Any stepwise procedure consists of what we might call “treads” and “risers”. In mathematical proofs, the treads are mathematical statements, and the risers involve logical rules and rules of inference. This chapter deals with rules of logic and inference and how these may be used in the construction and understanding of proofs.

We begin with a simplified version of symbolic logic, the propositional calculus, in which so-called quantification does not occur. The propositional calculus analyzes the truth relationships between compound statements and their subsidiary parts. A later chapter, on the predicate calculus, expands on this by introducing quantification.

Symbolic logic is sometimes called formal or syntactic, in the sense that, after the basic rules have been established, symbolic logic focuses exclusively on the form of statements
and not on their meaning. The idea is to find universal rules that apply to all complex statements, depending only on their form.

Needless to say, mathematics, just as any other systematic field of study, is very much concerned with the meaning of its assertions. However, a careful analysis of these assertions reveals that certain formal, logical relationships occur again and again. Therefore, it is profitable to study these formal relationships in their own right as tools or short cuts for constructing and understanding mathematical statements.

Profitability aside, when the basic tools of symbolic logic are combined with the concepts of set theory, as we do later, the resulting mix is powerful enough to generate virtually all of what we mean by mathematics. Later chapters will substantiate this claim by showing how to develop many of the notions and theorems of analysis, algebra, and geometry in this way.

1. Truth-value

As defined in the Glossary, a statement is a meaningful assertion that is either true or false. It is sometimes convenient to express the truth or falsity of a statement as though it were a certain numerical value assigned to the statement. We call this its truth-value. More precisely, if \( P \) is a statement that is true, we say that its truth-value is 1 and express this as \( tv(P) = 1 \); if \( P \) is false, we say that its truth value is 0 and write \( tv(P) = 0 \).

2. Elementary logical operations and truth-values

Suppose we are considering two statements, which we call \( P \) and \( Q \) for short. The Glossary describes four ways of using logical connectives to construct new statements from these:

- **negation:** \( not P \), written symbolically as \( \neg P \);
- **conjunction:** \( P \text{ and } Q \), written symbolically as \( P \land Q \);
- **disjunction:** \( P \text{ or } Q \), written symbolically as \( P \lor Q \);
- **implication:** \( P \text{ implies } Q \), written symbolically as \( P \Rightarrow Q \);

We adjoin to these one more operation, which is “trivial,” in the sense that it does nothing: it is the identity operation, which, given, say, \( P \), just produces \( P \) again. This is
not interesting in and of itself, but it is convenient to have when discussing more general operations later.

These constructions are called *elementary logical operations*. The symbolic expression on the right corresponding to each operation is called an *elementary logical expression*. It gives a convenient shorthand for describing the operation and for building more complex operations. The statements $P$ and $Q$ in the expressions are called *atomic statements*, or more simply, *atoms* of the expression, since they are not resolved more finely into subsidiary statements. The entire statement formed in this way from the atoms is sometimes called a *compound statement*.

It is remarkable that all of what we call deductive reasoning (without quantification) consists of what we can construct by repeating or combining the above simple operations. Before going into how such combination works, let us first look at the relationship between the operations and truth values.

We are interested in how the elementary logical operations behave with respect to truth-values; i.e., how the truth values of

$$P, \quad \neg P, \quad P \land Q, \quad P \lor Q, \quad P \Rightarrow Q$$

relate to the truth-value of the atom $P$ and the truth value of the atom $Q$. Note that we are not simply playing a game with symbols here. We are interested in using the symbolism we introduced to model what actually happens when we, as human beings, reason about certain aspects of the world described by various statements. Therefore, truth-values should be assigned in such a way as to reflect these well-known patterns in reasoning. That is, we should determine the appropriate assignment of truth values for each elementary operation by referring to its meaning.

2.1. **Identity.** This operation does nothing to the given statement $P$, so it obviously does not affect the truth-value.

2.2. **Negation.** By definition, the negation $\neg P$ of the statement $P$ asserts the contrary of $P$. This means that when $tv(P) = 1$, then $tv(\neg P) = 0$, and when $tv(P) = 0$, then $tv(\neg P) = 1$. 


2.3. **Conjunction.** Since $P \land Q$ asserts both $P$ and $Q$, we have $tv(P \land Q) = 1$ when both $tv(P) = 1$ and $tv(Q) = 1$, but $tv(P \land Q) = 0$ otherwise. That is, $tv(P \land Q) = 0$ whenever at least one of $tv(P) = 0$ or $tv(Q) = 0$ and only then.

2.4. **Disjunction.** By definition, $P \lor Q$ affirms at least one of the statements $P$ or $Q$. Therefore, $tv(P \lor Q) = 1$ whenever at least one of $tv(P) = 1$ or $tv(Q) = 1$; $tv(P \lor Q) = 0$ otherwise, i.e., when both $tv(P) = 0$ and $tv(Q) = 0$.

2.5. **Implication.** The truth-values produced by the operations of identity, negation, conjunction and disjunction flow in a straightforward way from their meanings in ordinary English. The case of implication is somewhat different.

When we say $P$ implies $Q$ in ordinary English, we usually refer to a situation in which $Q$ is causally or inferentially connected to $P$. For example, when we say “If it is sunny tomorrow, then Jane will go swimming,” we have in mind a fairly complex set of circumstances connecting the weather to Jane’s activities.

