CSC2323 Discrete Structures Lecture Notes

Baffa Sani and Abubakar Sadiq Mustapha

August 1, 2023

Contents

Reference books:

1. Discrete Mathematics and Its Applications By Kenneth H. Rosen
2. discrete mathematics with applications By Susanna S. Epp

1. Propositional Logic and Predicate Logic

Introduction

The rules of logic give precise meaning to mathematical statements. These rules are used to distinguish between valid and invalid mathematical arguments. Because a major goal of this book is to teach the reader how to understand and how to construct correct mathematical arguments, we begin our study of discrete mathematics with an introduction to logic.

Besides the importance of logic in understanding mathematical reasoning, logic has numerous applications to computer science. These rules are used in the design of computer circuits, the construction of computer programs, the verification of the correctness of programs, and in many other ways. Furthermore, software systems have been developed for constructing some, but not all, types of proofs automatically.

1.1 Propositions

A **proposition** (or **statement**) is a declarative sentence (that is, a sentence that declares a fact) that is either ***true*** or ***false***, but not both.

Example 1.1. Consider, the following sentences:.

1. Abuja is the capital of Nigeria.
2. $1 + 1 = 2$.
3. $2 + 2 = 3$.
4. China is in Europe.
5. Where are you going?
6. Do your homework.
7. $x + 1 = 2$.

The first four are propositions, the last three are not. Also, (i) and (ii) are true, but (iii) and (iv) are false.

We use letters to denote propositional variables (or sentential variables), that is, variables that represent propositions, just as letters are used to denote numerical variables. The conventional letters used for propositional variables are p, q, r, s,... . The truth value of a proposition is true, denoted by T, if it is a true proposition, and the truth value of a proposition is false, denoted by F, if it is a false proposition.

Compound Propositions

Many propositions are *composite*, that is, composed of *subpropositions* and various connectives discussed subsequently. Such composite propositions are called **compound propositions**. A proposition is said to be **primitive** (or **atomic**) **propositions** if it cannot be broken down into simpler propositions, that is, if it is not composite.

For example, the above propositions (i) through (iv) are primitive propositions. On the other hand, the following two propositions are composite:

"It is hot and it is not sunny." and "John is smart or he studies every night."

1.2 Basic Logical Operations

This section discusses the three basic logical operations of conjunction, disjunction, and negation which correspond, respectively, to the English words "and," "or," and "not."

Conjunction, $p \wedge q$

Definition 1: Conjunction

Let p and q be propositions. The ***conjunction*** of p and q, denoted by $p \wedge q$, is the proposition "p and q." The conjunction $p \wedge q$ is **true** when both p and q are true and is false otherwise.

Table 1: Truth Table for $p \wedge q$

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Example 1.2. Consider the following four statements:

1. Abuja is the capital of Nigeria and $2 + 2 = 4$.
2. Abuja is the capital of Nigeria and $2 + 2 = 5$
3. China is in Europe and $2 + 2 = 4$.
4. China is in Europe and $2 + 2 = 5$.

Only the first statement is true. Each of the others is false since at least one of its substatements is false.

Definition 2: Disjunction

Let p and q be propositions. The ***disjunction*** of p and q, denoted by $p \vee q$, is the proposition "p or q." The disjunction $p \vee q$ is false when both p and q are false and is true otherwise.

Table 2: Truth Table for $p \vee q$

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Example 1.3. Consider the following four statements:

1. Abuja is the capital of Nigeria and $2 + 2 = 4$.
2. Abuja is the capital of Nigeria and $2 + 2 = 5$
3. China is in Europe and $2 + 2 = 4$.
4. China is in Europe and $2 + 2 = 5$.

Only the last statement (4) is false. Each of the others is true since at least one of its sub-statements is true.

Remark: The English word "or" is commonly used in two distinct ways. Sometimes it is used in the sense of "p or q or both," i.e., at least one of the two alternatives occurs, as above, and sometimes it is used in the sense of "p or q but not both," i.e., exactly one of the two alternatives occurs. For example, the sentence "He will go to BUK or to ABU" uses "or" in the latter sense, called the ***exclusive disjunction***. Unless otherwise stated, "or" shall be used in the former sense. This discussion points out the precision we gain from our symbolic language: $p \vee q$ is defined by its truth table and always means "p and/or q."

