ f(a_1) \neq f(a_2)$.

Here is another formulation of a function's being one-to-one:

Theorem 23.5 Let $f: A \to B$. Then f is one-to-one iff for each b in the range of f there exists a unique $a \in A$ such that $f(a) = b$.

Proof: Exercise 7.

In proving statements of the form "there exists a unique", the wording used in a format for proving uniqueness depends on whether or not existence has been previously established.

Format for proving uniqueness:

i. Let x_1 and x_2 have property $\mathcal{P}$.

.

.

j. $x_1 = x_2$

j+1. There exists a unique x such that $\mathcal{P}$. (if existence has already been shown)

or j+1. There is at most one x such that $\mathcal{P}$. (if existence has not already been shown)

Recall that in our discussions all sets consist of elements from some universal set $\mathbb{U}$ which may be $\mathbb{N}$, $\mathbb{Z}$, or any other set that stays fixed for the discussion. All sets under consideration, then, will be subsets of $\mathbb{U}$.

The definition of $A \subseteq B$ is given by the statement:

(1) $for\,all\ x \in A:\ x \in B$

Since A and B are both subsets of $\mathbb{U}$, it seems clear that $A \subseteq B$ could be defined by

(2) $for\,all\ x \in \mathbb{U}:\ if\ x \in A, then\ x \in B.$

It's not difficult to show (1) is equivalent to (2) (Exercise 6). Using and proving statements in the form of (2) is more complicated than doing the same for statements in the form of (1) — which is why we didn't use (2) to begin our development of proofs. Abbreviations of (2) are commonly used in informal mathematics, however. First, since every element x under consideration must come from $\mathbb{U}$, saying so is not always necessary. Thus (2) can be abbreviated:

(3) $for\,all\ x:\ if\ x \in A, then\ x \in B$

Secondly, the quantification "$for\,all\ x:$" is omitted giving:

(4) $if\ x \in A, then\ x \in B$

In (4), x is called a *free variable*, being neither quantified nor previously defined. However, (4) is not considered to be an open sentence (one that could be either true or false depending on what is substituted for x). It is considered to be an abbreviation of (2) or (3).

Many mathematicians, if asked the question "How is $A \subseteq B$ defined?", would reply that it means "If $x \in A$, then $x \in B$."—using an undefined symbol "x". Since x has not been defined previously, what is meant is "If x is an arbitrarily chosen element of A, then $x \in B$." This use of the "if- then" construction departs from our formal language. We are not allowed to use undefined symbols in proof statements. Thus the only allowable statements involving a new variable x would either define it, as in "let $x \in A$ be arbitrary" or "let $x = 2 +$ ... ", or "$there\,exists\,x\,such\,that$ ...", or use it as a local variable in a $for\,all$ statement .

One frequently sees the definition of a function's being one-to-one given informally by "$f: A \to B$ is one-to-one provided $if\ f(a_1) = f(a_2), then\ a_1 = a_2$." Since a_1 and a_2 have not appeared before, we would tend to think of this as an abbreviation of $for\,all\ a_1, a_2:\ if$

$f(a_1) = f(a_2)$, *then* $a_1 = a_2$. However, $f(a_1)$ and $f(a_2)$ need be defined not for arbitrary elements of $\mathbb{U}$, but only for elements of A. Thus this definition makes the additional assumption that a_1 and a_2 are restricted to a domain in which the notation ($f(a_1)$ and $f(a_2)$) makes sense, that is, restricted to A. This construction is common in informal mathematics:

Convention If $\mathcal{P}(x,y)$ is an assertion in a proof involving previously undefined symbols "x" and "y", then x and y are taken to be arbitrarily chosen elements subject only to the constraint of having $\mathcal{P}(x,y)$ make sense.

It is natural to make implicit use of the convention above—especially in paragraph proofs.

EXERCISES

1. Suppose $f: A \to B$.

1. _____	
2. ...	
3. ...	
4. _____	
5. _____	(1—4; pr. $\forall \Rightarrow$)
6. f is one-to-one.	(5; def. 1-1, exp.)

2. Let $f: \mathbb{N} \to \mathbb{N}$ be defined by $f(x) = 3x + 7$. Show that f is one-to-one.

3. Prove Theorem 23.1.

4. Let $f: \mathbb{N} \to \mathbb{N}$ be defined by $f(x) = x + 1$. Prove that $f \circ f$ is one-to-one.

5. Recall Exercise 22.6a. Prove the following cancellation property of composition: Let $f: A \to B$ and $g: A \to B$. Let $h: B \to C$ be one-to-one. Then if $h \circ f = h \circ g$, then $f = g$.

6. Let A and B be sets and $\mathbb{U}$ the universal set. Prove that $for\,all\ x \in A:\ x \in B$ and $for\,all\ x \in \mathbb{U}:\ if\ x \in A,\ then\ x \in B$ are equivalent statements.

7. Prove Theorem 23.5.

Onto Functions

Conjecture 23.2b states: if $f: A \to B$, $g: B \to C$, and $g \circ f$ is one-to-one, then g is one-to-one. Counterexample 3 in the last section shows that this is not true. Recall that this example was manufactured so that there was a $b \in B$ with no $a \in A$ mapping to b by f. In this section, we will see that we can "fi"x the conjecture to make it true. That is, we can add another hypothesis that will prevent us from constructing an example like Counterexample 3 of Section 23. To do this, we need a definition for functions $f: A \to B$ that have the property that for each $b \in B$ there is some $a \in A$ such that $f(a) = b$.

In this section we relax the requirement that the defining condition for new definitions be given in our formal language. This will continue our trend toward informality. Of course, it is absolutely essential that the meaning of the new definitions be clear. This means that proof formats for proving and for using the defining condition should both be evident.

Mathematics is written in informal language, and it is up to the reader to interpret the meaning—which can be unequivocally understood in terms of proof formats for using and proving the statements. Interpretations in terms of formats can be found by translating the informal statements into our formal language and then using our rules of inference for these. Our formal statements formalize the meaning in common mathematical language, and our formal rules of inference copy what mathematicians generally do to prove or use these statements. The goal in our approach is to be able to understand statements in a very precise way. Thus the formal language and rules are there to build precise mathematical writing and reading habits.

Definition A function $f: A \to B$ is called *onto* iff for each $b \in B$ there exists some $a \in A$ such that $f(a) = b$.

The informal statement

"for each $b \in B$ there exists some $a \in A$ such that $f(a) = b$"

in the definition above means exactly the same as

$$for\ all\ b \in B : f(a) = b\ for\ some\ a \in A$$

or

$$for\ all\ b \in B : there\ exists\ a \in A\ such\ that\ f(a) = b.$$

Recall that

$$f(a) = b\ for\ some\ a \in A$$

and

$$there\ exists\ a \in A\ such\ that\ f(a) = b$$

are two formal statements that mean the same thing.

The reason for using the word "each" in the phrase "for each $b \in B$" is that the weight of the word "all" would tend to make some people violate the grammar of the condition defining onto, as if it meant one a worked for all b. Note the difference between

$$(there\ exists\ a \in A\ such\ that\ f(a) = b)\ for\ all\ b \in B$$

and $\quad there\ exists\ a \in A\ such\ that\ (f(a) = b\ for\ all\ b \in B)$

The defining condition is given by the first of these statements and not the second. Using the word "each" makes it clearer that first b is chosen and then some a (that depends on the choice of b) is found.

Suppose we wish to prove a theorem with the conclusion "f is onto". Since "onto" has not been defined in terms of our formal language, the form of the conclusion does not automatically lead to a proof format or suggest proof steps. It is up to us to capture the meaning of "onto" in the proof steps we select. This can be done by following the rules suggested by an equivalent language statement.

Example 1:

The function $f: \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = x + 4$ is onto.

By the definition of "onto" we need to show that $for\,all\ c \in \mathbb{Z} : there\ exists\ a \in \mathbb{Z}\ such\ that\ f(a) = c$. The following steps therefore prove that f is onto:

Proof:

1. Let $c \in \mathbb{Z}$. (because $\mathbb{Z}$ is the codomain of f)

.

(define a in here)

.

k. $f(a) = c$

k+1. f is onto.

Since $f(a) = a + 4$, we want $c = a + 4$. We are given c and want to define a in terms of c.Hence $c - 4 = a$.

1. Let $c \in \mathbb{Z}$.
2. Let $a = c - 4$
3. $a + 4 = (c - 4) + 4$ (2: add 4)
4. $a + 4 = (c + \text{-}4) + 4$ (3; def. subtraction)
5. $a + 4 = c + (\text{-}4 + 4)$ (4; assoc.)
6. $a + 4 = c + 0$ (5; def. inverse)
7. $a + 4 = c$ (6; $+$ id.)
8. $f(a) = c$ (7; def. f)
9. f is onto (1—8; def. onto)

□

Here is a paragraph form for the proof in Example 1.

Proof:

Let $c \in \mathbb{Z}$ be arbitrary. Define a to be $c - 4$. Then $f(a) = c$ by the definition of f, so that f is onto.

□

In order that a function $f: A \to B$ not be onto, it must satisfy the negation of the defining condition for onto:

Condition: $for\ all\ b \in B:\ there\ exists\ a \in A\ such\ that\ f(a) = b$

Negation: $for\ some\ b \in B:\ \neg(there\ \ exists\ a \in A\ such\ that\ f(a) = b)$

That is, $for\ some\ b \in B:\ for\ all\ a \in A:\ f(a) \neq b$

Thus, to show that $f: A \to B$ is not onto, we must define an element $b \in B$ and then show that there is no $a \in A$ that f sends to b.

Example 2:

Show that $f: \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x + 4$ is not onto.

Proof:

$f(a) \neq 2$ for all $a \in \mathbb{N}$.

□

The assertion that a function is onto amounts to saying no more than that its range is equal to its codomain.

