Logic and the Axiomatic Method

Introduction

Mathematicians use a large number of methods to discover new results---trial and error, computation of special cases, inspired guessing, pulling results from thin air. The difference in this and an astrologer, for example, is that we have an accepted method, called the axiomatic method, for *proving* that these results are correct. Proofs give us assurance that results are correct. In many cases they also give more *general* results. For example, the Egyptians and Hindus knew by experiment that if a triangle has sides of lengths 3, 4, and 5, it is then a right triangle. But the Greeks proved that if a triangle has sides of lengths a, b, and c, and if $a^2+b^2 = c^2$, then the triangle is a right triangle. There is no amount of checking by experiment that could give this general result. Proofs give us insight into relationships among different things that we are studying, forcing us to organize our thoughts in a coherent way. If you gain nothing else from the course than this, you have still gained the greatest gift that mathematics has to offer.

I wish to persuade you that a certain statement is true or false by *pure reasoning*. I could do this by showing you that the statement follows logically from some other statement that you may already believe. I may have to convince you that that statement is also true, and follows from another statement. This process may continue until I reach a statement which you are willing to believe, one which does not need justification. That statement plays the role of an *axiom*. If no such statement exists, then I will be caught in an *infinite regress*, giving one proof after another *ad infinitum*. There are three requirements that must be met before we can agree that a proof is correct.

Requirement 1 There must be mutual understanding of the words and symbols used in the discourse.

Requirement 2 There must be acceptance of certain statements called *axioms* without justification.

Requirement 3 There must be agreement on how and when one statement *follows logically* from another, *i.e.*, agreement on certain rules of reasoning.

There should be no problem in reaching mutual understanding so long as we use terms familiar to both and use them **consistently**. If I use an unfamiliar term, you have the right to demand a *definition* of this term. Definitions cannot be given arbitrarily; they are subject to the rules of reasoning referred to in Requirement 2. Also, we cannot define every term that we use. In order to define one term we must use other terms, and to define these terms we must use still other terms, and so on. If we were not allowed to leave some terms *undefined*, we would get involved in infinite regress.

Let us begin with this.

Sets

We need some basic information about sets in order to study the logic and the axiomatic method. This is not a formal study of sets, but consists only of basic definitions and notation.

Braces { and } are used to name or enumerate sets. The *roster* method for naming sets is simply to list all of the elements of a set between a pair of braces. For example the set of integers 1, 2, 3, and 4 could be named {1,2,3,4}. This does not work well for sets containing a large number of elements, though it can be used. The more common method for this is known as the *set builder notation*. A property is specified which is held by all objects in a set. $P(x)$, read *P of x*, will denote a sentence referring to the variable x. For example,

$$x = 23$$
x is an odd integer.
$$1 \le x \le 4.$$

The set of all objects x such that x satisfies $P(x)$ is denoted by $\{x \mid P(x)\}$. The set {1,2,3,4} can be named $\{x \mid 1 \le x \le 4, x \in \mathbf{Z}\} = \{x \in \mathbf{Z} \mid 1 \le x \le 4\}$.

From hence forth, the words *object*, *element*, and *member* mean the same thing when referring to sets. Sets will be denoted mainly by capital Roman letters and elements of the sets by small letters. The following have the same meaning:

$a \in A$
a is in set A
a is a member of set A
a is an element of set A.

Likewise, $a \notin A$ means that a is **not** an element of set A. A is a *subset* of B if every element of A is also an element of B. The following have the same meaning:

$A \subset B$
Every element of A is an element of B
If $a \in A$, then $a \in B$
A is included in B
B contains A
A is a subset of B

Note that a set is always a subset of itself.
If A and B are sets, then we say that $A = B$ if A and B represent the same set:

$A = B$

A and B are the same set
A and B have the same members
$A \subset B$ and $B \subset A$

The set which contains no elements is known as the *empty set*, and is denoted by $\varnothing$. Note that for every set A, $\varnothing \subset A$.

The *intersection* of two sets A and B is the set of all elements common to both sets. The intersection is symbolized by $A \cap B$ or $\{x \mid x \in A \text{ and } x \in B\}$. The *union* of two sets A and B is the set of elements which are in A or B or both. The union is symbolized by $A \cup B$ or $\{ x \mid x \in A \text{ or } x \in B\}$.

Universal Sets and Compliments

When we are working in an area or on a certain problem, we always have a frame of reference in which we are working called a *universal set*. In our geometry course, it will be the set of points that lie on a plane. In calculus we consider the set of real numbers, the set of real functions, the set of differentiable functions, and the set of continuous functions as universal sets.