Definition 3: Negation

If p is a proposition, the ***negation*** of p is "not p" or "It is not the case that p" and is denoted $\sim p$. It has opposite truth value from p: if p is true, $\sim p$ is false; if p is false, $\sim p$ is true.

Table 3: Truth Table for $\sim p$

p	$\sim p$
T	F
F	T

Example 1.4. Consider the following four statements:

1. Ice floats in water.
2. It is false that ice floats in water.
3. Ice does not float in water.
4. $2+2=5$
5. It is false that $2+2=5$.
6. $2+2\neq 5$

Then (2) and (3) are each the negation of (1); and (5) and (6) are each the negation of (4).

Remark: The logical notation for the connectives "and," "or," and "not" is not completely standardized. For example, some texts use:

p & q, $p\,.\,q$ or pq **for** $p\wedge q$

$p+q$ **for** $p\vee q$

$p\prime$, $\bar{p}$ or $\neg p$ **for** $\sim p$

1.3 Propositions and Truth Tables

Definition 4: Compound Statements

Let $P(p,q,...)$ denote an expression constructed from logical variables $p,q,...$, which take on the value TRUE (T) or FALSE (F), and the logical connectives $\wedge$, $\vee$, and $\sim$ (and others discussed subsequently). Such an expression $P(p,q,...)$ will be called a ***proposition***.

The main property of a proposition $P(p,q,...)$ is that its truth value depends exclusively upon the truth values of its variables, that is, the truth value of a proposition is known once the truth value of each of its variables is known. A simple concise way to show this relationship is through a truth table. We describe a way to obtain such a truth table below.

Example 1.5.

Consider, the proposition $\sim(p\wedge\sim q)$. Table 4 indicates how the truth table of $\sim(p\wedge\sim q)$ is constructed. Observe that the first columns of the table are for the variables $p,q,...$ and that there are enough rows in the table, to allow for all possible combinations of **T** and **F** for these variables. (For 2 variables, as above, 4 rows are necessary; for 3 variables, 8 rows are necessary; and, in general, for n variables, 2^nrows are required.) There is then a column for each "elementary" stage of the construction of the proposition, the truth value at each step being determined from the previous stages by the definitions of the connectives $\wedge$, $\vee$, $\sim$. Finally we obtain the truth value of the proposition, which appears in the last column.

Table 4: Truth Table for $\sim(p\wedge \sim q)$

p	q	$\sim q$	$p\wedge\sim q$	$\sim(p\wedge\sim q)$
T	T	F	F	T
T	F	T	T	F
F	T	F	F	T
F	F	T	F	T

Alternate Method for Constructing a Truth Table

Another way to construct the truth table for $\sim(p\wedge\sim q)$ follows:

(a) First we construct the truth table shown in Table 5. That is, first we list all the variables and the combinations of their truth values. Also there is a final row labeled "step." Next the proposition is written on the top row to the right of its variables with sufficient space so there is a column under each variable and under each logical operation in the proposition. Lastly (Step 1), the truth values of the variables are entered in the table under the variables in the proposition.

(b) Now additional truth values are entered into the truth table column by column under each logical operation as shown in Table 5. We also indicate the step in which each column of truth values is entered in the table.

Table 5: Truth Table for $\sim(p\wedge\sim q)$

p	q	$\sim$	$(p$	$\wedge$	$\sim$	$q)$
T	T	T	T	F	F	T
T	F	F	T	T	T	F
F	T	T	F	F	F	T
F	F	T	F	F	T	F
Step		4	1	3	2	1

Example 1.6. Construct the truth table for the statement form $(p\vee q)\wedge\sim(p\wedge q)$.