Example 3:

The function $f: \mathbb{N} \to \mathbb{N}$ given by $f(x) = x + 4$ in Example 3 is not onto. The only reason it is not is that we have chosen to specify the codomain of f as $\mathbb{N}$. The range of f, $f(\mathbb{N})$, is the set $\{r \in \mathbb{N} \mid r \geq 5\}$, which we will call S. The function $h: \mathbb{N} \to S$ given by $h(x) = x + 4$ is onto. Although h is onto and f is not, the only reason h is not equal to f by definition is that the two functions have different codomains. One reason for requiring equal functions to have the same codomain is that otherwise we might have two equal functions one of which was onto and the other not.

Example 4:

The function $f: \{1,2,3\} \to \{a,b,c\}$ defined by $1 \to a$, $2 \to b$, and $3 \to a$ is not onto since f maps no element of A to the element c in the codomain of f.

Theorem 24.1 If $f: A \to B$ and $g: B \to C$ are onto, then $g \circ f$ is onto.

Proof:

Assume: 1. f onto
2. g onto

Show: $g \circ f$ onto

Observe that $g \circ f: A \to C$ by definition of composition.

1. Let $c \in C$.
.
(define a here)
.

k. $g \circ f(a) = c$
k+1. $g \circ f$ is onto. (1—k; def. onto)

Backing up from Step k, we get:

1. Let $c \in C$.
.
.
k-1. $g(f(a)) = c$
k. $g \circ f(a) = c$ (k-1; def. $\circ$)
k+1. $g \circ f$ is onto (1—k; def. onto)

Since g is onto, it will map something to c; call it b. Then $g(b) = c$. Since f is onto, it will map something to b; call it a. (We have now found a.)

1. Let $c \in C$.
2. $There\ exists\ b \in B\ such\ that\ g(b) = c$ (1, hyp. 2; def. g onto)
3. $There\ exists\ a \in A\ such\ that\ f(a) = b$ (2, hyp. 1; def. f onto)
4. $g(f(a)) = c$ (2,3; sub.)
5. $(g \circ f)(a) = c$ (4; def. $\circ$)
8. $g \circ f$ is onto (1—5; def. onto)

□

In Step 3 we "found" a by using the hypothesis that f is onto. This is the usual pattern for existence proofs.

A paragraph proof of this theorem amounts to no more than writing these steps down with a few connecting words to smooth the flow.

Proof:

Assume f and g are onto. We will show $g \circ f$ is onto. Let $c \in C$. Then, since g is onto, there exists $b \in B$ such that $g(b) = c$. Since f is onto, there exists $a \in A$ such that $f(a) = b$. Substituting, $g(f(a)) = c$, so that $(g \circ f)(a) = c$. Thus $g \circ f$ is onto.

□

Note the mention of the use of hypotheses in the proof: "since f is onto" and "since g is onto". Not all reasons are given in a paragraph proof, but it is a good idea to tell the reader just where you are using the hypotheses.

Style Rule Paragraph Proofs: It is not necessary to give all justifications in a paragraph (narrative) proof, but always say where hypotheses are used.

Recall from the last section:

Conjecture 23.2 Let $f: A \to B$ and $g: B \to C$ be functions.

(a) If $g \circ f$ is one-to-one, then f is one-to-one.

(b) If $g \circ f$ is one-to-one, then g is one-to-one.

Part (a) was proved and renumbered as Theorem 23.3; part (b) was found to be false. Our attempted proof of (b), however, can be made to "go through" if we add another hypothesis, namely, that f is onto:

Theorem 24.2 Let $f: A \to B$ and $g: B \to C$ be functions. If $g \circ f$ is one-to-one and f is onto, then g is one-to-one.

Proof: Exercise 2.

Investigation 7 Make further conjectures about the functions $f: A \to B$, $g: B \to C$, and $g \circ f: A \to C$ in terms of the conditions (used as either hypotheses or conclusions) of being one-to-one or onto. Look for statements analogous to theorems in this and the previous section. Give counterexamples for false conjectures, and then seek to add hypotheses that will make these conjectures true—in a manner analogous to Theorem 24.2. Prove your conjectures that are true.

EXERCISES

1. Let $f: A \to B$. Fill in Step 1 with a formal language statement.

   1.
   2. f is onto (1; def. onto)

2. Prove Theorem 24.2.

3. Decide and prove whether or not each of the following functions is onto:
   (a) $f: \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x + 2$
   (b) $f: \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x + 2$
   (c) $f: \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x^2$
   (d) $f: \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2$

4. Let $E = \{..., -4, -2, 0, 2, 4, 6, ...\}$ be the set of even integers, and let $O = \{..., -5, -3, -1, 1, 3, 5, ...\}$ be the set of odd integers. Define the function $f: \mathbb{Z} \to \mathbb{Z}$ by $f(x) = 3x$ if x is even and $f(x) = 5x$ if x is odd. Decide and prove whether or not f is onto.

Products, Pairs, and Definitions

The set $\{3, 5\}$ is the same as the set $\{5, 3\}$, whereas the ordered pairs $(3, 5)$ and $(5, 3)$ are different. The two ordered pairs represent different points in the coordinate plane. We would like to define the idea of an ordered pair of either numbers or elements in a set. This definition will be necessary, of course, in order for us to prove facts about ordered pairs.

The critical property we wish to establish from the definition is that the ordered pair (a, b) is the same as the ordered pair (c, d) if and only if $a = c$ and $b = d$. This property can't be considered a definition because it doesn't tell us what an ordered pair is. (We don't know formally what a set is either, but the idea in mathematics is to keep the number of undefined things to a minimum.)

Definition Let A and B be sets. For any a $\in A$, $b \in B$, the ordered pair (a,b) is the set $\{\{a\},\{a,b\}\}$.

This unlikely looking candidate for the role of ordered pair will do the job required; that is, with this definition we can prove the following theorem:

Theorem 25.1 For a_1, $a_2 \in A$ and b_1, $b_2 \in B$ we have $(a_1, b_1) = (a_2, b_2)$ iff both $a_1 = a_2$ and $b_1 = b_2$.

Proof: Exercise 7.

Theorem 25.1 embodies the property we wish to be characteristic of ordered pairs. After we use the definition above to prove Theorem 25.1, we will never have to use this definition again. It serves only to reduce the number of undefined terms. This same sort of trick can be used to define "function" in terms of sets. For this we will need the following:

Definition Let X and Y be sets. The *Cartesian product* of X and Y (denoted $X \times Y$) is the set $\{(x, y) \mid x \in X, y \in Y\}$ (also written $\{a \mid a = (x, y)\ for\ some\ x \in X, y \in Y\}$).

Example 1:

If $X = \{1, 2\}$ and $Y = \{2, 3, 4\}$, we have $\mathrm{X} \times Y = \{(1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4)\}$

Example 2:

In algebra, $\mathbb{R}$ denotes the set of real numbers. $\mathbb{R} \times \mathbb{R}$ is the set of all ordered pairs of real numbers, represented by the entire coordinate plane.

Example 3:

$A \times B = \emptyset$ iff $A = \emptyset$ or $B = \emptyset$.

Proof:

We need to prove $if\ A \times B = \emptyset,\ then\ A = \emptyset\ or\ B = \emptyset$ and also the converse of this statement. In order to show $if\ A \times B = \emptyset,\ \ then\ A = \emptyset\ or\ B = \emptyset$, we will show the contrapositive instead, namely, $if\ \neg(A = \emptyset\ or\ B = \emptyset),\ then\ A \times B \neq \emptyset$. That is, $if\ (A \neq \emptyset\ and\ B \neq \emptyset),\ then\ \ A \times B \neq \emptyset$. So assume $A \neq \emptyset\ and\ B \neq \emptyset$. Then there exists $a \in A$ and $b \in B$ so that $(a,b) \in A \times B \neq \emptyset$.

Also, to show $if\ A = \emptyset\ or\ B = \emptyset,\ then\ A \times B = \emptyset$ we again use the contrapositive: $if\ A \times B \neq \emptyset,\ then\ A \neq \emptyset\ and\ B \neq \emptyset$. Assume $A \times B \neq \emptyset$. Then there exists $(a,b) \in A \times B$ so that $a \in A$ and $b \in B$.

□

Note that the contrapositives of the two implications in Example 3 were useful since they gave us nonempty sets to work with. As an attempt at a formal definition of "function" one frequently sees the following:

Definition Let A and B be nonempty sets. A *function* f from A to B is a subset of $A \times B$ such that (1) for all $x \in A,\ y_1, y_2 \in B:$ if $(x, y_1) \in f$ and $(x, y_2) \in f$, then $y_1 = y_2$ and (2) for all $x \in A$: $(x, z) \in f$ for some $z \in B$.

If $f: A \to B$ is a function according to this definition, the pair (x, y) is in f when f is viewed as mapping x to y. Thus $(x, y) \in f$ and $f(x) = y$ mean the same thing. f must map x to a unique element y in B. Part (1) of the definition assures uniqueness by the usual scheme: we assume different names, y_1 and y_2, for the element in B to which x maps and then require $y_1 = y_2$. Part (2) assures us that the rule for mapping x applies to all elements of A.

The problem with the definition above is that it doesn't quite tell us what a function is. A function must be more than just a set of ordered pairs since, from the set of ordered pairs alone, it is not possible to determine the codomain of the function. The domain of the function may be determined as the set of all first coordinates, but if we try to determine the codomain the same way, we get that the function is onto. Using the definition above would mean that all functions were either onto or had an unspecified codomain — where it could not be determined from the definition whether or not they were onto. Since our goal is to reduce the number of undefined terms by *defining* "function", the definition above will not do. For "function" to be properly defined, all properties must follow from the definition.

To this end, we first define the ordered triple (a, b, c) as $((a, b), c)$. With this definition we can prove:

Theorem 25.2 For $a_1, a_2 \in A$, $b_1, b_2 \in B$, $c_1, c_2 \in C$, we have: $(a_1, b_1, c_1) = (a_2, b_2, c_2)$ iff $a_1 = a_2$, $b_1 = b_2$, and $c_1 = c_2$.

Proof: Exercise 8.

This makes possible the formal definition of "function":

Definition A function $f: A \to B$ is a triple (A, B, f), where f is a subset of $A \times B$ such that:

(1) for all $x \in A$, $y_1, y_2 \in B$: if $(x, y_1) \in f$ and $(x, y_2) \in f$ then $y_1 = y_2$

and (2) for all $x \in A$: $(x, z) \in f$ for some $z \in B$.