The mathematical operation $P \implies Q$, however, does not delve into such connections. Yes, the definition is motivated by the ordinary usage of the word “implication.” But technically, the definition is expressed only in terms of truth-values. The implication $P \implies Q$ is deemed to be true unless it is falsified. And it is falsified (i.e., false) precisely when $P$ is true and $Q$ is false. Notice that when $P$ is false, $P \implies Q$ cannot be falsified, so it is true in this case. We sometimes say in this case that $P \implies Q$ is vacuously true.

We now give a few examples of $P \implies Q$ (or “if $P$, then $Q$”).

(a) Let $n$ denote an integer. If $n$ is even and is a perfect square, then $n$ is divisible by 4.

(b) Suppose you are given a right triangle. If one of the angles of the right triangle is $45^\circ$, then the triangle is isosceles.

(c) Consider a real number $x$. If $x^2 + 1 = 0$, then $x$ is negative.

(d) Let $R$ denote a square. If $R$ has side of length 3, then the area of $R$ equals 6.

In example (a), if $n = 16$, then both $P$ and $Q$ are true. But if $n = 7$, both are false. However, in either case, $P \implies Q$ is true because it is not falsified. Indeed, there is no value of $n$ that falsifies $P \implies Q$ in this example.
Example (b) is similar. Either both \( P \) and \( Q \) are true (which happens when one of the angles is \( 45^\circ \)) or both are false (when no angle is \( 45^\circ \)). In either situation, \( P \Rightarrow Q \) is not falsified, so it’s true.

In example (c), no value of \( x \) satisfies \( P \). That is, it is false whatever \( x \) is considered. Therefore, \( P \Rightarrow Q \) is not falsified for any \( x \), and so it’s true for all \( x \).

In example (d), \( P \) is false precisely when \( R \) has a side of length other than 3, so \( P \Rightarrow Q \) is vacuously true in all these cases. However, when the side has length 3, then \( P \) is true and \( Q \) is false, so \( P \Rightarrow Q \) is then false.

To summarize, we have the following rules about the truth-values of implication:

\[
\text{tv}(P \Rightarrow Q) = 1 \quad \text{when either} \quad \text{tv}(P) = 0 \quad \text{or when} \quad \text{tv}(Q) = 1;
\]
\[
\text{tv}(P \Rightarrow Q) = 0 \quad \text{when} \quad \text{tv}(P) = 1 \quad \text{and} \quad \text{tv}(Q) = 0.
\]

There is a more convenient way of summarizing this rule by using truth tables, as we explain shortly.

A number of ordinary-English constructions are used as synonyms for “\( P \) implies \( Q \)”: “if \( P \), then \( Q \),” “\( P \) only if \( Q \),” “\( P \) is sufficient for \( Q \),” “\( Q \) is necessary for \( P \),” “\( Q \) is a consequence of \( P \),” “\( Q \) follows from \( P \).” The statement \( P \) is often called the hypothesis or antecedent of the implication, and the statement \( Q \) is often called the conclusion or consequence.

**Exercise 1.** Convince yourself, by using specific examples of statements for \( P \) and \( Q \), that the statements just mentioned are truly synonyms for “\( P \) implies \( Q \).”

**Exercise 2.** Some statements do not appear to be implications, but they can be reformulated so as to be implications. For example, the statement “The square of a real number is non-negative” can be reformulated as “If \( x \) is a real number, then \( x^2 \geq 0 \).” Reformulate the following statements as implications:

- Every differentiable function is continuous.
- All right angles are equal.
- A matrix with a zero eigenvalue is not invertible.
Exercise 3. Identify each of the following statements as a non-trivial compound statement, indicating the atoms and the logical operation that are used. In case the statement is an implication, indicate which atom is the hypothesis and which is the conclusion. (Note: the statement is not necessarily true.)

- A necessary condition for a positive integer \( n \) to be a prime is that it be odd.
- Base angles of an isosceles triangle are equal.
- All that glitters is not gold.
- Both 97 and 87 are prime.
- At least one of the integers 71 and 73 is prime.

2.6. Truth-value dependence.

The elementary logical connectives are modeled after our real-world usage of these terms, and we use the real-world meanings of the connectives to justify our assignment of truth values to the resulting compound statements. However, we are not concerned with the particular meanings of the atomic statements. Our assignment of truth values has the feature that a compound statement \( S \) formed from atoms \( P \) and \( Q \) via an elementary logical operation has truth-value \( tv(S) \) depending only on \( tv(P) \) and \( tv(Q) \) and not on any further aspects of the meaning of \( P \) or of \( Q \). Therefore, for the purposes of looking at truth-values, we are liberated from any complex analysis of meanings (i.e., from semantics) and can focus entirely on the formal, syntactic way that compound statements are constructed from their atoms.

These logical constructions, which we look at more carefully later, have an algebraic flavor to them, since both propositional calculus and traditional algebra involve the manipulation of atomic symbols and connectives. This similarity is not accidental. One of the founding works of symbolic logic is George Boole’s 1848 treatise, “The Laws of Thought,” in which he developed symbolic logic in an algebraic form. The modern descendant of his work is known as a Boolean algebra; it plays an important role in computer design. The relevant “number” system for such algebra is the field of two elements, or what is sometimes called ‘mod two arithmetic.’
3. MOD 2 ARITHMETIC AND TRUTH-VALUES

The symbolism used for the elementary logical operations is suggestive of algebraic notation, and, indeed, we shall soon discuss how to combine the operations in an algebraic manner. However, we can already use fairly standard algebra when working with the truth-values of statements and the elementary logical operations. These truth-values are numbers 0 and 1, and there is a well-known ‘mod two’ arithmetic that we shall apply to these.