Solution. Set up columns labeled p, q, $(p\vee q)$, $(p\wedge q)$, $\sim(p\wedge q)$, and $(p\vee q)\wedge\sim(p\wedge q)$. Fill in the p and q columns with all the logically possible combinations of T's and F's. Then use the truth tables for $\vee$ and $\wedge$ to fill in the $(p\vee q)$ and $(p\wedge q)$ columns with the appropriate truth values. Next fill in the $\sim(p\wedge q)$ column by taking the opposites of the truth values for $(p\wedge q)$.

Table 6: Truth Table for $(p\vee q)\wedge\sim(p\wedge q)$

p	q	$(p\vee q)$	$(p\wedge q)$	$\sim(p\wedge q)$	$(p\vee q)\wedge\sim(p\wedge q)$
T	T	T	T	F	F
T	F	T	F	T	T
F	T	T	F	T	T
F	F	F	F	T	F

■

Example 1.7. Construct the truth table for the statement form $(p\wedge q)\vee\sim r$.

Solution. Make columns headed p, q, r, $p\wedge q$, $\sim r$, and $(p\wedge q)\vee\sim r$. Enter the eight logically possible combinations of truth values for p, q, and r in the three left-most columns. Then fill in the truth values for p ' q and for ,r. Complete the table by considering the truth values for $(p\wedge q)$ and for $\sim r$ and the definition of an *or* statement.

■

Table 7: Truth Table for $(p \wedge q) \vee \sim r$

p	q	r	$p \wedge q$	$\sim r$	$(p \wedge q) \vee \sim r$
T	T	T	T	F	T
T	T	F	T	T	T
T	F	T	F	F	F
T	F	F	F	T	T
F	T	T	F	F	F
F	T	F	F	T	T
F	F	T	F	F	F
F	F	F	F	T	T

1.4 Logical Equivalence

Definition 5: Logical Equivalence

Two propositions $P(p, q, ...)$ and $Q(p, q, ...)$ are said to be logically equivalent, or simply equivalent or equal, denoted by

$$P(p, q, ...) \equiv Q(p, q, ...)$$

if they have identical truth tables.

Example 1.8. Show that $\sim (p \wedge q)$ and $(\sim p \vee \sim q)$ are logically equivalent

Solution. Observe that both truth tables are the same, that is, both propositions are false in the first case and true in the other three cases.

Table 8: Truth Table for $\sim (p \wedge q)$ and $(\sim p \vee \sim q)$

p	q	$\sim p$	$\sim q$	$p \wedge q$	$\sim (p \wedge q)$	$\sim p \vee \sim q$
T	T	F	F	T	F	F
T	F	F	T	F	T	T
F	T	T	F	F	T	T
F	F	T	T	F	T	T

Symbolically,

$$\sim (p \wedge q) \equiv (\sim p \vee \sim q)$$

■

Example 1.9. Show that $\sim (p \vee q)$ and $(\sim p \wedge \sim q)$ are logically equivalent

Solution. Exercise! ■

1.5 Tautologies and Contradictions

Definition 6: Tautologies

Some propositions $P(p, q, ...)$ contain only T in the last column of their truth tables or, in other words, they are true for any truth values of their variables. Such propositions are called tautologies.

Definition 7: Contradictions

A proposition $P(p, q, ...)$ is called a contradiction if it contains only F in the last column of its truth table or, in other words, if it is false for any truth values of its variables.

Example 1.10. Show that $(p \vee \sim p)$ is tautology ■

Solution. We draw the truth table for $(p \vee \sim p)$ as follows:

Table 9: Truth Table for $(p \vee \sim p)$

p	$\sim p$	$(p \vee \sim p)$
T	F	T
F	T	T

Example 1.11. Show that $(p \wedge \sim p)$ is contradiction ■

Solution. We draw the truth table for $(p \wedge \sim p)$ as follows:

Table 10: Truth Table for $(p \wedge \sim p)$

p	$\sim p$	$(p \wedge \sim p)$
T	F	F
F	T	F

Example 1.12. If $\mathbf{t}$ is a tautology and $\mathbf{c}$ is a contradiction, show that $p \wedge \mathbf{t} \equiv p$ and $p \wedge \mathbf{c} \equiv \mathbf{c}$. ■