Here A is called the domain of $f: A \to B$, and B is called the codomain. From this definition, equal functions have the same codomain by Theorem 25.2.

From the definition it is easy to see the following: For any set B, there is exactly one function f from $\emptyset$ to B, corresponding to the empty subset (which is the only subset) of $\emptyset \times B$. f is one-to-one, since the defining condition is vacuously satisfied. If B is nonempty, then f is not onto. The function $f: \emptyset \to \emptyset$ is one-to-one and onto. If A is nonempty, there is no function from A to $\emptyset$.

Since we now know what a function is by definition, we can no longer define what we mean by "equal" functions. "Equal" must mean "same" according to the definition. Thus our former definition of equal functions ought to be a theorem:

Theorem 25.3 Two functions $f: A \to B$ and $g: A \to B$ are equal iff $for\ all\ x \in A:\ f(x) = g(x)$.

Proof: Exercise 10.

There will be no occasion where we will need to use the definition of function. Instead, we will appeal to Theorem 25.3 (or, equivalently, to the definition of equal functions). This parallels the situation for ordered pair, where the useful characterization is given by a theorem instead of the definition.

EXERCISES

1.
1. $(a, b) = (c, d)$
2. _____ (1; Thm. 25.1)
3. _____ (1; Thm. 25.1)

2. Let $A = \{1, 2, 3, 4\}$ and $B = \{x, y, z\}$. Find $A \times B$.

3. Let $A = \{1, 2, 3\}$ and $B = \{1, 2\}$. Find $A \times B$ and $B \times A$. Is $A \times B = B \times A$?

5. Let A and B be nonempty sets. Prove that there exists a one-to-one function from $A \times B$ onto $B \times A$.

6. Let $A,\ B,\ C$ be sets. Prove or disprove:
(a) $A \times B \cup C) = A \times B \cup A \times C$
(b) $A \times (B \cap C) = A \times B \cap A \times C$
(c) $A \times (B - C) = A \times B - A \times C$

7. Prove Theorem 25.1. The difficulty with this problem is keeping track of all the cases. Use arguments like the following: If $\{x, y\} \subseteq \{a, b\}$, then $x = a\ \ or\ \ x = b$ by definition of set containment.

8. Prove Theorem 25.2.

9. Let $A = \{1, 2, 3\}$ and $B = \{1, 2, 3\}$. For each of the following subsets f of $A \times B$, decide whether (A, B, f) is a function and, if so, whether it is one-to-one or onto.
(a) $f = \{(1, 1), (2, 2), (3, 3)\}$
(b) $f = \{(1, 1), (1, 2), (2, 3)\}$
(c) $f = \{(1, 3), (2, 1), (3, 2)\}$
(d) $f = \{(1, 1), (2, 2)\}$
(e) $f = \{(1, 2), (2, 2), (3, 2)\}$
(f) $f = \{(2, 1), (2, 2), (2, 3)\}$

10. To prove Theorem 25.3, we need to show $f = g$ iff $for\ all\ x \in A : f(x) = g(x)$. In order to avoid stumbling over notation, we can rewrite this $for\ all$ statement $for\ all\ x \in A,\ y, z \in B :\ if\ (x, y) \in f\ and\ (x, z) \in g,\ then\ y = z$. Prove Theorem 25.3 by showing this $for\ all$ statement holds iff $f = g$. Note: by definition f and g are sets.

The Rational Numbers

In order to work on computational examples in the following section, we need to enlarge our number system from the set $\mathbb{Z}$ of integers—to the set of rational numbers. The word "rational" comes from "ratio", and the rational numbers are just ratios of integers, that is, fractions and whole numbers. We denote the set of rational numbers by $\mathbb{Q}$. Since $\mathbb{Q}$ is an extension of the number systems we have already considered, we have the following axiom:

Axiom $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$

The notation $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$ is shorthand for $\mathbb{N} \subseteq \mathbb{Z}$ *and* $\mathbb{Z} \subseteq \mathbb{Q}$. The axioms that relate to addition and multiplication for $\mathbb{Z}$ also hold for $\mathbb{Q}$. Thus we have the following properties of $\mathbb{Q}$**:**

Axioms

For all a,$b \in \mathbb{Q}$: $a + b \in \mathbb{Q}$	(closure under addition)
For all a,$b \in \mathbb{Q}$: $a + b = b + a$	(commutativity of addition)
For all a,b,$c \in \mathbb{Q}$: $a + (b + c) = (a + b) + c$	(associativity of addition)
For all a,$b \in \mathbb{Q}$: $a \cdot b \in \mathbb{Q}$	(closure under multiplication)
For all a,$b \in \mathbb{Q}$: $a \cdot b = b \cdot a$	(commutativity of multiplication)
For all a,b,$c \in \mathbb{Q}$: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$	(associativity of multiplication)
For all a,b,$c \in \mathbb{Q}$: $a \cdot (b + c) = a \cdot b + a \cdot c$	(distributivity)
For all $a \in \mathbb{Q}$: $0 + a = a = a + 0$	(property of $+$ identity)
For all $a \in \mathbb{Q}$: $1 \cdot a = a = a \cdot 1$	(property of $\cdot$ identity)
For all $a \in \mathbb{Q}$: $a + b = 0$ $for\ some\ b \in \mathbb{Q}$	(existence of $+$ inverse)

The additive inverse of the rational number a, denoted by -a, is unique. The proof is exactly the same as the proof for the integers. The axioms for $\mathbb{Z}$ analogous to those above are subsumed under those above; that is, since the axioms above hold for all elements of $\mathbb{Q}$, they hold also for the subset $\mathbb{Z}$ of $\mathbb{Q}$—so the analogous axioms for $\mathbb{Z}$ can be replaced by those above. The other axioms for $\mathbb{Z}$ and $\mathbb{N}$ (such as closure and trichotomy) don't follow from those above, however, so we need to carry these axioms (about subsets of $\mathbb{Q}$) forward.

In $\mathbb{Q}$ we have an additional axiom, which asserts that a nonzero element has a multiplicative inverse:

Axiom For each $a \in \mathbb{Q}$ such that $a \neq 0$, there exists $b \in \mathbb{Q}$ such that $a \cdot b = 1$

The element b in the axiom above is called the multiplicative inverse of a. It is uniquely determined, as the next theorem asserts.

Theorem 26.1 For each rational number a, not equal to zero, there exists a unique $b \in \mathbb{Q}$ such that $a \cdot b = 1$.

Proof: Exercise 1.

Subtraction is defined for rational numbers exactly as it is for the integers:

Definition For $a, b \in \mathbb{Q}$, the difference $a - b$ is defined to be a plus the additive inverse of b, symbolically: $a - b = a + \text{-}b$.

The expression $a - b$ is read "a minus b", and the operation "$-$" between rational numbers is called *subtraction.*

Definition For any a,$b \in \mathbb{Q}$, where $b \neq 0$, the quotient (or ratio) a/b is defined to be a multiplied by the multiplicative inverse of b.

The expression a/b is read "a divided by b" or "a over b", and the operation "$/$" between rational numbers is called division.

Example 4:

For any $b \neq 0$, $1/b$ is 1 times the multiplicative inverse of b, and is therefore the multiplicative inverse of b itself. This gives us a way to denote the multiplicative inverse of b.

Multiplication by the natural number 5 can be interpreted as taking 5 copies of something. In particular, since $5 \cdot (1/5) = 1$ (by the definition of multiplicative inverse), 5 copies of $1/5$ gives 1, so that $1/5$ must be less than 1 (five times less, in fact). $1/4$ is also less than one, but since only 4 copies of $1/4$ produce 1, $1/4$ is greater than $1/5$. In general, for natural numbers a and b, if $a < b$, then $1/b < 1/a$.

We have yet to give a formal definition of $<$ for $\mathbb{Q}$. We want the definition we do give to satisfy the following conditions: (1) the relation $<$ on $\mathbb{Q}$ should be the same as our previous relation, when we consider elements in the subsets $\mathbb{N}$ and $\mathbb{Z}$ of $\mathbb{Q}$, and (2) for natural numbers a and b, if $a < b$, then we want $1/b < 1/a$.

Recall the following definition of $<$ for the integers:

For a,$b \in \mathbb{Z}$, $a < b$ iff $b - a \in \mathbb{N}$.

The same definition won't work for extending $<$ from $\mathbb{Z}$ to $\mathbb{Q}$, since the difference between two rational numbers need not be a whole number. In order to make a similar definition, we define the following subset of $\mathbb{Q}$:

Definition Define $\mathbb{Q}^+ = \{x \in \mathbb{Q} \mid x = a/b \ for\ some\ a, b \in \mathbb{N}\}$. $\mathbb{Q}^+$ is called the subset of positive rational numbers.

Example 5:

$5 \in \mathbb{Q}^+$, since $5 = 5/1$. $3/7 \in \mathbb{Q}^+$, and $17/5 \in \mathbb{Q}^+$. The elements of $\mathbb{Q}^+$ are the positive fractions and whole numbers.

Definition For $a, b \in \mathbb{Q}$, define $a < b$ iff $there\,exists\ x \in \mathbb{Q}^+\ such\,that\ b = a + x$. Equivalently, $a < b$ iff $b - a \in \mathbb{Q}^+$.

If a and b are in the subset $\mathbb{Z}$ of $\mathbb{Q}$, then this definition agrees exactly with the definition of $a < b$ that we already have. In order to prove this, we need to show that for $a, b \in \mathbb{Z}$: ($b - a \in \mathbb{Q}^+$ iff $b - a \in \mathbb{N}$). You are asked to do this as Exercise 5. It is a corollary to Theorem 26.2.

Theorem 26.2 $\mathbb{Q}^+ \cap \mathbb{Z} = \mathbb{N}$

Proof: Exercise 3.

Theorem 26.3 For $a, b \in \mathbb{N}$, if $a < b$, then $1/b < 1/a$.

Proof: Exercise 4.