We all have learned that even and odd integers when added or multiplied satisfy certain rules, such as \( \text{odd} + \text{odd} = \text{even} \), \( \text{odd} + \text{even} = \text{odd} \), \( \text{odd} \times \text{odd} = \text{odd} \), \( \text{odd} \times \text{even} = \text{even} \), etc. If we use the number 0 to represent even numbers and the number 1 to represent odd numbers, then these rules can be displayed in an addition table and a multiplication table as follows:

\[
\begin{array}{c|cc}
+ & 0 & 1 \\
0 & 0 & 1 \\
1 & 1 & 0 \\
\end{array}
\quad \quad \quad \quad 
\begin{array}{c|cc}
\times & 0 & 1 \\
0 & 0 & 0 \\
1 & 0 & 1 \\
\end{array}
\]

These tables define the operations of mod 2 addition and multiplication To simplify notation, we use the usual convention for multiplication and replace the \( \times \) sign by simple juxtaposition. Notice that since addition and multiplication are binary operations (that is, they operate on two numbers at a time), we need to put parentheses around a sum or product when using it in a more complicated expression, just as in ordinary algebra. Sometimes these parentheses may be dropped when there is no possibility of error.

We now use mod 2 arithmetic to express the truth values of elementary logical operations algebraically. Let \( P \) and \( Q \) be any given statements, and let \( tv(P) \) be denoted by \( x \) and \( tv(Q) \) by \( y \).

**Exercise 4.** Verify the following equalities in mod 2 arithmetic.

(a) \( tv(\neg P) = 1 + x \).

(b) \( tv(P \land Q) = xy \).

(c) \( tv(P \lor Q) = x + y + xy \).

(d) \( tv(P \Rightarrow Q) = 1 + x + xy \).
4. Truth tables for the elementary logical operations

From now on, let us consider some set $S$ of statements that is \emph{closed} under the elementary logical operations. That is, whenever $P$ and $Q$ are statements in $S$, then $\neg P$, $P \land Q$, $P \lor Q$, and $P \Rightarrow Q$ are also statements in $S$.

For each such elementary logical expression, its truth-values can be completely described by a small table, which lists all the possible combinations of truth-values of the atoms, and then, next to each combination, gives the corresponding truth-value of the expression. Such a table is called a truth table:

\begin{align*}
\begin{array}{ccc}
P & Q & P \land Q \\
0 & 0 & 0 \\
0 & 1 & 0 \\
1 & 0 & 0 \\
1 & 1 & 1 \\
\end{array} & \begin{array}{ccc}
P & Q & P \lor Q \\
0 & 0 & 0 \\
0 & 1 & 1 \\
1 & 0 & 1 \\
1 & 1 & 1 \\
\end{array} & \begin{array}{ccc}
P & Q & P \Rightarrow Q \\
0 & 0 & 1 \\
0 & 1 & 1 \\
1 & 0 & 0 \\
1 & 1 & 1 \\
\end{array}
\end{align*}

\begin{align*}
\begin{array}{c}
P \\
0 \\
1 \\
\end{array} & \begin{array}{c}
\neg P \\
0 \\
1 \\
\end{array} & \begin{array}{c}
P \\
0 \\
1 \\
\end{array}
\end{align*}

Figure 1. The truth tables of the elementary logical operations

The information in these tables just repeats the information given above in 2.1 — 2.5, but it displays it in a more convenient format. Notice that the number of rows in each truth table depends only on the number of atoms in the elementary logical expression. If there is only one atom, as in negation and identity, the table has two rows plus the header row; if there are two atoms, as in the three other cases, there are four rows plus the header row.

The format of truth tables extends easily to more general logical operations, as we describe next.

5. General logical operations and logical expressions

In using the elementary logical connectives, we can start with one or two statements in $S$ and produce another statement in $S$, and so it is possible to use the end product again in
a similar way. That is we can apply elementary logical operations to statements repeatedly to build more and more complex expressions, each representing a compound statement.

For a random example, suppose that we are given statements $L, M, P, Q$ in $\mathcal{S}$. We may first form, say, $L \land M$ and $P \lor Q$, then form $\neg (L \land M)$ and $P \lor (\neg (L \land M))$, and then, finally,

$$(P \lor Q) \Rightarrow (P \lor (\neg (L \land M))).$$

We have inserted parentheses to indicate that what they enclose is to be regarded as denoting a statement. This avoids possible notational ambiguity when there are many logical connectives floating around in the expression. Since there is no ambiguity in the case of the entire statement, we do not put parentheses around the entire expression.

The resulting expression describes a statement in $\mathcal{S}$. It is built by applying the elementary logical operations to some of the statements $L, M, P, Q$ to get new statements, then using these and the original statements and logical connectives to get further statements, etc., finally, applying an elementary operation to the two penultimate statements to get the final expression. In this particular case, the last operation performed is an implication applied to the penultimate statements $P \lor Q$ and $P \lor (\neg (L \land M))$. The expression we obtain for the end result is a convenient representation of how it is constructed.