Solution. We draw the truth table for $p \wedge \mathbf{t} \equiv p$ and $p \wedge \mathbf{c} \equiv \mathbf{c}$ as follows:

Table 11: Truth Table for $p \wedge \mathbf{t} \equiv p$ and $p \wedge \mathbf{c} \equiv \mathbf{c}$

p	$\mathbf{t}$	$p \wedge \mathbf{t}$	$\mathbf{c}$	$p \wedge \mathbf{c}$
T	T	T	F	F
F	T	F	F	F

Theorem 1.1. *Logical Equivalences*

Given any statement variables p, q, and r, a tautology $\mathbf{t}$ and a contradiction $\mathbf{c}$, the following logical equivalences hold.

1. Commutative laws:	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
2. Associative laws:	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
3. Distributive laws:	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
4. Identity laws:	$p \wedge \mathbf{t} \equiv p$	$p \vee \mathbf{c} \equiv p$
5. Negation laws:	$p \vee \sim p \equiv \mathbf{t}$	$p \wedge \sim p \equiv \mathbf{c}$
6. Double negative law:	$\sim (\sim p) \equiv p$	
7. Idempotent laws:	$p \wedge p \equiv p$	$p \vee p \equiv p$
8. Universal bound laws:	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathbf{c}$
9. De Morgan's laws:	$\sim (p \wedge q) \equiv \sim p \vee \sim q$	$\sim (p \vee q) \equiv \sim p \wedge \sim q$
10. Absorption laws:	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
11. Negations of $\mathbf{t}$ and $\mathbf{c}$:	$\sim \mathbf{t} \equiv \mathbf{c}$	$\sim \mathbf{c} \equiv \mathbf{t}$

Example 1.13. Prove theorem 1.1

Solution. Exercise! ∎

Example 1.14. Use Theorem 1.1 to verify the logical equivalence $\sim(\sim p \wedge q) \wedge (p \vee q) \equiv p$

Solution. Use the laws of Theorem 1.1 to replace sections of the statement form on the left by logically equivalent expressions. Each time you do this, you obtain a logically equivalent statement form. Continue making replacements until you obtain the statement form on the right.

$$\begin{aligned}
\sim(\sim p \wedge q) \wedge (p \vee q) &\equiv (\sim(\sim p) \vee \sim q) \wedge (p \vee q) && \text{by De Morgan's laws}\\
&\equiv (p \vee \sim q) \wedge (p \vee q) && \text{by the double negative law}\\
&\equiv p \vee (\sim q \wedge q) && \text{by the distributive law}\\
&\equiv p \vee (q \wedge \sim q) && \text{by the commutative law for } \wedge\\
&\equiv p \vee \mathbf{c} && \text{by the negation law}\\
&\equiv p && \text{by the identity law}
\end{aligned}$$

∎

Example 1.15. Show that $\sim(p \vee (\sim p \wedge q))$ and $\sim p \wedge \sim q$ are logically equivalent by developing a series of logical equivalences.

Solution. Use the laws of Theorem 1.1 to replace sections of the statement form on the left by logically equivalent expressions. Each time you do this, you obtain a logically equivalent statement form. Continue making replacements until you obtain the statement form on the right.

$$\begin{aligned}
\sim(p \vee (\sim p \wedge q)) &\equiv \sim p \wedge \sim(\sim p \wedge q) && \text{by the second De Morgan law}\\
&\equiv \sim p \wedge (\sim(\sim p) \vee \sim q) && \text{by the first De Morgan law}\\
&\equiv \sim p \wedge (p \vee \sim q) && \text{by the double negation law}\\
&\equiv (\sim p \wedge p) \vee (\sim p \wedge \sim q) && \text{by the second distributive law}\\
&\equiv \mathbf{c} \vee (\sim p \wedge \sim q) && \text{because } \sim p \wedge p \equiv \mathbf{c}\\
&\equiv (\sim p \wedge \sim q) \vee \mathbf{c} && \text{by the commutative law for disjunction}\\
&\equiv (\sim p \wedge \sim q) && \text{by the identity law for } \mathbf{c}
\end{aligned}$$

∎

1.6 Conditional and Biconditional Statements

Definition 8: Conditional

Let p and q be propositions. The conditional statement $p \to q$ is the proposition "if p, then q." The conditional statement $p \to q$ is false when p is true and q is false, and true otherwise. In the conditional statement $p \to q$, p is called the **hypothesis** (or **antecedent** or **premise**) and q is called the **conclusion** (or **consequence**).