The *complement* of a set A is defined to be the set of all elements of the universal set which are not in A, and is symbolized by $CA = A' = A^c$. Note that $A \cup A^c$ is always the universal set, while $A \cap A^c = \varnothing$.

Sentences and Statements

Logic and mathematical proof can be studies just like algebra. In fact, much of symbolic logic is just that. A declarative sentence which is true or false, but not both, is called a *statement*. The following are statements:

Babe Ruth hit 714 home runs.
Jack Nicklaus has won 20 major golf titles.
$2 + 3 = 6$
The 25,000$^{\text{th}}$ digit of π is 7.

The following are not statements:

He is a golfer.
Why is a duck?
$x + 1 = 0$
$x - y = a$

The sentence

He is a golfer.

cannot be judged true or false because we do not know who *He* is. If the word *He* is replaced by *Tiger Woods* forming the sentence

Tiger Woods is a golfer.

the sentence becomes a true statement. Similarly, if x in the sentence $x + 1 = 0$ is replaced by 2, forming the sentence $2 + 1 = 0$, the sentence then becomes a false statement.

The letter x is a **variable** in the sentence $x + 1 = 0$. A letter or other symbol that can represent various elements of a universal set is called a **variable**. We can make a sentence a statement by replacing its variables by elements of the universal set or by attaching phrases such as *For every* or *There exists* to the sentence. For example, $x < 3$ is not a statement, but each of the following is a statement:

$1 < 3$
$5 < 3$
For every real number x, $x < 3$.
There exists a real number x, such that $x < 3$.

Replacements for variables of a sentence are always chosen from some universal set. Any replacement which makes a sentence true is called a **solution**. The set of all solutions is called the *solution set* of the sentence.

Connectives

If P and Q are sentences, then the sentence *P and Q* is called the **conjunction** of P and Q, denoted by $P \wedge Q$. For any statement there are just two possible truth values, true (T) or false (F). If P and Q are both true, then $P \wedge Q$ is true. If one or both of P and Q are false, then $P \wedge Q$ is false. The truth table below defines the truth values of $P \wedge Q$ for all possible truth value combinations of P and Q.

If P and Q are sentences, then the sentence *P or Q* is called the **disjunction** of P and Q, denoted by $P \vee Q$. In mathematics we use an *inclusive* or. That is, $P \vee Q$ is true when P is true, or Q is true, or both are true. $P \vee Q$ is false only when P and Q are false. The truth table for $P \vee Q$ is thus defined below.

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

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

A *negation*, or *denial*, of a sentence is formed in many ways. For example the *negation* of the statement ***P:*** *2 is rational* is represented by each of the following:

~P
It is false that 2 is rational.
2 is not rational.

P	$\sim P$
T	F
F	T

2 is irrational.

The truth table for negation is obvious. You should realize that there are other symbols, besides ~, for negations that are in common usage.

$a \neq b$ means ~($a = b$)
$a \geq b$ means ~($a < b$)
$a \notin A$ means ~($a \in A$)$

If P and Q are sentences, the sentence *If P, then Q* is denoted by $P \to Q$ or $P \Rightarrow Q$. We construct a truth table for $P \Rightarrow Q$ just as for the other connectives $\wedge$, $\vee$, and ~. However, the construction is not at all obvious. Consider the sentence:

If I get an A in mathematics, then I will take the next course.

Suppose a fellow student says this. When is the sentence true and when is it false? Let P denote the statement *I get an A in mathematics* and let Q denote the statement *I will take the next course*. Consider the following four cases.

1. P (true): He gets an A in mathematics.
   Q (true): He takes the next course.
2. P (true): He gets an A in mathematics.
   Q (false): He does not take the next course.
3. P (false): He does not get an A in mathematics.
   Q (true): He takes the next course.
4. P (false): He does not get an A in mathematics.
   Q (false): He does not take the next course.

It is easy to see that (1) is true and that (2) is false. You cannot claim that the original statement was false in (3) since he takes the next course even though he did not get an A. Likewise, in (4) you cannot claim that the statement was false, since he did not get an A and he did not take the next course. The truth table for this sentence is shown.

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

The sentence $P \Rightarrow Q$ is called a **conditional** with P the **antecedent** and Q the **consequent**. In mathematics the conditional is encountered in many forms. The following have the same meaning:

$P \Rightarrow Q$
If P, then Q
P implies Q
Q if P, P only if Q
Q provided P
Q whenever P, Q when P
P is a sufficient condition for Q
Q is a necessary condition for P.

Biconditionals and Combinations of Connectives

A sentence of the type $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ is called a **biconditional**, denoted $P \Leftrightarrow Q$. When P and Q are sentences, the truth table for $P \Leftrightarrow Q$ is as shown.