Here is another very simple example that deserves special attention because it is used so often: namely, consider the expression

$$(P \Rightarrow Q) \land (Q \Rightarrow P),$$

which, of course says that $P$ implies $Q$ and $Q$ implies $P$. Because of its frequent use, it receives a special symbol, just like one of the elementary operations: namely, we write $P \iff Q$.

Most typically, we express this in English as “$P$ if and only if $Q$,” but we also sometimes use as synonyms “$P$ is equivalent to $Q$,” “$P$ is logically equivalent to $Q$ or “$P$ is necessary and sufficient for $Q$.” Mathematicians sometimes use the shorthand notation “iff” to stand for “if and only if.”
Exercise 5. Convince yourself that the above synonyms really do say the same thing about the relationship between $P$ and $Q$ as “$P$ if and only if $Q$.”

In general, a *logical operation* is defined to be the application of a sequence of elementary logical operations to statements $P, Q, R, \ldots$ of $S$, as in the two examples above. The result is called a *logical expression*, and $P, Q, R, \ldots$ are called its *atoms*, just as before. This description can be made more precise and formal, but that is not needed for our purposes. We may denote such a general logical operation or expression by such symbols as $L(X_1, X_2, \ldots, X_r)$ or perhaps $G(P_1, P_2, \ldots, P_r)$, or $F(P, Q, R, S)$, where $X_1, X_2, P_1, P_2, P, Q$ etc., denote the atoms in the expressions. When we do not care to be specific about naming the atoms, we may write the expressions simply as $L$, $G$, or $F$.

Given logical expressions $F$ and $G$, we may choose to go further and use them to build other more complex logical expressions by using elementary logical operations on them. For example, we might want to construct $F$ and then apply negation to it. We can denote this simply as $\neg F$. Or, we might want to construct $F$ and $G$ and then form the conjunction of the two. This can be conveniently denoted by $F \land G$. Therefore, using this convention, we can apply all of the elementary logical operations to $F$ and $G$, obtaining new logical expressions

$$F, \neg F, F \land G, F \lor G, F \Rightarrow G.$$  

We also may apply the non-elementary logical operation $\iff$ to form $F \iff G$, with the same understanding as above as to what this means.

6. Truth tables for general logical operations

Since a general logical expression is built by successively applying elementary operations, its truth-value depends only on the truth-values of the individual atoms. Therefore, just as for elementary logical expressions, a general logical expression has a truth table. This is a rectangular array with initial columns (starting on the left side) headed by the atoms of the expression, and the last column (on the right) headed by the expression itself. There may be intermediate columns to represent subsidiary terms of the expression. Each row corresponds to a specific assignment of truth values to the atoms. So, if there are $r$ atoms,
there must be $2^r$ rows to accommodate all the possible combinations of such truth-value assignments.

**Exercise 6.** Check the validity of this last assertion for the value $r = 4$. Can you explain why it is valid in general?

In each row the atoms are assigned some set of truth values, and then a truth value is filled in for every subsequent column according to the rules established for the elementary operations.

As an example of such a truth table, let us consider the following logical expression with three atoms, say, $F = F(P, Q, R) = (P \land R) \Rightarrow (Q \lor R)$.

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$P$</td>
<td>$Q$</td>
<td>$R$</td>
<td>$P \land R$</td>
<td>$Q \lor R$</td>
<td>$F$</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Figure 2.** The truth table of $(P \land R) \Rightarrow (Q \lor R)$

Since the number of atoms is three, the truth table of $F$ has eight rows. We have inserted columns corresponding to the subsidiary terms $P \land R$ and $Q \lor R$.

This example of a truth table is fairly typical in most respects, except that its last column consists entirely of 1's. This does not happen in general, as can be seen by looking at the truth tables for the elementary logical operations. When this does happen, however, it means that no matter what the truth-values of the atoms, the end result is always true. Therefore, such an operation is what we called in the Glossary a tautology. To summarize, a tautology is a logical expression such that the last column in its truth table consists entirely of 1's.
As noted in the Glossary, the opposite of a tautology is called a contradiction. This can be described as a logical expression whose truth table has only 0’s in its last column.

Obviously, if a logical expression \( F \) is a tautology, then \( \neg F \) is a contradiction, and, conversely, if \( F \) is a contradiction, then \( \neg F \) is a tautology.

**Exercise 7.** Verify that each of the following logical expressions is a tautology by computing its truth table:

(a) \( P \lor \neg P \).

(b) \( \neg(P \land \neg P) \).

(c) \( (P \Rightarrow \neg(P) \land (\neg(P) \Rightarrow P) \).

(d) \( P \Rightarrow (P \lor Q) \).

(e) \( (P \land (P \Rightarrow Q)) \Rightarrow Q \).

(f) \( (P \Rightarrow Q) \Rightarrow (\neg Q \Rightarrow \neg P) \).

(g) \( (\neg Q \Rightarrow \neg P) \Rightarrow (P \Rightarrow Q) \)

(h) \( ((P \Rightarrow Q) \land (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R) \).

**Exercise 8.** Construct the truth table for \( P \iff Q \), including columns for the subsidiary statements \( P \Rightarrow Q \) and \( Q \Rightarrow P \).

If you do this exercise correctly, you will see that \( P \iff Q \) is true precisely when \( P \) and \( Q \) have the same truth-values, and it is false otherwise.

**Exercise 9.** Construct truth tables for the following logical expressions:

(a) \( (P \lor Q) \Rightarrow P \).

(b) \( P \Rightarrow (P \land Q) \).