The conditional $p \to q$ is frequently read "p implies q" or "p only if q." In expressions that include $\rightarrowtail$ as well as other logical operators such as $\wedge$, $\vee$, and $\sim$, the **order of operations** is that $\to$ is performed last. Thus, according to the specification of order of operations, $\sim$ is performed first, then $\wedge$ and $\vee$, and finally $\to$.

Example 1.16. Construct a truth table for the statement form $p \vee \sim q \to \sim p$.

Solution. By the order of operations given above: ∎

Table 12: Truth Table for $p \to q$

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Table 13: Truth Table for $p \vee \sim q \to \sim p$

p	q	$\sim p$	$\sim q$	$p \vee \sim q$	$p \vee \sim q \to \sim p$
T	T	F	F	T	F
T	F	F	T	T	F
F	T	T	F	F	T
F	F	T	T	T	T

Example 1.17. Show That $p \vee q \to r \equiv (p \to r) \wedge (q \to r)$

Solution. Exercise. ∎

Representation of If-Then as Or

The truth table of $\sim p \vee q$ and $p \to q$ are identical, that is, they are both *false* only in the second case. Accordingly, $p \to q$ is logically equivalent to $\sim p \vee q$; that is,

$$p \to q \equiv \sim p \vee q$$

Example 1.18. Show that $\sim (p \to q)$ and $p \wedge \sim q$ are logically equivalent.

Solution. We could use a truth table to show that these compound propositions are equivalent. Indeed, it would not be hard to do so. However, we want to illustrate how to use logical identities that we already know to establish new logical identities, something that is of practical importance for establishing equivalences of compound propositions with a large number of variables. So, we will establish this equivalence by developing a series of logical equivalences, using one of the equivalences in Theorem 1.1

$\sim (p \to q)$	$\equiv$	$\sim (\sim p \vee q)$	by the conditional-disjunction equivalence
	$\equiv$	$\sim (\sim p) \wedge \sim q$	by the second De Morgan law
	$\equiv$	$p \wedge \sim q$	by the double negation law

∎

Example 1.19. Show that $(p \wedge q) \to (p \wedge q)$ is a tautology.

Solution. To show that this statement is a tautology, we will use logical equivalences to demonstrate that it is logically equivalent to **t**. (Note: This could also be done using a truth table.)

$(p \wedge q) \to (p \vee q)$	$\equiv$	$\sim (p \wedge q) \vee (p \vee q)$	by the conditional-disjunction equivalence
	$\equiv$	$(\sim p \vee \sim q) \vee (p \vee q)$	by the first De Morgan law
	$\equiv$	$(\sim p \vee p) \vee (\sim q \vee q)$	by the associative and commutative laws for disjunction
	$\equiv$	$\mathbf{t} \vee \mathbf{t}$	by Example 1 and the commutative law for disjunction
	$\equiv$	$\mathbf{t}$	by the domination law

∎

The Contrapositive of a Conditional Statement

Definition 9: Contrapositive

The **contrapositive** of a conditional statement of the form "If **p** then **q**" is

$$\text{If} \sim q \text{ then} \sim q.$$

Symbolically,

$$\text{The contrapositive of } p \to q \text{ is } \sim q \to \sim p.$$

Example 1.20. Write each of the following statements in its equivalent contrapositive form:

a If John can swim across the lake, then John can swim to the island.

b If today is Sunday, then tomorrow is Monday.