The axioms we have so far for $\mathbb{Q}$ apply to the larger real and complex number systems, as well as the rational numbers. If we wish our axiom system for the rational numbers to be specific for that system, we need to introduce another axiom that will insure that the system is not too large; that is, that it contains the positive and negative whole numbers and fractions, but nothing else. The following axiom does just this.

Axiom Trichotomy for $\mathbb{Q}$: For any $a \in \mathbb{Q}$, exactly one of the following holds: (1) $a = 0$, (2) $a \in \mathbb{Q}^+$, (3) -$a \in \mathbb{Q}^+$.

The following definition repeats for the rational numbers, definitions that we have already for the integers:

Definition For $a, b \in \mathbb{Q}$, define

(a) $a > b$ iff $b < a$

(b) $a \leq b$ iff $a < b$ *or* $a = b$

(c) $a \geq b$ iff $a > b$ *or* $a = b$

Theorem 26.4 For any a,$b \in \mathbb{Q}$, exactly one of the following holds: (1) $a < b$, (2) $a = b$, (3) $a > b$.

Proof: Exercise 6.

Investigation 8 Using previous theorems about the integers as a guide, make up analogous theorems for the rational numbers. Prove the theorems that you have made up.

Recall that the natural number 1 is defined as the identity of multiplication—given by an axiom. The numbers 2, 3, 4, and so on are defined as $2 = 1 + 1$, $3 = 2 + 1$, $4 = 3 + 1$, and so on. The axioms that we have so far for $\mathbb{N}$ hold for larger number systems; that is, there is no axiom that *limits* the set $\mathbb{N}$ to these numbers. The following theorem states that $\mathbb{N}$ is limited to numbers so defined.

Theorem 26.5 For every natural number n: $(n = 1)\, or\, (there\, exists\, k \in \mathbb{N}\, such\, that\, n = k + 1)$.

EXERCISES

1. Prove Theorem 26.1

2. Show that the two forms of the definition of $<$ for $\mathbb{Q}$ are equivalent, that is, show for a,$b \in \mathbb{Q}$, $there\,exists\, x \in \mathbb{Q}^+\ such\, that\, b = a + x$ iff $b - a \in \mathbb{Q}^+$.

3. Prove Theorem 26.2.

4. Prove Theorem 26.3.

5. Prove that for a,$b \in \mathbb{Z}$, $b - a \in \mathbb{Q}^+$ iff $b - a \in \mathbb{N}$.

6. Prove Theorem 26.4.

7. Give rules for addition, subtraction, multiplication , and division of rational numbers, in terms of integers; that is, for integers a, b, c, d, fill in the boxes below with integers given in terms of a, b, c, d. Prove your results.

$$\tfrac{a}{b} + \tfrac{c}{d} = \tfrac{\square}{\square}$$

$$\tfrac{a}{b} - \tfrac{c}{d} = \tfrac{\square}{\square}$$

$$\tfrac{a}{b} \cdot \tfrac{c}{d} = \tfrac{\square}{\square}$$

$$\tfrac{a}{b} \div \tfrac{c}{d} = \tfrac{\square}{\square}$$

Induction

Consider the following way to add all the numbers from 1 to 100: add 1 and 100, to get 101, then add 2 and 99, again to get 101, then 3 plus 98 again gives 101. There are just 50 such pairs of numbers, the last being 50 plus 51. All pairs sum to 101. So the correct sum is $50 \cdot 101 = 5050$.

In general we wish to find the sum of the first n natural numbers:

$$1 + 2 + 3 + 4 + ... + (n-1) + n$$

If there are an even number of numbers, then there are $n/2$ pairs, such as 1 plus n, and 2 plus $(n-1)$. Each of the pairs sums to $n+1$, so

$$1 + 2 + 3 + 4 + ... + (n-1) + n = (n+1) \cdot n/2$$

If there are an odd number of numbers, then the number in the center of the list is $(n+1)/2$, $n-1$ is even, and there are $(n-1)/2$ pairs that remain if we delete the number $(n+1)/2$ from the center of the list. Each of the remaining pairs, such as 1 and n, and 2 and $(n-1)$, sum to $n+1$. Therefore the sum of the paired elements is $(n+1) \cdot (n-1)/2$. If we add the deleted center element we get $(n+1) \cdot (n-1)/2 + (n+1)/2$. By the distributive property

$$(n+1) \cdot (n-1)/2 + (n+1)/2 = [(n-1)+1] \cdot (n+1)/2 = n(n+1)/2$$

which is the same sum that we get in the case with an even number of terms.
Thus for all natural numbers n, we have

$$1 + 2 + 3 + 4 + ... + (n-1) + n = (n+1) \cdot n/2$$

There is a very powerful idea in mathematics, called *mathematical induction*, that lets us prove statements of the form $for\ all\ n \in \mathbb{N} : \mathcal{P}(n)$. Induction has theoretical, as well as computational uses, and its computational uses enable us to prove things for which there are no easy methods. In order to introduce the idea in a simple context, however, we illustrate the use of induction by proving statements like the formula above for the sum of the first n natural numbers.

The left hand side of this formula is an expression for the sum of the first n natural numbers. For the values 1, 2, and 3 for n, we get the following interpretation of the sum:

$$\begin{array}{lll} n=1: & 1+2+3+4+...+(n-1)+n = 1 & = 1 \\ n=2: & 1+2+3+4+...+(n-1)+n = 1+2 & = 3 \\ n=3: & 1+2+3+4+...+(n-1)+n = 1+2+3 & = 6 \end{array}$$

Let $\mathcal{P}(n)$ be the statement $1 + 2 + 3 + 4 + ... + n - 1 + n = (n+1) \cdot n/2$. Then

$\mathcal{P}(1)$ is the statement $1 = (1+1) \cdot 1/2$

$\mathcal{P}(2)$ is the statement $1+2 = (2+1) \cdot 2/2$

$\mathcal{P}(3)$ is the statement $1+2+3 = (3+1) \cdot 3/2$

Notice that these statements are all true.

Inference Rule Mathematical Induction: In order to prove a statement of the form $for\ all\ n \in \mathbb{N} : \mathcal{P}(n)$ by induction, first show that $\mathcal{P}(1)$ is true, then assume that $\mathcal{P}(n)$ is true for an arbitrary n, and show that $\mathcal{P}(n+1)$ is true.

Example 1:

The following assertion holds for all $n \in \mathbb{N}$:

$$(1) \qquad 2 + 4 + 6 + ... + (2n) = n(n + 1)$$

If $n \in \mathbb{N}$, then $2n$ is an even natural number. The expression $2 + 4 + 6 + ... + (2n)$ means the sum of all even numbers up to and including $2n$. If $n = 1$, then the expression is taken to mean just 2 (or equivalently, $2n$) since 2 is the only even number up to 2.

Proof of (1):

First we verify that (1) is true for $n = 1$: $2 = 1(1 + 1)$ is true.
For the second part of he proof,

Assume: $n \in \mathbb{N}$

$$2 + 4 + 6 + ... + (2n) = n(n + 1)$$

Show: $2 + 4 + 6 + ... + (2(n + 1)) = (n + 1)((n + 1) + 1)$

By adding $2n + 2$ to each side of the expression in the hypothesis, we get:

$$2 + 4 + 6 + ... + (2n) + 2(n + 1) = n(n + 1) + 2(n + 1)$$

or $2 + 4 + 6 + ... + (2n) + 2(n + 1) = (n + 1)(n + 2)$

or $2 + 4 + 6 + ... + (2n) + 2(n + 1) = (n + 1)((n + 1) + 1)$

□

Note that the conclusion is exactly the same as the hypothesis, except that every occurrence of n is replaced by $n + 1$.

A proof done according to the preceding scheme is said to be a proof "by induction on n". The same scheme will work for the straightforward exercises at the end of this section. Thus a proof by induction consists of two parts: (1) showing that the assertion holds for $n = 1$ and (2) showing that, if the assertion is true for an arbitrary n, then it is true for $n + 1$. In proving (2), many people find it convenient to use slightly different notation: we assume the truth of the assertion for n, let $k = n + 1$, and then show that the assertion holds for k. Thus the statement to be shown in (2) has exactly the same form as the statement assumed except that k has replaced n. In proving (1), the number 1 is substituted for n. For example, a proof of Example 1 (by induction) would take the following form:

First, show: $2 = 1(1 + 1)$

Proof: Definition of 2 (as $1 + 1$), and identity for multiplication.

Second:

Assume: $2 + 4 + 6 + ... + (2n) = n(n + 1)$

$$k = n + 1$$

Show: $2 + 4 + 6 + ... + (2k) = k(k + 1)$

By adding $2n + 2$ to each side of the expression in the hypothesis, we get:

$$2 + 4 + 6 + \ldots + (2n) + 2(n + 1) = n(n + 1) + 2(n + 1)$$

or $\quad 2 + 4 + 6 + \ldots + (2n) + 2(n + 1) = (n + 1)(n + 2)$

or $\quad 2 + 4 + 6 + \ldots + (2n) + 2(n + 1) = (n + 1)((n + 1) + 1)$

or $\quad 2 + 4 + 6 + \ldots\ldots\ldots\ldots + (2k) = (k)(k + 1)$ by substitution.

□

Example 2:

Suppose that x and y are positive integers with $x < y$. Prove that $for\ all\ n \in \mathbb{N} :\ x^n < y^n$.

Proof:

By induction on n: First $n = 1$: Show: $x^1 < y^1$
Proof: By hypothesis.

Next,

Assume: $x^n < y^n$

$k = n + 1$

Show: $x^k < y^k$

It is frequently helpful to do the first few cases ($n = 2, 3,$ or 4) to get an idea of how to proceed in general:

$n = 2$: $x < y$

$x^2 < yx,\ xy < y^2$, so that $x^2 <\ y^2$

$n = 3$: $x^2 < y^2$, so that $x^3 < y^2x$

$x < y,$ so that $xy^2 < y^3,$ so that $x^3 < y^3$

$x < y,$ so that $xy^n < y^{n+1}$	(multiplying both sides by y^n; y^n is positive by Exercise 6)
$x^n < y^n$, so that $x^{n+1} < y^n x$	(multiplying both sides by x)
therefore $x^{n+1} < y^{n+1}$	(transitivity of $<$)
that is, $x^k < y^k$	

□

The validity of the inference rule for doing proofs by induction follows from the following axiom. We have given it as a rule, since a rule is a more obvious guide in doing proofs than is the use of an axiom.