(c) \( (\neg P \lor Q) \land (\neg R \lor P) \).

**Exercise 10.** (a) Display the truth tables for \( A = P \land Q, B = \neg P \land Q, C = P \land \neg Q, \) and \( D = \neg P \land \neg Q \). Then compute the truth tables for \( A \lor B, C \lor D, \) and \( B \lor C \lor D \).
Suppose you are given a column 4-tuple of 0’s and 1’s. Explain how to construct an expression with atoms $P$ and $Q$ whose truth table has that as its last column. (Hint: If the 4-tuple has only 0’s, construct some contradiction involving $P$ and $Q$. If the 4-tuple has at least one 1, explain how a suitable disjunction of $A$, $B$, $C$, and $D$ from part (a) will do the trick.)

Consider truth tables for expressions involving exactly two atoms (i.e., four rows plus the row of headers). Call such a table reduced if it has no intermediate columns, i.e., it has only columns for the atoms and for the entire expression. Show that there are at most 16 reduced truth tables for logical expressions involving two atoms.

Use (b) to show that there are at least 16 reduced truth tables for logical expressions involving two atoms.

What would you guess the number to be for expressions with three atoms? Or $n$ atoms? How would you prove that these are indeed the correct numbers? (Don’t try to give a proof. Just explain what you would need to verify.)

7. LOGICAL EQUIVALENCE

Now let $F$ and $G$ be any logical expressions involving the same number of atoms, say $r$ of them, each atom ranging over all the statements in $S$. We shall say that $F$ and $G$ are logically equivalent, provided that, for all possible statements, $P_1, P_2, \ldots, P_r$ in $S$, $F(P_1, P_2, \ldots, P_r)$ has the same truth-value as $G(P_1, P_2, \ldots, P_r)$. According to the comment after Exercise 8, we may formulate this as follows: $F$ and $G$ are logically equivalent provided that the compound expression $F \iff G$ is a tautology, i.e., the last column of the truth table for $F \iff G$ consists entirely of 1’s. We may abbreviate this by simply writing $F \iff G$.

This definition has the following obvious consequences for any logical expressions $F, G$, and $H$:

(a) $F \iff F$.

(b) If $F \iff G$, then $G \iff F$.

(c) If $F \iff G$ and $G \iff H$, then $F \iff H$. 
Each of these assertions may easily be checked by simply looking at the truth-values of the expressions $F, G, H$ for any choice of truth-values of atomic statements $P_1, P_2, \ldots, P_r$.

The following exercise presents properties of logical equivalence which show that it respects the elementary logical operations.

**Exercise 11.** Suppose that $F \iff F'$ and $G \iff G'$.

(a) Verify that

\[
\neg F \iff \neg F', \quad (F \land G) \iff (F' \land G'), \quad (F \lor G) \iff (F' \lor G'),
\]

\[(F \Rightarrow G) \iff (F' \Rightarrow G').\]

(b) Verify that $(F \iff G) \iff (F' \iff G')$.

(c) Suppose that $L$ is any logical expression involving two atoms. Can you show that

$L(F, G) \iff L(F', G')$? (Hint: Show that $L(F, G)$ has the same reduced truth-table as $L(F', G')$.)

This exercise suggests the general fact that we may always substitute logical expressions for logically equivalent ones without affecting truth-values. We shall be using this general fact frequently.

It remains to give some useful examples of logical equivalences. The following exercise lists eight of the most commonly used equivalences.

**Exercise 12.** Verify the following logical equivalences:

(a) $P \land (Q \lor R) \iff (P \land Q) \lor (P \land R)$

(b) $P \lor (Q \land R) \iff (P \lor Q) \land (P \lor R)$

(c) $\neg(\neg P) \iff P$

(d) $\neg(P \land Q) \iff \neg P \lor \neg Q$

(e) $\neg(P \lor Q) \iff \neg P \land \neg Q$

(f) $P \Rightarrow Q \iff (\neg P) \lor Q$

(g) $P \Rightarrow Q \iff \neg Q \Rightarrow \neg P$

(h) $\neg(P \Rightarrow Q) \iff P \land \neg Q$. 


Notice that equivalences (a) and (b) resemble the *distributive law* for multiplication and addition in ordinary arithmetic.

The implication on the right in item (g) is known as the *contrapositive* of the implication $P \Rightarrow Q$, as described in the Glossary. This logical equivalence leads to a very useful method for proving implications, as we discuss later. Logical equivalence (f) also involves implication. It shows that implication may be expressed in terms of negation and disjunction.

Equivalences (d) and (e) are known as *DeMorgan’s Laws*. They show how negation affects disjunction and conjunction, which is often useful in proofs. The following exercise, asks the student to apply De Morgan’s laws to slightly more complicated expressions.

**Exercise 13.** Derive the following logical equivalence from the logical equivalences in Exercise 12, giving your reasons for each step.

$$
\neg (P \vee (Q \land R)) \iff (\neg P \land \neg Q) \lor (\neg P \land \neg R).
$$

### 8. Rules of Inference and Proofs

The Glossary describes a proof of a mathematical statement $P$ as a valid chain of reasoning that begins with statements known to be true and concludes with $P$. More precise terminology would probably call this a description of a *deductive proof*, since it presents a stepwise process in which each step involves a deduction or inference. Indeed this is the notion of proof that we shall be focusing on throughout this course. It is, however, worth pointing out that there is a more general concept of proof that does play a role in mathematics.