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

In mathematics the biconditional is encountered in many forms. The following have the same meaning:

$P \Leftrightarrow Q$
P is equivalent to *Q*
P if and only if *Q*
Q if and only if *P*
P iff *Q*
If *P*, then *Q* and conversely
If *Q*, then *P* and conversely
P is a necessary and sufficient condition for *Q*
Q is a necessary and sufficient condition for *P*.

Combinations of ~, $\Rightarrow$, $\Leftrightarrow$, $\wedge$, and $\vee$ often occur. A facility at recognizing them is essential for mathematical reading and proof. Consider the following statement:

If P is prime, then if P is even P must be smaller than 7.

This breaks up into three statements:

P: *P* is prime.
Q: *P* is even.
R: *P* must be smaller than 7.

We can then translate the original statement into $P \Rightarrow (Q \Rightarrow R)$.

If k is perpendicular to ℓ and ℓ is perpendicular to m, then k is parallel to m.

Let

P: *k* is perpendicular to ℓ
Q: ℓ is perpendicular to *m*
R: *k* is parallel to *m*.

Then the sentence translates as $(P \wedge Q) \Rightarrow R$.

Quantifiers

Sentences involving the phrases *For every …* and *There exists …* also play a very important role in the structure of mathematical sentences. The symbol $\forall$, called the **universal quantifier**, denotes phrases such as *For each*, *For every*, *For all*. A sentence such as

For every x, $P(x)$

can be translated symbolically into $\forall\ x\ P(x)$; or $\forall\, x,\ P(x)$. The following sentences have the same meaning:

$\forall\, x$, x is an integer $\Rightarrow x \in \mathbf{Q}$,
For every x, if x is an integer, then $x \in \mathbf{Q}$,
For all x, if x is an integer, then $x \in \mathbf{Q}$,
For each x, if x is an integer, then $x \in \mathbf{Q}$,
Every integer belongs to **Q**,
Every integer is a rational number,
If x is an integer, then $x \in \mathbf{Q}$.

Note that in the last sentence the universal quantifier is understood and not written.

The symbol $\exists$, called the **existential quantifier** symbolizes phrases such as *There exists*, *There is at least one*, *For at least one*, and *Some*. A sentence such as

There exists an x such that P(x)

translates symbolically to $\exists\ x\ P(x)$ or $\exists\ x,\ P(x)$.
The following have the same meaning:

$\exists\ x$, x is a natural number.
There exists an x such that x is a natural number.
Some number is a natural number.
There is at least one natural number.

Quantifiers often appear together. Consider the following examples.

$\forall\ x\ \forall\ y,\ x + y = 0$	For every x and for every y, $x + y = 0$.
$\forall\ x\ \exists\ y,\ x + y{=}0$	For every x there exists a y so that $x + y = 0$.
$\exists\ \mathrm{x}\forall\ \mathrm{y},\ x + y{=}0$	There exists an x such that for all y, $x + y{=}0$.
$\exists\ \mathrm{x}\exists\ \mathrm{y},\ x + y{=}0$	There exists an x and there exists a y such that $x + y{=}0$.

The following sentence

For every x, if x is even, then there exists a y such that $x = 2y$.

translates as $\forall\ x\ (x \text{ is even} \Rightarrow \exists\ y,\ x{=}2y)$.

These quantifiers refer to some universal set, which if not explicitly given, must be easily inferred from the context. We will be interested only in nonempty universal sets.

Definition: The sentence $\forall\ x\ P(x)$ is **true** if and only if the solution set of $P(x)$ equals the universal set. This sentence is **false** if the solution set is a proper subset of the universal set; *i.e.*, if there is at least one element of the universal set for which $P(x)$ is false.

Definition: The sentence $\exists\ x\ P(x)$ is **true** if the solution set of $P(x)$ is nonempty. This sentence is **false** if the solution set of $P(x)$ is empty; *i.e.*, if for every replacement of x by a member a of the universal set, $P(a)$ is false.

For more complicated mathematical sentences containing more quantifiers let us look at a few examples.

Example: Suppose $P(x,y)$ is a sentence with variables x and y. The sentence $\forall x \forall y$ $P(x,y)$ is true if and only if for every replacement of x and y by members a and b from the universal set, the statement $P(a,b)$ is true. The sentence is false if there is a replacement for x or a replacement for y for which the statement is false.