Axiom Induction: Let S be a subset of $\mathbb{N}$ that has the following two properties:

(1) $1 \in S$

(2) for all $n \in \mathbb{N}$: if $n \in S$, then $n + 1 \in S$.

Then $S = \mathbb{N}$.

From the axiom, we can see that the inference rule is valid. For, given any proposition $\mathcal{P}(n)$ involving the natural number n, let S be the set of all natural numbers for which $\mathcal{P}(n)$ is true. If we establish $\mathcal{P}(1)$ according to the inference rule, then $1 \in S$, so condition (1) of the axiom is satisfied. If we assume the truth of $\mathcal{P}(n)$ for an arbitrary $n \in \mathbb{N}$, and can show $\mathcal{P}(n+1)$ as the inference rule dictates, then we have proved "for all $n \in \mathbb{N}$: if $n \in S$, then $n + 1 \in S$", so condition (2) of the axiom is satisfied. From the assertion of the axiom, then, $S = \mathbb{N}$, and this says that $\mathcal{P}(n)$ is true for all $n \in \mathbb{N}$, by the definition of S. Thus it follows from the axiom that the inference rule gives a valid way of proving $\mathcal{P}(n)$ for all $n \in \mathbb{N}$.

Our next use of induction is to prove a theoretical result: Theorem 27.6, the "division algorithm". An algorithm is a fixed procedure for calculating some mathematical quantity, for example, the procedure of "long division". The division algorithm comes in two versions: (1) division of numbers to get a decimal to any desired degree of accuracy, and (2) division of whole numbers to get a whole number quotient and a whole number remainder. Here we will be concerned exclusively with the latter.

Example 3:

We wish to divide 14 by 3. The idea is first to find the largest number less than or equal to 14 that is a multiple of 3. This number is $12 = 4 \cdot 3$. We then subtract 12 from 14 to get the remainder 2. Then we write $14 = 4 \cdot 3 + 2$. In this expression, 4 is the quotient. Given an integer, such as 14, that we wish to divide by another integer, such as 3, the division algorithm produces a quotient and a remainder.

Theorem 27.6 Division Algorithm: Let a and b be integers, with $b > 0$. Then there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.

Theorem 27.6 is known itself as the division algorithm, although it is not really an algorithm but identifies the relationship that holds for the quantities q and r, which are determined by the algorithm.

Proof:

We first show the existence part for positive a by induction on a. If $a = 1$, we have: Case 1, $b = 1$: $1 = 1 \cdot 1 + 0$. Case 2 $b > 1$: $1 = 0 \cdot b + 1$. Therefore the existence of q and r is shown when $a = 1$.

Now let $a = n$ and assume existence of q and r, that is, $n = qb + r$ for $0 \leq r < b$. Hence $n + 1 = qb + r + 1$. If $r + 1 < b$, then $n + 1 = qb + r'$ where $0 \leq r' < b$. Otherwise $r + 1 = b$ so that $n + 1 = (q + 1)b + 0$ and again $n + 1 = qb + r'$ where $0 \leq r' < b$. It follows that q and r exist when $a = n + 1$. By induction, existence is shown for all positive integers.

We next show the existence part for negative a and $a = 0$. Case 1, $a = 0$: $0 = 0 \cdot b + 0$. Case 2, $a < 0$: By part (a) $-a = qb + r$ for $0 \leq r < b$ so that $a = (-q)b + (-r)$. If $r = 0$, we are done. Otherwise $0 < r < b$ so that $0 > -r > -b$ and $b > b - r > b - b$. Here $a = (-q - 1)b + (b - r)$ and we are also done.

Finally we show uniqueness:

Assume: $q_1 b + r_1 = q_2 b + r_2$ for $0 \leq r_1, r_2 < b$.

Show: $q_1 = q_2$ and $r_1 = r_2$

Case 1, $r_1 = r_2$: Here $q_1 b = q_2 b$ so that $q_1 = q_2$ by Theorem 32.5b.

Case 2, (without loss of generality $0 \leq r_1 < r_2 < b$: Here $q_1 b + r_1 = q_2 b + r_2$ so that $(q_1 - q_2)b = r_2 - r_1$. Since b is positive and $r_2 - r_1$ is positive, $q_1 - q_2$ is positive. By Exercise 6b, $(q_1 - q_2)b \geq b$, but $b > r_2 - r_1$ so that $(q_1 - q_2)b > r_2 - r_1$ contradicting $(q_1 - q_2)b = r_2 - r_1$. Hence this case leads to a contradiction. Therefore Case 1, $r_1 = r_2$, must hold, and from this it follows that $q_1 = q_2$.

□

EXERCISES

Prove the following by induction on n:

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

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

3. $1 + 3 + 9 + ... + 3^n = \frac{3^{n+1}-1}{2}$.

4. $1^2 + 2^2 + 3^2 + ... + n^2 = \frac{1}{6}n(n + 1)(2n + 1)$.

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

6. Suppose $y \in \mathbb{Z}$ and $y > 0$. Prove:
   (a) for all $n \in \mathbb{N}$: $y^n > 0$
   (b) for all $n \in \mathbb{N}$: $ny \geq y$

7. Prove $n < 2^n$ for all $n \in \mathbb{N}$.

8. Let $A = \{x \in \mathbb{N} \mid (x = 1)\ or\ (x = y + 1\ for some\ y \in \mathbb{N})\}$. Use the induction axiom to show that $A = \mathbb{N}$. Conclude that $1 \leq n\ for all\ n \in \mathbb{N}$ and that there is no integer between 0 and 1. Show that there is no integer between 1 and 2. Can you generalize?

Primes, Divisors, and Multiples in $\mathbb{N}$

Prime numbers can be considered in the context of either the integers or the natural numbers. The former approach is the more powerful, and leads to easier deductive access to the theorems of elementary *number theory*. The approach is, however, more abstract than we wish the present text to be. Theorems about the topics we consider here are found in Volume 3 of the series—which is written at a higher level. The present treatment is descriptive—not deductive. That is, we will make some definitions and do some computations, but there will be no significant theorems. Our definitions will be made in the context of the natural numbers, since it is the simplest. Before we restrict attention to the natural numbers, however, we will say something briefly about how things work in the integers.

Certain of the axioms relating addition and multiplication in $\mathbb{Z}$ are exactly the same as those relating addition and multiplication in $\mathbb{Q}$. Any set on which there are two operations satisfying these axioms is called a commutative *ring*. Since the axioms hold in $\mathbb{Z}$ and $\mathbb{Q}$, $\mathbb{Z}$ and $\mathbb{Q}$ are examples of commutative rings[12]. $\mathbb{N}$ is not a commutative ring since, for example, there is no additive identity, nor do elements have additive inverses. (Elements in a ring may have, but need not have, multiplicative inverses.)

In a ring, divisors of the multiplicative identity 1 are called *units*. Since $(\text{-}1) \cdot (\text{-}1) = 1$ and $1 \cdot 1 = 1,$ both 1 and -1 are divisors of 1, and are therefore units in $\mathbb{Z}$. In fact, 1 and -1 are the only units in $\mathbb{Z}$. In $\mathbb{Q}$, since every nonzero element has a multiplicative inverse, every nonzero element is a unit. Thus in $\mathbb{Z}$ there are elements that are neither zero nor units, but this is not true for $\mathbb{Q}$. In a ring, an element a is called *irreducible* iff whenever $a = bc$ (for some b and c in the ring), we have that either b or c is a unit. Thus 7 is an irreducible element of $\mathbb{Z}$, since if we had $7 = bc$, then either $b = \pm 1$ and $c = \pm 7$, or $c = \pm 1$ and $b = \pm 7$—so that either b or c is a unit. The integer 6, however, is not irreducible, since $6 = 2 \cdot 3$, but neither 2 nor 3 is a unit.

In a ring, an element a is called *prime* iff whenever a divides a product bc, then a must divide either b or c. In $\mathbb{Z}$, for example, the number 6 is *not* prime since 6 divides $9 \cdot 4$ or 36, but 6 does not divide 9, nor does it divide 4. The number 7 *is* prime in $\mathbb{Z}$, since any time 7 divides a product bc, it must divide one of the factors b or c.

Although there are rings (sets that satisfy the axioms) for which prime and irreducible elements are sometimes different, it can be proved that in $\mathbb{Z}$ any number is prime iff it is irreducible. (This is, however, not an elementary result.) The definition of *prime* that we give for natural numbers could be either the definition above of prime for rings, or the definition of irreducible—since these ideas are equivalent for natural numbers. The easier, and most widely seen, definition for primality in the natural numbers is actually the ring-theoretic definition of irreducibility. It is the definition people used for the two thousand years preceding the definition of the integers.

Definition A natural number is called *prime* iff its only divisors (in $\mathbb{N}$) are 1 and itself.

A natural number that is not prime and not 1 (that is, not a unit) is called *composite*.

[12] The set of polynomials in x is another example of a commutative ring.

Example 1:

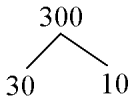
$6 = 2 \cdot 3$ so that 2 and 3 are divisors of 6. Thus 6 is composite. 7 is prime, having only 1 and 7 as divisors

Any composite number can be written as a product of its prime divisors. (Recall that a divisor is also called a *factor*).

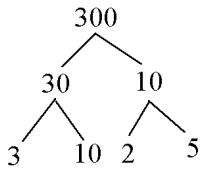
Example2:

Write 300 as a product of its prime factors.

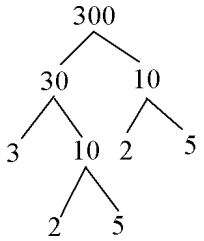
We begin by writing 300 as a product of two of its factors: $300 = 30 \cdot 10$. This is done in the following beginning of a "factorization tree".