In its most general sense, a proof can be defined simply as a convincing argument, or even better, as a convincing demonstration. Logical steps and rules of inference are not a necessary part of this definition. With this notion of proof, the demonstration may appear holistically, perhaps visually, and it is often at least as convincing as any deductively linked chain of statements. We give one example of this, which is a well-known proof of the Pythagorean Theorem.
Recall that the Pythagorean Theorem states that in a right triangle with sides of lengths $a$ and $b$ and hypotenuse of length $c$, the quantities $a, b$ and $c$ satisfy the relation $a^2 + b^2 = c^2$.

There are many, many proofs of this theorem. Euclid’s proof, among many others, is a deductive proof, since it is essentially a compilation of deductive steps that begin with Euclid’s axioms for geometry. But there are also holistic proofs, that is, proofs which demonstrate the result more or less directly by means of a picture. The following pair of diagrams comprise the picture that provides perhaps the most direct and convincing example of this.

Both large squares pictured are assumed to be congruent, so that they have the same area. In each square, there are four right triangles, all congruent but assembled differently in each square. The viewer is invited to draw the obvious conclusion that the remaining regions in each large square have equal areas. In the right-hand picture, the remaining region is a square with side of length $c$—hence, area $c^2$— whereas in the other picture, the remaining region is comprised of two non-overlapping squares of sides $a$ and $b$, respectively—hence, with total area $a^2 + b^2$. So, as Agatha Christie’s Hercule Poirot would say, “Voila, Hastings, my little grey cells perceive that the Pythagorean Theorem is correct.”

Now the careful reader may notice that it is possible to reduce the “picture-proof” to a deductive proof by being very precise and painstaking about how the two large squares are constructed, how the areas are computed, how the regions are compared, and so on. And this is true. Indeed, to my knowledge, there is no proof, holistic or otherwise that cannot be reduced to a deductive proof in this manner. It follows that deductive proofs can be taken as the universal proof procedure, provided we are principally interested in using the
method of proof as a validating procedure. Indeed, this is our interest and what we shall do in this course. The above “picture-proof” shows that other kinds of proof are possible and may reveal geometric relationships or stimulate other intuition in the way some deductive proofs would not. This is their great strength. Their weakness is that, almost by definition, they resist systematization. It is very difficult to teach how to have a stroke of genius.

To be sure, deductive proofs often also require such ingenuity, particularly in their initial conception. But because the construction of a deductive proof proceeds by breaking a problem down into smaller problems, and then perhaps these, in turn, into yet smaller ones — cf., the “divide and conquer” rule of computer programming — the deductive approach can reduce the amount of high-level ingenuity required. In this way, there is a chance that many useful mathematical results can be proved by all of us.

What we describe in this section are techniques for beginning a deductive proof of some statement $P$ according to the form of $P$ as a compound statement. This often reduces the problem of constructing a proof to smaller problems which can then be attacked in the same way. However, the specific choices and steps that you use to “fill in” this architecture will still require your active imagination.

To begin, we discuss the basic dynamic principles in proofs: rules of inference. We then discuss different possible logical structures for proofs—the “architecture”— and give examples. The rules of inference and logical structures will all be based on our discussion of the propositional calculus.

Further practical tips for doing the “nitty-gritty” of proving something can be found in Solow’s book, “How to Read and Do Proofs,” and will also be discussed in class.

In subsequent parts of these notes, we shall encounter some more specific kinds of tools of proof, including the method of induction and various counting arguments.

8.1. Rules of Inference. As defined in the Glossary, a rule of inference is what allows us to proceed correctly from one set of statements to another statement. It provides the dynamic that allows us to prove theorems. There is one basic rule of inference in logic from which any other may be derived. It has a Latin name, *modus ponens*, because it was first
used by the ancient Greeks. :-) We shall first say informally what *modus ponens* is, and then we discuss how it ties in with logical operations.

*Modus ponens* tells us that if \( S \) and \( T \) are two statements such that \( S \) and \( S \implies T \) are true, then we may deduce that \( T \) is true. This follows from the meaning of implication, as we discussed earlier, because in the presence of a true \( S \), a false \( T \) provides precisely the criterion for \( S \implies T \) to be false. And this last is contrary to assumption. Therefore, the two true statements \( S \) and \( S \implies T \) lead to the true statement \( T \). To summarize:

\[
S \text{ true and } (S \implies T) \text{ true yield } T \text{ true.}
\]

The *modus ponens* rule also may be viewed as simply our interpretation of the tautology \((P \land (P \implies Q)) \implies Q\) (cf. Exercise 7(e)).

*Modus ponens* can also be used with logical operations, say \( F \) and \( G \), both built from atomic statements \( P_1, P_2, \ldots \). Suppose that some choices of these statements are such that the corresponding expressions \( F(P_1, P_2, \ldots) \) and \( F(P_1, P_2, \ldots) \implies G(P_1, P_2, \ldots) \) are true. Then, *modus ponens* allows us to conclude that \( G(P_1, P_2, \ldots) \) is true. The reasoning for this is the same as before.