Example: The sentence $\exists x \forall y$, $P(x,y)$ is true if there exists a replacement A for x such that $\forall$ y $P(a,y)$ is true. This same A makes the sentence $P(a,b)$ true for every B in the universal set. Note that the sentence $\exists$ x $\forall$ y, $x > y$ is false. There is no replacement A for x which makes the sentence $\forall$ y, $a > y$ true.

Rules of Reasoning

Mathematicians assume a certain class of sentences to be true before we ever prove any theorems in a mathematical system. We call these sentences *rules of reasoning*. They could be called reasoning axioms.

An important class of these rules of reasoning is the class of **tautologies**. A tautology is a sentence which is true no matter what the truth value of its constituent parts.

Example: The sentence $P \Rightarrow (P \vee Q)$ is a tautology, where P and Q represent arbitrary mathematical sentences. We can show that this is a tautology from a truth table. The way in which we do this is to compute the truth values for $P \vee Q$ in the third column first, and then use columns one and three to compute the truth values in column four.

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

Logic Axiom 1: Every tautology is a rule of reasoning.

The following are tautologies that we commonly use. You will find these listed in the *Rules of Logic* that you have been given.

1. $(P \Rightarrow Q) \Leftrightarrow (\sim Q \Rightarrow \sim P)$ *contrapositive*
2. $[P \wedge (P \Rightarrow Q)] \Rightarrow Q$ *Modus ponens*
3. $[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$ *Law of Syllogism*
4. $\sim (P \wedge Q) \Leftrightarrow (\sim P \vee \sim Q)$
5. $\sim (P \vee Q) \Leftrightarrow (\sim P \wedge \sim Q)$[1]
6. $\sim (P \Rightarrow Q) \Leftrightarrow (P \wedge \sim Q)$
7. $(P \Rightarrow Q) \Leftrightarrow (\sim P \vee Q)$

[1] Items 4 and 5 comprise De Morgan's Laws

8. $\left(P \wedge Q\right) \Rightarrow P$
9. $\sim\left(\sim P\right) \Leftrightarrow P$
10. $\left(P \wedge Q\right) \Rightarrow \left(P \vee Q\right)$
11. $\left(P \Rightarrow \sim Q\right) \Rightarrow \left(Q \Rightarrow \sim P\right)$
12. $\left[\sim P \Rightarrow \left(R \wedge \sim R\right)\right] \Rightarrow P$
13. $\left[\left(P \wedge \sim Q\right) \wedge \left(R \wedge \sim R\right)\right] \Rightarrow \left(P \Rightarrow Q\right)$ [2]
14. $P \vee \sim P$ (*Law of the Excluded Middle*)
15. $P \Leftrightarrow P$
16. $P \Rightarrow P$
17. $\left[P \Rightarrow \left(Q \vee R\right)\right] \Rightarrow \left[\left(P \wedge \sim Q\right) \Rightarrow R\right]$
18. $\left[\left(P \Rightarrow S_1\right) \wedge \left(S_1 \Rightarrow S_2\right) \wedge \ldots \wedge \left(S_{n-1} \Rightarrow S_n\right) \wedge \left(S_n \Rightarrow R\right)\right] \Rightarrow \left(P \Rightarrow R\right)$ (*Law of Syllogism*)
19. $\left[\left(P \Rightarrow R\right) \wedge \left(Q \Rightarrow R\right)\right] \Rightarrow \left(P \vee Q\right) \Rightarrow R$ (*Proof by Cases*)
20. $\left(P \wedge Q\right) \Leftrightarrow \left(Q \wedge P\right)$
21. $\left(P \vee Q\right) \Leftrightarrow \left(Q \vee P\right)$ [3]
22. $\left[P \Rightarrow \left(R \Rightarrow Q\right)\right] \Leftrightarrow \left(P \wedge R\right) \Rightarrow Q$
23. $\left[P \wedge \left(Q \wedge R\right)\right] \Leftrightarrow \left[\left(P \wedge Q\right) \wedge R\right]$
24. $\left[P \vee \left(Q \vee R\right)\right] \Leftrightarrow \left[\left(P \vee Q\right) \vee R\right]$ [4]
25. $\left[P \wedge \left(Q \vee R\right)\right] \Leftrightarrow \left(P \wedge Q\right) \vee \left(P \wedge R\right)$
26. $\left[P \vee \left(Q \wedge R\right)\right] \Leftrightarrow \left(P \vee Q\right) \wedge \left(P \vee R\right)$ [5]
27. $\left[\left(P \Leftrightarrow Q_1\right) \wedge \ldots \wedge \left(Q_n \Leftrightarrow Q\right)\right] \Rightarrow \left(P \Rightarrow Q\right)$

Valid Arguments

The tautologies in the preceding section are not all that there are. If you want to make a deduction based on a sentence, check its truth table. If it is a tautology, use it. Tautologies provide lots of reasoning theorems before we ever start deduction within a mathematical system.