Next, we write both 30 and 10 as products of their factors:



The numbers 3, 2, and 5 are prime, and cannot be factored further. However, 10 can be factored into 2 times 5:



Thus $300 = 3 \cdot 2 \cdot 5 \cdot 2 \cdot 5$. The prime factors of a number are usually listed in order of increasing size: $300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5$. Also, it is customary to use exponential notation for repeated factors. Thus $300 = 2^2 \cdot 3 \cdot 5^2$.

It is possible to generate a list of all the factors of a number, by taking all combinations of exponents not exceeding the exponents in the prime factorization.

Example 3:

Find all the factors of 300.

Solution:

$2^2 \cdot 3^1 \cdot 5^2 = 300$ $\quad$ $2^2 \cdot 3^1 \cdot 5^1 = 60$ $\quad$ $2^2 \cdot 3^1 \cdot 5^0 = 12$

$2^1 \cdot 3^1 \cdot 5^2 = 150$ $\quad$ $2^1 \cdot 3^1 \cdot 5^1 = 30$ $\quad$ $2^1 \cdot 3^1 \cdot 5^0 = 6$

$2^0 \cdot 3^1 \cdot 5^2 = 75$ $\quad$ $2^0 \cdot 3^1 \cdot 5^1 = 15$ $\quad$ $2^0 \cdot 3^1 \cdot 5^0 = 3$

$2^2 \cdot 3^0 \cdot 5^2 = 100$ $\quad$ $2^2 \cdot 3^0 \cdot 5^1 = 20$ $\quad$ $2^2 \cdot 3^0 \cdot 5^0 = 4$

$2^1 \cdot 3^0 \cdot 5^2 = 50$ $\quad$ $2^1 \cdot 3^0 \cdot 5^1 = 10$ $\quad$ $2^1 \cdot 3^0 \cdot 5^0 = 2$

$2^0 \cdot 3^0 \cdot 5^2 = 25$ $\quad$ $2^0 \cdot 3^0 \cdot 5^1 = 5$ $\quad$ $2^0 \cdot 3^0 \cdot 5^0 = 1$

It is frequently necessary to know the greatest common factor for two numbers. If the numbers aren't large, this can be found by determining the sets of all factors of each number, and then finding the greatest one they have in common.

Example 4:

Find the greatest common factor of 36 and 50.

Solution:

Using factorization trees, first obtain the prime factorizations of both 36 and 30. (The figures are omitted.) We get: $36 = 2^2 \cdot 3^2$ and $30 = 2 \cdot 3 \cdot 5$. We then generate lists of all the factors of 36 and 30:

Factors of 36	Factors of 30
$2^2 \cdot 3^2 = 36$	$2^1 \cdot 3^1 \cdot 5^1 = 30$
$2^1 \cdot 3^2 = 18$	$2^0 \cdot 3^1 \cdot 5^1 = 15$
$2^0 \cdot 3^2 = 9$	$2^1 \cdot 3^0 \cdot 5^1 = 10$
$2^2 \cdot 3^1 = 12$	$2^0 \cdot 3^0 \cdot 5^1 = 5$
$2^1 \cdot 3^1 = 6$	$2^1 \cdot 3^1 \cdot 5^0 = 6$
$2^0 \cdot 3^1 = 3$	$2^0 \cdot 3^1 \cdot 5^0 = 3$
$2^2 \cdot 3^0 = 4$	$2^1 \cdot 3^0 \cdot 5^0 = 2$
$2^1 \cdot 3^0 = 2$	$2^0 \cdot 3^0 \cdot 5^0 = 1$
$2^0 \cdot 3^0 = 1$	

By inspection, we see that $\{1, 2, 3, 6\}$ is the set of common factors for 36 and 30. Thus 6 is the greatest common factor.

Suppose we wish to find the greatest common factor n of numbers a and b. It's not necessary to actually list the sets of factors for each of a and b. Instead, we seek the prime factorization of n. Since n is found in the list of factors of a, it is expressed as a product of the prime factors of a to some powers. The powers in the factorization of n can't exceed the powers in the factorization of a. Similarly, n must be also expressed as a product of powers of the prime factors of b.

Example 5:

Let n be the greatest common factor of 30 and 36. Find n by determining its prime factorization.

Solution:

Since it occurs in the list of factors of 36, n is of the form $2^j \cdot 3^k$ for some $j, k,$. It is also of the form $2^r \cdot 3^s \cdot 5^t$, for some $r, s, t,$ since it occurs in the list of factors of 30. Since it occurs in the first list, the exponent of 5 must be zero. Since it occurs in the second list, the exponents of 2 and 3 must be less than or equal to 1. In order that n be the *greatest* of the common factors, the exponents of 2 and 3 should be as large as possible—subject to the constraints above. Thus the exponents of 2 and 3 are both 1. Thus $n = 2^1 \cdot 3^1 = 6$.

Example 6:

Let $a = 2^2 \cdot 3 \cdot 5^3 \cdot 11$ and $b = 2 \cdot 3^2 \cdot 5^2 \cdot 7^2$ be given in terms of their prime factorizations, and let n be the greatest common factor of a and b. Find n in terms of its prime factorization.

Solution:

We can simplify notation by using zero as an exponent to describe the prime factorizations of a and b. Thus $a = 2^2 \cdot 3^1 \cdot 5^3 \cdot 7^0 \cdot 11^1$ and $b = 2^1 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 11^0$. Then n has a prime factorization involving these primes, where for each prime the exponent is as large as possible

subject to the constraint that it can't be larger than the exponent in the factorization of a or of b. Thus $n = 2^1 \cdot 3^1 \cdot 5^2 \cdot 7^0 \cdot 11^0$.

The method of Example 6 can be summarized in general as follows:

Procedure In order to find the greatest common divisor n of natural numbers a and b, write a and b in terms of their prime factorizations. Use zero as an exponent, when necessary, so as to write a and b in terms of the same prime numbers. Then n has a prime factorization involving the same set of primes, where the exponent for each prime is found by taking the *minimum* of the exponents for that prime in the factorizations of a and b.

There is a method, called the *Euclidean algorithm*, for calculating the greatest common factor of two numbers, without finding their prime factorizations: Suppose we wish to find the greatest common factor n of a and b. Suppose also (without loss of generality) that $a < b$. By the division algorithm, $b = q_1 a + r_1$ where $0 \leq r_1 < a$. Now use the division algorithm to divide a by the remainder r_1 to obtain a second, smaller remainder r_2: $a = q_2 r_1 + r_2$, where $0 \leq r_2 < r_1$. Then divide the first remainder by the second, to get a third. Then divide the second by the third to get a fourth, and so on, until we get a remainder of zero:

$$b = q_1 a + r_1, \text{ where } 0 < r_1 < a$$

$$a = q_2 r_1 + r_2, \text{ where } 0 < r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3, \text{ where } 0 < r_3 < r_2$$

$$r_2 = q_4 r_3 + r_4, \text{ where } 0 < r_4 < r_3$$

.

.

$$r_{k-2} = q_k r_{k-1} + r_k, \text{ where } 0 < r_k < r_{k-1}$$

$$r_{k-1} = q_{k+1} r_k + 0$$

We claim that r_k, the last nonzero remainder, is the greatest common factor n of a and b. To see this, first observe that since $n \mid a$ and $n \mid b$, $n \mid r_1$, by Theorem 7.1 and the first equation. Then since $n \mid a$ and $n \mid r_1$, $n \mid r_2$, by Theorem 7.1 and the second equation. We continue in this manner to find that n divides all the remainders in the sequence. Thus $n \mid r_k$.

From the last equation, $r_{k-1} = q_{k+1} r_k + 0$, we see that r_k divides r_{k-1}. From the equation $r_{k-2} = q_k r_{k-1} + r_k$, we see that r_k must also divide r_{k-2}. From the preceding division r_k must also divide r_{k-3}, and so on. Thus r_k divides all the remainders and b and a. Thus r_k is a common divisor of a and b. Since n is by definition the greatest common divisor, we have $r_k \leq n$. Since also $n \mid r_k$, we have that $n = r_k$. That is, the greatest common divisor of $a$and b is the last nonzero remainder that we get in the process of dividing by successive remainders.

Example 7:

Use the Euclidean algorithm to find the greatest common factor of 675 and 1800.

Solution:

Dividing 1800 by 675 gives: $1800 = 2 \cdot 675 + 450$.
Dividing 675 by 450 gives: $675 = 1 \cdot 450 + 225$.
Dividing 450 by 225 gives: $450 = 2 \cdot 225 + 0$.
Since 225 is the last nonzero remainder, it is the greatest common factor of 1800 and 675.

The *least common multiple* of a and b is, as its name suggests, the smallest of all the multiples that a and b have in common.

Example 8:

Find the least common multiple of 12 and 18.

Solution:

The set of multiples of 12 is $\{12, 24, 36, 48, 60, 72, 84, 96, 108, 120, \ldots\}$.
The set of multiples of 18 is $\{18, 36, 54, 72, 90, 108, 126, 144, 162, 180, \ldots\}$.
The set of common multiples will be the intersection of the two sets above: $\{36, 72, 108, 144, \ldots\}$.
The least common multiple is the smallest element in this set, namely, 36.

It is easier to find the least common multiple of two numbers in terms of its prime factorization than by listing all multiples of the numbers. For example, 12 has the prime factorization $12 = 2^2 \cdot 3^1$ and 18 has the prime factorization $18 = 2^1 \cdot 3^2$. If m is the least common multiple of 12 and 18, then m must contain all the factors of 12 (2 as a factor twice, and 3 once), and all the factors of 36 (2 as a factor once, and 3 twice). Any multiple of 12 will contain at least two factors of 2 and one factor of 3. Any multiple of 18 will contain one factor of two and two factors of 3. The common multiples of 12 and 18 are therefore the numbers that contain at least two factors of 2 and two factors of 3. The least common multiple contains exactly (no more than what is necessary) two factors of 2 and two factors of 3.