*Modus ponens* can be used to derive other rules of inference. We give one example here. Suppose we know that \( T \) is false and that \( S \implies T \) is true. We may then use *modus ponens* to prove that \( S \) is false. For, were \( S \) true, *modus ponens* would imply that \( T \) is true, which it isn’t. So \( S \) is false. This is the basis for so-called *proof by contrapositive*, which we discuss further below. So, *modus ponens* implies the rule of inference:

\[
T \text{ false and } (S \implies T) \text{ true yield } S \text{ false.}
\]

This rule also has a Latin name: *modus tolens*. However, we shall not use this name because *modus tolens* and other such rules can be derived from *modus ponens*. Instead, we usually say something like “by an application of *modus ponens*.”

**Exercise 14.** Show that the following rule can be derived from *modus ponens*: Suppose \( P, Q \) and \( R \) are statements such that \( P \implies Q \) is true and \( Q \implies R \) is true. Then, the statement \( P \implies R \) is true. (Hint: Use Exercise 7(h).)

**8.2. Methods of proof.** Every proof in mathematics may be viewed as the derivation of some conclusion \( B \) from some hypothesis \( A \). Sometimes \( A \) remains tacit, as part of the
background, but often it is given explicitly. The task is to prove that the implication \( A \Rightarrow B \) is true. Once this is done, the validity of \( A \) produces the desired validity of \( B \) by *modus ponens*.

But how do we prove \( A \Rightarrow B \)? The detailed answer to this, of course, will depend on the particulars of \( A \) and \( B \), but one basic step is always used: namely, we assume that \( A \) is true, and then use that information, together with any other knowledge we have that is appropriate to the mathematical context, to derive the statement \( B \). Notice that to proceed, we do not need to know whether \( A \) is actually true or not; we simply assume the truth. This approach is justified in precisely the same way that we justified the truth-values in the truth table for implication. For, to assert \( A \Rightarrow B \) means only that \( B \) holds whenever \( A \) does. So, if we can verify that \( B \) is true under the assumption that \( A \) is true, we have eliminated the only possibility for the implication to fail.

The book by Solow, gives a number of techniques for proving \( A \Rightarrow B \), classified according to the particular form that \( A \) or \( B \) takes. Here, we look at some of these from the viewpoint of symbolic logic, seeing that *the methods are simply consequences of certain tautologies or logical equivalences in the propositional calculus*. We cover only some of the methods, because others will require the concepts and techniques of quantification, which we shall discuss later.

We now give some examples of the methods, all of which refer to the implication \( A \Rightarrow B \). In these examples, we shall be assuming facts from earlier mathematics courses, such as basic facts from geometry, algebra, and so on. Solow’s book provides a convenient, short list of some of these in his Chapter 3, p.24

**direct proof:** Assume \( A \) (plus already established facts) and prove \( B \). This is the basic task, as we’ve already discussed. In many simple cases, no further formal technique is needed or helpful. What is needed on a practical level is an understanding of precisely what \( A \) and \( B \) are saying, determining some commonality between them, and then using this knowledge to “build a logical bridge” from \( A \) to \( B \). This is the “filling in” mentioned earlier.
proof by contradiction: Assume $A$ and $\neg B$ and derive a contradiction $C$. This method is based on the logical equivalence

$$(A \Rightarrow B) \iff ((A \land \neg B) \Rightarrow C),$$

where $C$ is any (conveniently chosen) contradiction. This logical equivalence can be verified by checking truth tables.

proof by contrapositive: Assume $\neg B$ and derive $\neg A$. This method is based on the logical equivalence

$$(A \Rightarrow B) \iff (\neg B \Rightarrow \neg A).$$

either/or method, type I: This method applies when the statement $A$ is a disjunction, say $A = E \lor F$. In this situation, you must do two proofs: namely, you must prove both $E \Rightarrow B$ and $F \Rightarrow B$. Thus, separately, assume $E$ and derive $B$ and also assume $F$ and derive $B$. This method is based on the logical equivalence

$$(E \lor F \Rightarrow B) \iff ((E \Rightarrow B) \land (F \Rightarrow B)).$$

either/or method, type II: This method applies when the statement $B$ is a disjunction, say $B = E \lor F$. In this case you have a choice of one of two possible methods. Either assume both $A$ and $\neg E$ and then derive $F$; or assume both $A$ and $\neg F$ and then derive $E$. This method is based on the two logical equivalences

$$(A \Rightarrow (E \lor F)) \iff ((A \land \neg E) \Rightarrow F)$$

and

$$(A \Rightarrow (E \lor F)) \iff ((A \land \neg F) \Rightarrow E).$$

Exercise 15. Verify each of the logical equivalences used in the two "either/or" methods above by computing truth tables for the expressions on each side of the equivalence.

More generally, any logical expression that is logically equivalent to $A \Rightarrow B$ can be used to obtain a method of proof of $A \Rightarrow B$. The ones just described above are perhaps the most
common, but they are not the only ones. Again, the particulars of the statements \( A \) and \( B \) will suggest which method to use.

We now give a few examples. We won’t always give complete proofs here, only the translations of the above methods into concrete terms.

**Examples of the methods above**

- Construction of a **direct proof** of \( B \), given \( A \) and other prior information, depends completely on the context, the nature of \( A \) and \( B \), the extent of prior knowledge, and so on. The point of this category is to focus on situations in which no further *formal* reduction of the problem into logically simpler constituents is obvious.