There are actually two branches of formal logic: the statement calculus, involving statements and reasoning by tautology; and the predicate calculus, involving quantified sentences. All we are doing is taking a quick guided tour through informal logic, and so we will not study these areas in great detail. However, from the predicate calculus we

[2] Items 12 and 13 comprise *Proof by Contradiction*.
[3] Items 20 and 21 are the *Commutative Laws*.
[4] Items 23 and 24 are the *Associative Laws*.
[5] Items 25 and 26 are the *Distributive Laws*.

get another collection of reasoning sentences, some of which are listed below. These cannot be verified by tautology.

Logic Axiom 2: Let U be a universal set. Each of the following is a rule of reasoning.

1. $[\forall x, P(x) \Rightarrow Q(x)] \Rightarrow [\forall x, P(x) \Rightarrow \forall x, Q(x)]$,
2. $\forall x, P(x) \Leftrightarrow P(a)$ for any $a \in U$,
3. $\exists x, P(x) \Leftrightarrow [P(a)$ for some $a \in U]$.

An **argument** is an assertion that from a certain set of sentences $S_1, \ldots, S_n$ (called *premises* or *assumptions*) one can deduce another sentence Q (called an *inference* or *conclusion*). Such an argument can be denoted by $S_1, \ldots, S_n \mapsto Q$. Arguments are either **valid** (correct) or **invalid** (incorrect).

Definition: $S_1, \ldots, S_n \mapsto Q$ is a valid argument if and only if $S_1 \wedge \ldots S_n \Rightarrow Q$ is a rule of reasoning.

Logic Axiom 3: [*Rule of Substitution*] Suppose $P \Leftrightarrow Q$. Then P and Q may be substituted for one another in any sentence.

***Logic Axiom 3*:** Every sentence of the type $\sim (\exists x, P(x)) \Leftrightarrow (\forall x, \sim P(x))$ is true.

***Logic Axiom 4*:** Every sentence of the type $\sim (\forall x, P(x)) \Leftrightarrow (\exists x, \sim P(x))$ is true.

To prove a sentence of the type $\forall x,\ P(x)$ false, one could try to prove $\exists x \sim P(x)$ true. This is referred to as *providing a counterexample*.

Proof

Mathematical Systems

A *mathematical system* consists of the following:

1. a set of undefined concepts,
2. a universal set,
3. a set of relations,
4. a set of operations,
5. a set of logical axioms,
6. a set of non-logical axioms—these axioms pertain to the elements being studied, the relations, and the operations; and not to the logic being used,
7. a set of theorems,
8. a set of definitions,
9. an underlying set theory.

In plane geometry the undefined concepts are those of point and line. The universal set is the set of points in the plane. The relations are such concepts as equality, perpendicularity, and parallelism. We have mentioned the logical axioms. A non-logical axiom would be of the form:

Two different points are on exactly one line.

Proof

Definition: Suppose $A_1, A_2, \ldots, A_K$ are all the axioms and previously proved theorems of a mathematical system. A **formal proof**, or deduction, of a sentence P is a sequence of statements $S_1, S_2, \ldots, S_n$, where

1. S_n is P, and **one of the following holds**
   a) S_i is one of $A_1, A_2, \ldots, A_K$, or
   b) S_i follows form the previous statements by a valid argument using the rules of reasoning.

A **theorem** is any sentence deduced from the axioms and/or the previous theorems. The same is true of **lemma** and **proposition**. For some mathematicians there is a hierarchy of lemma, proposition, and theorem; with lemma being the easiest to prove and theorem the most difficult, or longest. Other mathematicians make little or no distinction between these objects, and will call everything a theorem.

Example: Suppose a mathematical system contains just the following axioms:

1. A_1: $(a+b=c) \Rightarrow [x<y \wedge (2=3)]$
2. A_2: $a+b=c$.

The following is a **formal proof** of $x<y$.

S1: $(a+b=c)\Rightarrow\left[x<y\wedge(2=3)\right]$ by A1

S2: $a+b=c$ by A2

S3: $(x<y)\wedge(2=3)$ by *modus ponens* on S1, S2

S4: $x<y$ by the tautology $(P\wedge Q)\Rightarrow P$

In practice mathematicians do **not** write formal proofs. They write informal proofs. An informal proof is an argument which shows the existence of a formal proof. As such it gives enough of the formal proof so that another person becomes *convinced*. Thus we might call an informal proof a *convincing argument*. Mathematicians try to convince other mathematicians. You will try to convince your fellow students and me, your professor.