Solution. a If John cannot swim to the island, then John cannot swim across the lake.

b If tomorrow is not Monday, then today is not Sunday. ■

When you are trying to solve certain problems, you may find that the contrapositive form of a conditional statement is easier to work with than the original statement. Replacing a statement by its contrapositive may give the extra push that helps you over the top in your search for a solution. This logical equivalence is also the basis for the contrapositive method of proof

The Converse and Inverse of a Conditional Statement

Definition 10: Converse and Inverse

Suppose a conditional statement of the form "If p then q" is given.

1. The **converse** is "If q then p."
2. The **inverse** is "If $\sim p$ then $\sim q$."

Symbolically,

$$\text{The converse of } p \to q \text{ is } q \to p,$$

and

$$\text{The inverse of } p \to q \text{ is } \sim p \to \sim q.$$

Example 1.21. Write the converse and inverse of each of the following statements:

a If John can swim across the lake, then John can swim to the island.

b If today is Sunday, then tomorrow is Monday.

Solution. a *Converse*: If Howard can swim to the island, then Howard can swim across the lake.
Inverse: If John cannot swim across the lake, then John cannot swim to the island.

b *Converse*: If tomorrow is Monday, then today is Sunday.
Inverse: If today is not Sunday, then tomorrow is not Monday. ■

1. A conditional statement and its converse are not logically equivalent.
2. A conditional statement and its inverse are not logically equivalent.
3. The converse and the inverse of a conditional statement are logically equivalent to each other.

Biconditional

Definition 11: Biconditional

Given statement variables p and q, the biconditional of p and q is "p if, and only if, q" and is denoted $p \leftrightarrow q$. It is true if both p and q have the same truth values and is false if p and q have opposite truth values. The words if and only if are sometimes abbreviated ***iff***.

The biconditional has the following truth table:

Table 14: Truth Table for $p \leftrightarrow q$

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Order of Operations for Logical Operators

1. $\sim$ Evaluate negations first.
2. $\wedge, \vee$ Evaluate $\wedge$ and $\vee$ second. When both are present.
3. $\rightarrow, \leftrightarrow$ Evaluate $\rightarrow$ and $\leftrightarrow$ third. When both are present.

According to the separate definitions of *if* and only *if*, saying "p if, and only if, q" should mean the same as saying both "p if q" and "p only if q." The following annotated truth table shows that this is the case:

Example 1.22. Rewrite the following statement as a conjunction of two if-then statements:

> This computer program is correct if, and only if, it produces correct answers for all possible sets of input data.

Solution. If this program is correct, then it produces the correct answers for all possible sets of input data; and if this program produces the correct answers for all possible sets of input data, then it is correct. ■

1.7 Arguments

Definition 12: Arguments

An *argument* is an assertion that a given set of propositions $P_1, P_2, ..., P_n$, called *premises*, yields (has a consequence) another proposition Q, called the *conclusion*. Such an argument is denoted by

$$P_1, P_2, ..., P_n \vdash Q$$

An argument $P_1, P_2, ..., P_n \vdash Q$ is said to be valid if Q is true whenever all the premises $P_1, P_2, ..., P_n$ are true.
An argument which is not valid is called *fallacy*.

Example 1.23. Determine the validity of the following argument:

If Socrates is a man, then Socrates is mortal.
Socrates is a man.
∴ Socrates is mortal.

Solution. The argument has the abstract form

if p the q
p
$\therefore q$

Table 15: Truth Table for the argument

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

■

Example 1.24. Determine the validity of the following argument:

$p \rightarrow q \vee \sim r$
$q \rightarrow p \wedge r$
$\therefore p \rightarrow r$

Solution. The truth table shows that even though there are several situations in which the premises and the conclusion are all true (rows 1, 7, and 8), there is one situation (row 4) where the premises are true and the conclusion is false. ■

p	q	r	$\sim r$	$q \vee \sim r$	$p \wedge r$	$p \rightarrow q \vee \sim r$	$q \rightarrow p \wedge r$	$p \rightarrow r$
T	T	T	F	T	T	T	T	T
T	T	F	T	T	F	T	F	
T	F	T	F	F	T	F	T	
T	F	F	T	T	F	T	T	F
F	T	T	F	T	F	T	F	
F	T	F	T	T	F	T	F	
F	F	T	F	F	F	T	T	T
F	F	F	T	T	F	T	T	T

not valid

Example 1.25. Determine the validity of the following argument:

If Zeus is human, then Zeus is mortal.
Zeus is not mortal.
∴ Zeus is not human.