Procedure

In order to find the least common multiple m of natural numbers a and b, write a and b in terms of their prime factorizations. Use zero as an exponent, when necessary, so as to write a and b in terms of the same prime numbers. Then m has a prime factorization involving the same set of primes, where the exponent for each prime is found by taking the *maximum* of the exponents for that prime in the factorizations of a and b.

Example 9:

Let $a = 2^2 \cdot 3 \cdot 5^3 \cdot 11$ and $b = 2 \cdot 3^2 \cdot 5^2 \cdot 7^2$ be given in terms of their prime factorizations, and let m be the greatest common factor of a and b. Find m in terms of its prime factorization.

Solution:

We simplify notation by using zero as an exponent to describe the prime factorizations of a and b. Thus $a = 2^2 \cdot 3^1 \cdot 5^3 \cdot 7^0 \cdot 11^1$ and $b = 2^1 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 11^0$. Then n has a prime factorization involving these primes, where for each prime the exponent is as small as possible subject to the constraint that it can't be smaller than the exponents in either factorization of a or of b. Thus $m = 2^2 \cdot 3^2 \cdot 5^3 \cdot 7^2 \cdot 11^1$.

Project

For numbers a and b, calculate the product ab, the least common multiple of a and b, and the greatest common factor of a and b. How are these related? Start with small numbers as examples of a and b in your calculations, and then work up to larger examples. Once you have found a relationship, try to verify it—at least informally. The product of a and b can also be found in terms of prime factorizations by the rule that to multiply powers, we add exponents.

The least common multiple of two numbers has application as the “least common denominator”, when we add fractions.

Example 10:

Add $\frac{1}{12}$ and $\frac{5}{18}$.

Solution:

By Example 2, the least common multiple of 12 and 18 is 36. Thus to add $\frac{1}{12}$ and $\frac{5}{18}$, we change both fractions to have denominator 36: $\frac{1}{12} = \frac{3}{3} \cdot \frac{1}{12} = \frac{3}{36}$, and $\frac{5}{18} = \frac{2}{2} \cdot \frac{5}{18} = \frac{10}{36}$. Therefore $\frac{1}{12} + \frac{5}{18} = \frac{3}{36} + \frac{10}{36} = \frac{1}{36} \cdot (3 + 10) = \frac{1}{36} \cdot 13 = \frac{13}{36}$, by the distributive property.

A Computational Practice Test

Problem 1 Count the first sixteen natural numbers
(a) in base ten
(b) in base four
(c) in base twelve

Solution (a) $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16$
(b) $1, 2, 3, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33, 100,$
(c) $1, 2, 3, 4, 5, 6, 7, 8, 9, T, E, 10, 11, 12, 13, 14$

Problem 2 Express 384 in expanded notation

Solution $3 \times (ten)^2 + 8 \times (ten)^1 + 4 \times (ten)^0$ [or $3 \times (ten)^2 + 8 \times (ten) + 4$]

Problem 3 Express 354_{six} in expanded notation

Solution $3 \times (six)^2 + 5 \times (six)^1 + 4 \times (six)^0$ [or $3 \times (six)^2 + 5 \times (six) + 4$]

Problem 4 Express 354_{six} in base ten

Solution
$3 \times (six)^2 + 5 \times (six)^1 + 4 \times (six)^0$
$= 3 \times 36 + 5 \times 6 + 4$
$= 108 + 30 + 4 = 142$

Problem 5 Express 354 in base four

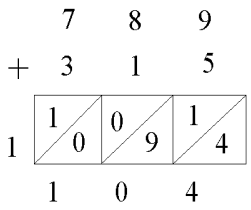
Solution
$4^5 = 1024 > 354$.
$4^4 = 256 < 354$
By the division algorithm: $354 = 1 \cdot 256 + 98 = 1 \times 4^4 + 98$.
$4^3 = 64 < 98$
By the division algorithm: $98 = 1 \cdot 64 + 34$
so $354 = 1 \times 4^4 + 98 = 1 \times 4^4 + 1 \times 4^3 + 34$
$4^2 = 16 < 34$
By the division algorithm: $34 = 2 \cdot 16 + 2$
so $354 = 1 \times 4^4 + 1 \times 4^3 + 34 = 1 \times 4^4 + 1 \times 4^3 + 2 \times 4^2 + 2$
$4^1 > 2$
$354 = 1 \times 4^4 + 1 \times 4^3 + 2 \times 4^2 + 0 \times 4^1 + 2$
$354_{ten} = 11202_{four}$

Problem 6 Express 11202_{four} in expanded notation

Solution
$11202_{four} = 1 \times (four)^{10_{four}} + 1 \times (four)^{3_{four}} + 2 \times (four)^{2_{four}} + 0 \times (four)^{1_{four}} + 2 \times (four)^{0_{four}}$
or $= 1 \times (four)^{10} + 1 \times (four)^3 + 2 \times (four)^2 + 0 \times (four) + 2$

Problem 7 Find $789 + 315$ using the lattice method

Solution



Note: The entries of $10\ (=7+3)$, $9\ (=8+1)$, and $14\ (=9+5)$ from an addition table are put in the boxes under the single digits being added. For a two digit entry from the addition table, the number of units is put below the diagonal, and the number of tens is put above the diagonal. We then add along the diagonals, from the right—"carrying" if necessary. The diagonals, from the right, give us the number of units, tens, hundreds, and thousands respectively. $789 + 315 = 1104$.

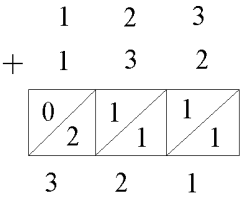
Problem 8 Make an addition table for base $four$.

Solution

$+$	1	2	3
1	2	3	10
2	3	10	11
3	10	11	12

Problem 9 Find $123_{four} + 132_{four}$ using the lattice method.

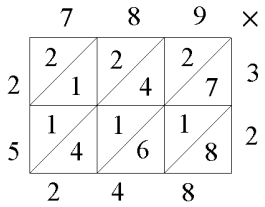
Solution



$123_{four} + 132_{four} = 321_{four}$.

Problem 10 Find 789×32 using the lattice method

Solution



$789 \times 32 = 25,248$

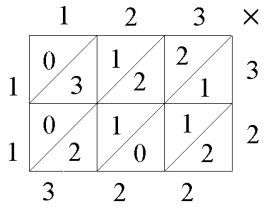
Problem 11 Make a multiplication table for base $four$.

Solution

$\times$	2	3
2	10	12
3	12	21

Problem 12 Find $123_{four} \times 32_{four}$ using the lattice method

Solution



$123_{four} \times 32_{four} = 11322_{four}$.

Problem 13 Subtract 706 from 2345, by adding the complement.

Solution Since $706 + 293 = 999$, the "complement" of 706 is 293. If we add 293 to 2345:

$$\begin{array}{r} 2345 \\ \underline{+\,293} \\ 2638 \end{array}$$

we get 2638. This number is 999 larger than $2345 - 706$. Therefore 2639 is 1000 larger than $2345 - 706$. Therefore $2345 - 706 = 2639 - 1000 = 1639$. Briefly:

$$\begin{array}{r} 2345 \\ \underline{+\,293} \\ 2638 \\ \underline{+\,1} \\ 2639 \end{array}$$

Answer: 1639

Problem 14 Subtract 23_{four} from 3112_{four}, by adding the complement.

Solution Since $23_{four} + 10_{four} = 33_{four}$, the "complement" of 23_{four} is 10_{four}. If we add 10_{four} to 3112_{four}:

$$\begin{array}{r} 3112 \\ \underline{+\,10} \\ 3122 \end{array}$$

we get 3122_{four}. This number is 33_{four} larger than $3112_{four} - 23_{four}$. Therefore 3123_{four} is 100_{four} larger than $3112_{four} - 23_{four}$. Therefore $3112_{four} - 23_{four} = 3123_{four} - 100_{four} = 3023_{four}$. Briefly:

$$\begin{array}{r} 3112 \\ \underline{+\,10} \\ 3122 \\ \underline{+\,1} \\ 3123 \end{array}$$

Answer: 3023_{four}.

Representations of Rational Numbers

Any rational number q has a representation as a fraction $\frac{a}{b}$, where a is an integer and b is a natural number. By formally dividing b into a, we get a decimal representation of q.

Example 1:

Let $q = \frac{2}{9}$. Find a decimal representation for q.

Solution:

$$\begin{array}{r|l} & \underline{0.2\ 2\ 2\ 2\ 2\ 2\ 2\ \cdots} \\ 9 & 2.0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ \cdots \end{array}$$

Thus $q = 0.2222\ \cdots$

Example 2:

Let $q = \frac{1}{4}$. Find a decimal representation for q.

Solution:

$$\begin{array}{r|l} & \underline{0.2\ 5\ 0\ 0\ \cdots} \\ 4 & 1.0\ 0\ 0\ 0\ \cdots \end{array}$$

Thus $q = 0.25$.

Project 1 Show that a rational number has a decimal representation that either has a cyclic repeating pattern (as in Example 1) or terminates (as in Example 2). What remainders are possible at each stage in the division? What happens when a remainder is repeated?

Project 2 Find examples of rational numbers that have repeating decimal representations, and examples that have terminating representations. Characterize (in terms of the numerators and denominators in their fractional representations) those rational numbers that will have terminating decimal representations.

Since rational numbers have either repeating or terminating decimal representations, a number such as $r = 0.101001000100001\cdots$, that neither terminates nor has a cyclic repeating pattern, is not a rational number. Such a number is called *irrational*[13]. Another irrational number is $\sqrt{2}$. To see why, suppose (to get a contradiction) that $\sqrt{2} = \frac{a}{b}$, where a and b are natural numbers. We can also suppose, without loss of generality, that a and b have no factor in common. Otherwise we could divide both numerator and denominator by the factor to get a representation where a and b have no common factor (reduce the fraction to "lowest terms"). Then

[13] The word "rational" comes from "ratio". Rational numbers are those that have fractional representations, that is, are ratios of integers. Irrational numbers are those that have no such representations. Although we call people "irrational" when they become illogical, irrational numbers are not at all illogical. Perhaps people were first called "irrational" because their ratio of response to stimulus was inappropriate.