An informal proof of the above example runs as follows:

From A1 and A2 it follows that $(x<y)\wedge(2=3)$. Thus, $x<y$.

Henceforth, we will be writing only informal proofs. The art of mathematics is creating proofs. Just as every other artisan, the mathematician has some basic modes of proof. We will now consider a few of these.

Proving Conditionals

You usually prove a sentence of the type $P\Rightarrow Q$ in plane geometry by assuming P and deducing Q. You consider Q the conclusion. In actually, $P\Rightarrow Q$ was the conclusion. It was what you were trying to prove.

To prove $P\Rightarrow Q$ first assume P to be true. Then using P and all other theorems and axioms try to deduce Q. Once Q is deduced in this manner you have completed a proof of $P\Rightarrow Q$. You have **not** shown that Q is true; you have only shown that Q is true if P is true. Whether P is true is another question; whether Q is true is another question. What you have shown to be true is $P\Rightarrow Q$.

This technique is called the *Rule of Conditional Proof* or the *Deduction Theorem*. More formally, suppose that $A_1, A_2, \ldots, A_K$ are the axioms and previously proved theorems. To prove $P\Rightarrow Q$ is to show that

From $A_1, A_2, \ldots, A_K$ *we can deduce* $P\Rightarrow Q$

is a valid argument. To do this temporarily assume P to be an axiom and show that

From $A_1, A_2, \ldots, A_K, P$ *we can deduce* Q

is a valid argument.

A second technique of proving $P\Rightarrow Q$ is by the *contrapositive*. We can prove $P\Rightarrow Q$ by proving $\sim Q\Rightarrow\sim P$. Often the rule of conditional proof is used to prove the contrapositive.

Proving Biconditionals

There are three modes of proof for biconditional sentences.

1. Prove $P \Rightarrow Q$ and $Q \Rightarrow P$.
2. Prove $P \Rightarrow Q$ and $\sim P \Rightarrow \sim Q$.
3. Provide an *iff*-string.

A word about the *iff-string*. We produce a string of equivalent sentences from P to Q. This is the *Law of Syllogism* from the list of tautologies.

Proving $\forall x\, P(x)$

To prove $\forall x\, P(x)$ let x represent an arbitrary element of the universal set and prove that $P(x)$ is true. Then since x was arbitrary element of the universal set, we may generalize that $\forall x\, P(x)$ is true. The justification is **Logical Axiom 2.**

Proof by Cases

Proof by cases is used several ways and involves the connective *or*. We will be trying to prove a sentence of the type $(P \vee R) \Rightarrow Q$. This type of proof utilizes the tautology

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

The proof is accomplished by proving the antecedent of this sentence, $[P \Rightarrow Q] \wedge [R \Rightarrow Q]$. Hence, $[P \Rightarrow Q]$ and $[R \Rightarrow Q]$ must be proved. Any mode of proof for conditional sentences can be used.

Similarly, a proof by cases of $(P_1 \vee P_2 \vee \ldots \vee P_n) \Rightarrow Q$ is accomplished by proving $(P_1 \Rightarrow Q) \wedge \ldots \wedge (P_n \Rightarrow Q)$.

The art of producing a proof by cases lies in the discovery of what set of exhaustive cases is appropriate.

Mathematical Induction

This is a technique that is all too often overlooked in geometry. I include it here for completeness. Suppose $P(n)$ is a sentence which is a statement for any $n \in \mathbf{N}$, then the *Principle of Mathematical Induction* is $[P(1) \wedge \forall k, P(k) \Rightarrow P(k+1)] \Rightarrow \forall n, P(n)$. If we can prove the antecedent of this statement, $[P(1) \wedge \forall k, P(k) \Rightarrow P(k+1)]$, then by *Modus ponens* we can deduce $\forall n, P(n)$. Thus there are two steps in the proof of $\forall n, P(n)$:

Basic Step. Prove $P(1)$.

Inductive Step. Prove $\forall k, P(k) \Rightarrow P(k+1)$.

Note that its name is misleading. *Mathematical induction*} is *deductive reasoning* not *inductive reasoning*. *Inductive reasoning* is making a conjecture or guess based on observations and your previous mathematical experience.

Proof by Contradiction

A **contradiction** is a statement which is false no matter what the truth value of its constituent parts. It can usually be expressed symbolically in the form $R \wedge \sim R$. A *proof by contradiction* of a statement P is a proof that assumes ~P and yields a sentence of the type $R \wedge \sim R$, where R is any sentence including P, an axiom, or any previously proved theorem. This is justified by the tautology $[\sim P \Rightarrow (R \wedge \sim R)] \Rightarrow P$. Intuitively, P can only be true or false (since we are assuming only a two-valued logic). If we assume its negation true and this yields another sentence both true and false, then ~P cannot be true, so P must be true.