Solution. Exercise ■

Example 1.26. Generalization: The following argument forms are valid:
(a)

p
$\therefore p \vee q$

(b)

q
$\therefore p \vee q$

Example 1.27. Specialization: The following argument forms are valid:
(a)

$p \wedge q$
$\therefore p$

(b)

$p \wedge q$
$\therefore q$

Example 1.28. Elimination: The following argument forms are valid:
(a)

$p \vee q$
$\sim q$
$\therefore p$

(b)

$p \vee q$
$\sim p$
$\therefore q$

Example 1.29. Transitivity: The following argument forms are valid:

$p \to q$
$q \to r$
$\therefore p \to r$

If n is divisible by 18, then n is divisible by 9.
If n is divisible by 9, then the sum of the digits of n is divisible by 9.
$\therefore$ If n is divisible by 18, then the sum of the digits of n is divisible by 9.

Example 1.30. Proof by Division into Cases: The following argument forms are valid:

$p \vee q$
$p \to r$
$q \to r$
$\therefore r$

x is positive or x is negative.
If x is positive, then $x^2 > 0$.
If x is negative, then $x^2 > 0$.
$\therefore x^2 > 0$.

Example 1.31. Show that the following argument is invalid:

$p \to q$
q
$\therefore p$

If Zeke is a cheater, then Zeke sits in the back row.
Zeke sits in the back row.
$\therefore$ Zeke is a cheater.

Theorem 1.2. *The argument $P_1, P_2, ..., P_n \vdash Q$ is valid if and only if the proposition $(P_1 \wedge P_2 ... \wedge P_n) \to Q$ is a tautology.*

Example 1.32. A fundamental principle of logical reasoning states:

"If p implies q and q implies r, then p implies r"

Show that the above argument is valid

Solution. Construct the truth table for "If p implies q and q implies r, then p implies r" ■

p	q	r	$p \to q$	$q \to r$	$p \to r$	$(p \to q) \wedge (q \to r)$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	T	F	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	T	F	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

Example 1.33. Show that the following argument is a fallacy: $p \to q, \sim p \vdash \sim q$.

Solution. Construct the truth table for $[(p \to q) \wedge \sim p] \to \sim q$ as in Fig. below Since the proposition $[(p \to q) \wedge \sim p] \to \sim q$ is not a tautology, the argument is a fallacy. Equivalently, the argument is a fallacy since in the third line of the truth table $p \to q$ and $\sim p$ are true but $\sim q$ is false. ■

p	q	$p \to q$	$\sim p$	$(p \to q) \wedge \sim p$	$\sim q$	$[(p \to q) \wedge \sim p] \to \sim q$
T	T	T	F	F	F	T
T	F	F	F	F	T	T
F	T	T	T	T	F	F
F	F	T	T	T	T	T

Example 1.34. Determine the validity of the following argument:

If 7 is less than 4, then 7 is not a prime number.
7 is not less than 4.

7 is a prime number.

Solution. First translate the argument into symbolic form. Let p be "7 is less than 4" and q be "7 is a prime number." Then the argument is of the form

$$p \rightarrow \sim q, \sim p \vdash q$$

Now, we construct a truth table. The above argument is shown to be a fallacy since, in the fourth line of the truth table, the premises $p \rightarrow \sim q$ and $\sim p$ are true, but the conclusion q is false.