$\sqrt{2} \cdot \sqrt{2} = \frac{a}{b} \cdot \frac{a}{b}$, that is, $2 = \frac{a^2}{b^2}$. From this we get $2 \cdot b^2 = a^2$. If a had no factor of 2, then a^2 would also be odd, and also have no factor of 2. This can't happen, since the left hand side of the equation $2 \cdot b^2 = a^2$ is even. Thus a has 2 as a factor, so that a^2 has 4 as a factor: that is, $a^2 = 4c$ for some natural number c. Therefore $2 \cdot b^2 = 4c$, which gives: $b^2 = 2c$. From this we see that b as well as a must be even—which contradicts the assumption that a and$b$ have no common factor. Since the assumption that $\sqrt{2}$ has a representation $\frac{a}{b}$, has led to a contradiction, $\sqrt{2}$ must be irrational.

Rational numbers have representations as fractions or "decimals" in bases other than *ten*.

Example 1:

$2 \times (four)^1 + 1 \times (four)^0 + 3 \times (four)^{-1} + 2 \times (four)^{-2}$ is expanded notation for the rational number 21.32_{four}.

Example 2:

Using the base four multiplication table from Appendix 2, we can find the "decimal" representation of the fraction $\frac{1_{four}}{2_{four}}$:

$$\begin{array}{r|l} & \underline{0.2\,0\,0\ \cdots} \\ 2 & 1.0\,0\,0\ \cdots \end{array}$$

$$\frac{1_{four}}{2_{four}} = 0.2_{four}$$

Example 3:

Consider the fraction $\frac{1}{3}$ to be written in turn in each of the bases $five$, six, and ten. Find "decimal" representations for $\frac{1}{3}$ in each of these bases.

Solution for base *five*:

In order to divide in base $five$, we first create a multiplication table for base $five$:

$\times$	2	3	4
2	4	11	13
3	11	14	22
4	13	22	31

$$\begin{array}{r|l} & \underline{0.1\,3\,1\,3\,1\,3\ \cdots} \\ 3 & 1.0\,0\,0\ \cdots \\ & \underline{3} \\ & 2\,0 \\ & \underline{1\,4} \\ & 1\,0 \end{array}$$

$$\frac{1_{five}}{3_{five}} = 0.131313\cdots_{five}$$

Solution for base *six*:

In order to divide in base six, we first create a multiplication table for base six:

$\times$	2	3	4	5
2	4	10	12	14
3	10	13	20	23
4	12	20	24	32
5	14	23	32	41

$$\begin{array}{r|l} & \underline{0.2\ 0\ 0} \\ 3 & 1.0\ 0\ 0 \end{array}$$

$\frac{1_{six}}{3_{six}} = 0.2_{\,six}$

Solution for base ten:

$$\begin{array}{r|l} & \underline{0.3\ 3\ 3\ 3\ 3\ \cdots} \\ 3 & 1.0\ 0\ 0\ \cdots \\ & \underline{9} \\ & 1\ 0 \end{array}$$

$\frac{1}{3} = 0.3333\cdots$

Project 3 From the preceding example, we see that $\frac{1}{3}$ represents repeating "decimals" in bases $five$ and ten, but a terminating "decimal" in base six. By looking at many examples, find a rule for which fractions give terminating "decimals" in an arbitrary base n.

Given a decimal representation of a rational number, it is possible to find a fractional representation by the following trick:

Example 4:

Suppose $q = 0.060606\cdots$. Then $100q = 6.060606\cdots$. Subtracting:

$$\begin{aligned} 100q &= 6.060606\cdots \\ \underline{q &= 0.060606\cdots} \\ 99q &= 6 \end{aligned}$$

Therefore, $q = \frac{6}{99} = \frac{2}{33}$.

Example 5:

Suppose $q = 0.22222\cdots_{five}$. Then $10_{five}q = 2.22222\cdots$. Subtracting:

$$\begin{aligned} 10q &= 2.22222\cdots \\ \underline{q &= 0.22222\cdots} \\ 4q &= 2 \end{aligned}$$

Therefore, $q = \frac{2}{4} = \frac{1}{2}$.

Example 6:

Suppose $q = (\frac{1}{2})_{five}$. Find a "decimal" (in base $five$) representation for q.

Solution :

Using the multiplication table for base $five$ from Example 3, we get the following division:

$$\begin{array}{r|l} & \underline{0.2\ 2\ 2\ 2\ 2\ \cdots} \\ 2 & 1.0\ 0\ 0\ \cdots \\ & \underline{4} \\ & 1\ 0 \end{array}$$

Therefore $(\frac{1}{2})_{five} = 0.22222\cdots$.

Example 7:

Suppose $q = 0.99999\cdots$. Then $10q = 9.99999\cdots$. Subtracting:

$$\begin{aligned} 10q &= 9.99999\cdots \\ \underline{q &= 0.99999\cdots} \\ 9q &= 9 \end{aligned}$$

Therefore, $q = \frac{9}{9} = 1$.

Example 7 shows that the same rational number may have different decimal representations. In particular $1.0 = 0.99999\cdots$. In order to avoid having different representations, the pattern of repeating 9's is not used. (All other cyclic repeating patterns are used.) Instead, any time we might see a pattern of repeating 9's, the digit preceding the pattern is raised by 1. For example, $13.249999\cdots$ is changed to 13.25. The numbers $13.249999\cdots$ and 13.25 are exactly the same, but the former representation is not generally used.

With the convention in the preceding paragraph, each rational number has a unique decimal representation. The same is not true, of course, for fractional representations. For example, $\frac{1}{2}$, $\frac{2}{4}$, $\frac{3}{6}$, and so on, all represent the same number. It is not possible to use only fractions in "lowest terms" (where numerator and denominator have no common factor), since other forms arise naturally in computations (and must be "reduced to lowest terms" later.) Rational numbers greater than 1 have expressions as either "mixed numbers" or "improper fractions". For example, $1\frac{1}{3} = \frac{4}{3}$. Both of these forms have their uses—another reason that we can't have a unique fractional representation for each rational number.

Inference Rule Formats

Rules for proving statements+

pr. $\Rightarrow$

1. Assume $\mathcal{P}$

k-1.$\mathcal{Q}$

k. $if\ \mathcal{P},\ then\ \mathcal{Q}$ (1—k-1; pr. $\Rightarrow$)

pr. *or*

1. Assume $\neg\mathcal{P}$

k-1.$\mathcal{Q}$

k.. $\mathcal{P}$ *or* $\mathcal{Q}$ (1—k-1; pr. *or*)

pr. *or*

1. Assume $\neg\mathcal{Q}$

k-1.$\mathcal{P}$

k.. $\mathcal{P}$ *or* $\mathcal{Q}$ (1—k-1; pr. *or*)

pr. *or* EZ

1. $\mathcal{P}$
2. $\mathcal{P}$ *or* $\mathcal{Q}$ (1; pr. *or* EZ)

pr. *or* EZ

1. $\mathcal{Q}$
2. $\mathcal{P}$ *or* $\mathcal{Q}$ (1; pr. *or* EZ)

pr. $\forall$

1. Let $x \in A$ be arbitrary

k-1.$\mathcal{P}(x)$

k. $for\,all\,x \in A : \mathcal{P}(x)$ (1—k-1; pr. $\forall$)

pr. &

j. $\mathcal{P}$

k-1.$\mathcal{Q}$

k. $\mathcal{P}\ and\ \mathcal{Q}$ (j, k-1; pr. &)

contradiction

1. Assume $\neg\mathcal{P}$

k-1. any contradiction # previous step, hyp., or thm. (reason for k-1)

k. $\mathcal{P}$ (1—k-1; #)

pr. $\exists$

i. <define x here>

j. $x \in A$

k-1. $\mathcal{P}(x)$

k. $there\,exists\,x \in A\,such\,that\,\mathcal{P}(x)$ (i, j, k-1; pr. $\exists$)

pr.$\forall \Rightarrow$

i. Let $x \in A$ and $\mathcal{P}(x)$

j. $\mathcal{Q}(x)$

j+1. $for\,all\,x \in A :\ if\ \mathcal{P}(x), then\ \mathcal{Q}(x)$ (i—j; pr.$\forall \Rightarrow$)

Rules for using statements

us. $\Rightarrow$

1. $if\ \mathcal{P},\ then\ \mathcal{Q}$
2. $\mathcal{P}$
3. $\mathcal{Q}$ (1, 2; us. $\Rightarrow$)

us. *or*

1. $\mathcal{P}$ *or* $\mathcal{Q}$

Case 1 2. Assume $\mathcal{P}$

j. $\mathcal{R}$

Case 2 j+1. Assume $\mathcal{P}$

k-1. $\mathcal{R}$

k. $\mathcal{R}$ (1—k-1; us. *or*)

us. *or* EZ

1. $\mathcal{P}$ *or* $\mathcal{Q}$
2. $\neg\mathcal{P}$
3. $\mathcal{Q}$ (1, 2; us. *or* EZ)

us. *or* EZ

1. $\mathcal{P}$ *or* $\mathcal{Q}$
2. $\neg\mathcal{Q}$
3. $\mathcal{P}$ (1, 2; us. *or* EZ)

us. &

1. $\mathcal{P}$ *and* $\mathcal{Q}$
2. $\mathcal{Q}$ (1; us. &)

us. &

1. $\mathcal{P}$ *and* $\mathcal{Q}$
2. $\mathcal{P}$ (1; us. &)

us. $\forall$

1. $for\,all\,x \in A : \mathcal{P}(x)$
2. $t \in A$
3. $\mathcal{P}(t)$ (1, 2; us. $\forall$)

us. $\forall \Rightarrow$

1. $for\,all\,x \in A : if\,\mathcal{P}(x),\,then\,\mathcal{Q}(x)$
2. $t \in A$
3. $\mathcal{P}(t)$
4. $\mathcal{Q}(t)$ (1, 2, 3; us. $\forall \Rightarrow$)

Index

I

L

M

N

O

P

R

S

T

U

V