The phrases *reductio ad absurdum* and *indirect proof* both refer to *proof by contradiction*. The importance of being able to form sentence negations is realized when doing proofs by contradiction. To begin such proofs you must know how to form negations.

Comparing proof techniques we see that with the *Rule of Conditional Proof* we assume P with the explicit intention of deducing Q. With the contrapositive we assume ~Q with the explicit intention of deducing ~P. But in using *Proof by Contradiction* we assume both P **and** ~Q and try to deduce any sentence R and its negation ~R.

Proofs of Existence and Uniqueness

The sentence

There exists an x such that $P(x)$

is denoted by $\exists x, P(x)$. The sentence

There exists exactly one x such that $P(x)$

is denoted by $\exists! x, P(x)$.

There are two parts to proving a sentence of this form.

Existence Part. Prove that there is an x such that $P(x)$ is true.

Uniqueness Part. Here you must prove that if there are two elements x and z such that $P(x)$ and $P(z)$ are each true, then $x = z$. Symbolically, $\forall x \forall z, [P(x) \wedge P(z)] \Rightarrow x = z$.

Proof Creativity

In the previous part of this chapter you learned several modes of proof. The intent is that these will become part of your mathematical toolbox. Just because you have the tools does not guarantee that you can create a proof. There are some helpful procedures to follow as aids in creating a proof.

Translate to Symbolic Logic. A typical comment made when proofs are attempted is

I do not know where to start!!!!

This statement is made with a great gnashing of teeth and wringing of hands. One procedure to follow is comparable to that of solving a problem in basic algebra.

First, translate what you are requested to prove into symbolic logic. Then seeing the structure of the translated sentence you can select a mode of proof. Still, knowing a mode of proof that could be used does not guarantee success. Suppose you want to attempt to prove a sentence of the type $P \Rightarrow Q$ by using the *Rule of Conditional Proof*. You want to assume *P* and deduce *Q*. A question often asked is

How do I get from P to Q?

There is no certain way. No one way will always work. Certainly, knowing to assume *P* and deduce *Q* is a step in the right direction. The mode of proof provides the structure for the proof; building this structure is usually a more creative task. I can give a few hints.

Analogy. An important aid in carrying out proofs is to get ideas from other proofs. This is supposed by comments of mathematicians who argue that to be good at mathematics you need lots of practice; lots of exposure to different proofs.

Analytic Process. This is known as *working backwards*. You want to prove $P \Rightarrow Q$. Start with *Q* and try to find an *R* such that $R \Rightarrow Q$. Then try to find and *S* such that $S \Rightarrow R$. Then look to see if $P \Rightarrow S$. If not, try to fill in another step. Continue this until you find a sentence R_n such that $P \Rightarrow R_n$ and $R_n \Rightarrow R_{n-1} \Rightarrow \cdots \Rightarrow R \Rightarrow Q$. Do not be surprised if you do not see this process outlined in a text or reference book. It is rare for this processed to be used. It is then explicitly mentioned. Usually the proof will be given as $P \Rightarrow R_n \Rightarrow R_{n-1} \Rightarrow \cdots \Rightarrow R \Rightarrow Q$.

Something Approach. This is simply trial-and-error. You want to prove $P \Rightarrow Q$ by assuming *P* and deducing *Q*. You have no particular way to get from *P* to *Q*; but start out, get involved, do something, try different approaches, prove all that you can. You do not have to show all of this in your final version of your proof, but it can help you get started. When reading proofs in mathematics texts and journals, you are not aware of the blind alleys and unsuccessful attempts preceding a successful proof. This leads you to think the established mathematician never follows a wrong path or makes a mistake. Trial and error is very much a part of mathematical creativity.

Use of Definitions. Another helpful procedure is to recall all relevant definitions. It is a tendency to read a definition and ignore its importance in later proofs.

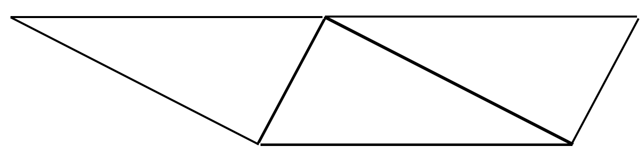
Use of Previously Proved Theorems. It is helpful—nay, it is essential in starting a proof to examine all previously proved theorems for results which might be relevant to the proof.