  **Here is one example from number theory:** Let \( A \) be the statement “\( m \) and \( n \) are odd integers, and let \( B \) be the statement “\( mn \) is an odd integer.” A direct proof of \( A \Rightarrow B \) might go as follows: We must find a way to relate the “oddness” of two numbers to the oddness of their product. Since forming a product is an algebraic operation, we want to express the fact that a number is odd in algebraic terms. From basic facts about integers, we know that to say that an integer is odd is equivalent to asserting that it has the form \( 2i + 1 \), for some integer \( i \). Therefore, by \( A \) we know that there are integers \( k \) and \( \ell \) such that \( m = 2k + 1 \) and \( n = 2\ell + 1 \). Then, we calculate \( mn = (2k + 1)(2\ell + 1) = 4k\ell + 2(k + \ell) + 1 = 2(2k\ell + k + \ell) + 1 \), which shows that \( mn \) has the needed form.

  **Here is one example from geometry:** Let \( A \) state that \( \Delta \) is an isosceles right triangle of area 8, and let \( B \) state that \( \Delta \) is an isosceles right triangle with hypotenuse of length \( 4\sqrt{2} \). Here, the commonality between \( A \) and \( B \) is that they both refer to quantities that involve the length \( s \) of the (non-hypotenuse) side of \( \Delta \). The area of a triangle equals \( 1/2 \) its base times its altitude, which is \( s^2/2 \) in the case of \( \Delta \). The hypotenuse of \( \Delta \) equals \( \sqrt{2s^2} \), by the Pythagorean Theorem. The proof then may be concluded by using the hypothesis that \( \text{area}(\Delta) = 8 \) to solve for \( s \).

  We give one further example from geometry in the form of an exercise.
Exercise 16. Let $A$ be the statement “$\Delta$ is a right triangle with one side of unit length and the other side of length $x$,“ and let $B$ be the statement “ The area of $\Delta$ is less than the length of the hypotenuse squared.” Prove $A \Rightarrow B$.

(a) Verify that $B$ is logically equivalent to the statement $x^2 - x/2 + 1 > 0$.

One important thing to notice at this point is that we do not know the value of $x$. We are not given a specific value of $x$ and asked to check the result for that. That is a trivial task. We are asked to prove something valid for a general $x$, that is for a general right triangle with one side of unit length. We need a general method or argument that guarantees the validity of the inequality for any value of $x$. There are at least two ways to proceed.

(b) For those comfortable with the methods of calculus, show that the minimum of the function $y = x^2 - x/2 + 1$ is achieved at $x = 1/4$. Conclude that the minimum function value is $y = 15/16$. Since this is the smallest value the function can assume, the inequality $x^2 - x/2 + 1 > 0$ holds for all $x$.

(c) For those who prefer to use algebra, complete the square of the quadratic expression $x^2 - x/2 + 1$. Namely, show that $x^2 - x/2 + 1 = (x - 1/4)^2 + 15/16$. Conclude that the original expression must be positive for all $x$.

This completes the proof.

- For proof by contradiction, we use a simple example involving positive integers $n$. Let $A$ be the statement “$n^2$ is odd,” and let $B$ be the statement “$n$ is odd.” Then, to prove $A \Rightarrow B$ by contradiction, we assume that both $n^2$ is odd and $n$ is not odd (i.e., it’s even) and derive a contradiction. We leave this last step to the reader.

- For proof by contrapositive, we could use the previous example and try to prove that $\neg A \Rightarrow \neg B$, which translates to: $n$ even implies $n^2$ even. The reader should be able to check this immediately. This example shows that proof by contradiction and proof by contrapositive are very similar. Often it’s simply a matter of taste to use one or the other. We’ll discuss this further in class.

- For the either/or method, type I, suppose that $T$ denotes either an equilateral triangle or a square, and consider the following statement: If $T$ has perimeter of
length $P$, then its area is $< P^2/12$. First notice that, although the hypothesis does not look like a disjunction, it really is, because $T$ is either an equilateral triangle of perimeter $P$ or a square of perimeter $P$. So, the implication is proved by first verifying that $< P^2/12$ when $T$ is an equilateral triangle of perimeter of length $P$ and then verifying the inequality when $T$ is a square with perimeter of length $P$. (Or do these in the reverse order.) We do not work out the geometric proof here but may discuss this in class.

This example suggests that this method of proof can be thought of as dealing with two separate cases; in each case separately, the conclusion must be verified. From this viewpoint, there is nothing special about the fact that we are dealing with two cases; there could be three or even more. In fact the hypothesis $A$ could be a disjunction $E \lor F \lor G \lor \ldots$ of many statements, thus requiring separate proofs of each of the implications $E \Rightarrow B$, $F \Rightarrow B$, $G \Rightarrow B$, etc. This could then be called the method of proof by cases. The logical equivalence given above to justify the method for two cases easily extends to as many cases as we like.

• For the either/or method, type II, let $A$ be the statement “$x$ is a real number satisfying $x^2 = 1$, and let $B$ be the disjunction “$x = 1$ or $x = -1$.” Then, the either/or method, type II, would have us assume $A$ and, say, $x \neq 1$, and then use these to prove $x = -1$. We’ll give a complete proof in this case:

(1) Assuming $A$ and performing the algebraic step of transposition, we get $x^2 - 1 = 0$.

(2) Factoring this expression, we get $(x - 1)(x + 1) = 0$

(3) Using the assumption $x \neq 1$, we conclude that $x - 1 \neq 0$.

(4) Dividing equation (2) by $x - 1$, we get $x + 1 = 0$, from which $x = -1$ follows.

This concludes the proof.