Proofs in Geometry

We often get the question, "Why do we need to prove this? It was true in all of the cases that I checked." Proof is an important part of mathematical investigation, but it is not the first part. Consider the following theorem:

THEOREM: *For any triangle in the Euclidean plane, the sum of the measures of the interior angles is two right angles.*

There are several ways to look at this. You can cut out triangles, measure the three interior angles with a protractor and add up the measures. You may not get exactly 180°, but it will be close. How close? It depends on the accuracy of your protractor and you! If we had to count on that all of the time, we could not find any consistency. Is there another way? You could cut out three copies of the same triangle, number the angles and rearrange them so that the three angles are adjacent to one another. Doesn't it look like a straight line? Can we be sure?



Consider the following problem:

Kevin divided a square with an area of 169 square units (13 × 13) into two trapezoids and two right triangles. But when he rearranged the four parts into a rectangle, he got an area of 168 square units (8 × 21)! So he then rearranged the four parts into a triangle (base measuring 16 and height measuring 21), again with an area of 168 square units!

What is going on? Try it yourself with the handout. Cut it up and create a rectangle and then rearrange them to be a triangle. What is wrong here? Can you just lose area? Or can you PROVE that the objects in question are not a rectangle or a triangle? Proof can answer this question, and proof answers the question as to why it works the way it does.

How does discovery lead to proof? Should discovery lead to proof? Many times discovery and experimental confirmation motivate us to start looking for a proof. We may not really experience a need for further certainty, but we may want an *explanation* (why was it true?) and we may want the *intellectual challenge* (can I prove it?).

Logically, mathematics is probably based on the following fundamental axiom "*Something is true (T), if and only if it can be deductively proven (P).*" However, we do not always think of things in this particular manner. We have some equivalent, but different logical forms that we use:

(a) the forward implication: *if something is true, then it can be proven*;

(b) the converse: *if something has been proven then it is true*;

(c) the inverse: *if something is false then it cannot be proven*;

(d) the contrapositive: *if something cannot be proven, then it is false*;

It is unfortunate that in textbooks and in our teaching only the converse is usually conveyed, in other words we tell our students that we must first prove results before we can accept them as true. However, in actual mathematical research and discovery, the forward implication, its inverse and contrapositive play a far greater role in motivating and guiding our actions.

For example, suppose we make a conjecture and then test some cases. If the conjecture is not supported by the cases that we test and we feel that we have been careful in testing various types of cases, then we reject the conjecture as false and according to the inverse we do not even bother trying to prove it. On the other hand, if our discovery and conjecture is supported by the cases that we check, we might begin to believe that it is true, which according to the forward implication gives us the encouragement to start looking for a proof. If after a while we are not successful in producing a proof, we might begin to question our conjecture and look at some further examples, thus starting the process over again.

Using many examples never really gives a satisfactory explanation of why something is true. I merely confirms that it is true in these examples and probably in general and even though the consideration of more and more examples may increase my confidence even more, it gives no psychological satisfactory sense of illumination. There is no insight or understanding into how it fits with other results. The more that you are convinced that something is true, the more you want to prove that it is true. This gives some psychological justification to your intuition and your ability to discern truth from untruth.

Not all proofs are explanatory; sometimes we can only be satisfied with a proof that verifies, but the ideal is to arrive at some sort of satisfactory explanation of what is happening. It is always nice to have a proof that something is true, but there are times when I have spent hours or days looking for a better, more explanatory proof as to why it is true. Robert Long has written:

> "Proofs that yield insight into the relevant concepts are more interesting and valuable to us as researchers and teachers than proofs that merely demonstrates the correctness of a

> result. We like a proof that brings out what seems to be essential. If the only available proof of a result is one that seems artificial or contrived it acts as an irritant. We keep looking and thinking."

Also to Manin and Bell, explanation is a criterion for a "*good*" proof. It is "*one which makes us wiser*", and it is expected "*to convey an insight into* ***why*** *the proposition is true*."

Another important function of proof is that of discovery. The production of a proof that identifies its underlying explanatory properties can sometimes lead to a further unanticipated result.

Mathematicians know that proving something is an intellectual challenge that can be compared to the physical challenge of completing a marathon. In this sense proof serves the function of self-realization and fulfillment. Proof is a testing ground for the intellectual stamina and ingenuity of the mathematician. To paraphrase Mallory's famous comment on the reason for climbing Mount Everest: "*we prove our results because they're there*."

We should challenge our students to explain why something is true. We should be quite honest with our students in telling them that mathematicians often prove results simply because of the intellectual challenge involved. We should not try to present a fairy tale of always wanting to obtain "*certainty*."