Remark: The fact that the conclusion of the argument happens to be a true statement is irrelevant to the fact that the argument presented is a fallacy. ∎

1.8 Propositional Functions, Quantifiers

Definition 13: Propositional Functions

Let A be a given set. A ***propositional function*** (or an *open sentence* or *condition*) defined on A is an expression

$$p(x)$$

which has the property that $p(a)$ is true or false for each $a \in A$. That is, $p(x)$ becomes a statement (with a truth value) whenever any element $a \in A$ is substituted for the variable x. The set A is called the domain of $p(x)$, and the set T_p of all elements of A for which $p(a)$ is true is called the truth set of $p(x)$. In other words,

$$T_p = \{x \mid x \in A, p(x) \text{ is true } \} \text{ or } T_p = \{x \mid p(x)\}$$

Frequently, when A is some set of numbers, the condition $p(x)$ has the form of an equation or inequality involving the variable x.

Example 1.35. Find the truth set for each propositional function $p(x)$ defined on the set $\mathbb{N}$ of positive integers.

(a) Let $p(x)$ be "$x + 2 > 7$."

(b) Let $p(x)$ be "$x + 5 < 3$."

(c) Let $p(x)$ be "$x + 5 > 1$."

Remark: The above example shows that if $p(x)$ is a propositional function defined on a set A then $p(x)$ could be true for all $x \in A$, for some$x \in A$, or for no $x \in A$. The next two subsections discuss quantifiers related to such propositional functions.

Universal Quantifier

Definition 14: Universal Quantifier

Let $p(x)$ be a propositional function defined on a set A. Consider the expression

$$(\forall x \in A)\ p(x) \text{ or } \forall x\ p(x)$$

which reads "For every x in A, $p(x)$ is a true statement" or, simply, "For all x, $p(x)$." The symbol

$$\forall$$

which reads "for all" or "for every" is called the ***universal quantifier***.

The statement above is equivalent to the statement

$$T_p = \{x \mid x \in A, p(x)\} = A$$

that is, that the truth set of $p(x)$ is the entire set A. The expression $p(x)$ by itself is an open sentence or condition and therefore has no truth value. Specifically:

$$Q1 : If \{x \mid x \in A, p(x)\} = A \text{ then } \forall x\ p(x) \text{ is true ; otherwise , } \forall x\ p(x) \text{ is false .}$$

Example 1.36. Consider the following propositional functions

(a) The proposition $(\forall n \in \mathbb{N})\ (n+4>3)$ is true since $\{n \mid n+4>3\} = \{1,2,3,...\} = \mathbb{N}$.

(b) The proposition $(\forall n \in \mathbb{N})\ (n+2>8)$ is false since $\{n \mid n+2>8\} = \{7,8,9,...\} = \mathbb{N}$.

Existential Quantifier

Definition 15: Existential Quantifier

Let $p(x)$ be a propositional function defined on a set A. Consider the expression

$$(\exists x \in A)\ p(x) \text{ or } \exists x,\ p(x)$$

which reads "There exists an x in A such that $p(x)$ is a true statement" or, simply, "For some x, $p(x)$." The symbol

$$\exists$$

which reads "there exists" or "for some" or "for at least one" is called the ***existential quantifier***.

The statement above is equivalent to the statement

$$T_p = \{x \mid x \in A,\ p(x)\} \neq \emptyset$$

i.e., that the truth set of $p(x)$ is not empty. Accordingly, $\exists x\ p(x)$, that is, $p(x)$ preceded by the quantifier $\exists$, does have a truth value. Specifically:

$$Q2 : If \{x \mid p(x)\} \neq \emptyset \text{ then } \exists x\ p(x) \text{ is true ; otherwise , } \exists x\ p(x) \text{ is false .}$$

Example 1.37. Consider the following propositional functions

(a) The proposition $(\exists n \in \mathbb{N})\ (n+4<7)$ is true since $\{n \mid n+4<7\} = \{1,2\} \neq \emptyset$.

(b) The proposition $(\exists n \in \mathbb{N})\ (n+6<4)$ is false since $\{n \mid n+6<4\} = \emptyset$.

Example 1.38. Consider the statement

$$\exists m \in \mathbb{Z}^+ \text{ such that } m^2 = m.$$

Solution. "There is at least one positive integer m such that $m^2 = m$." Observe that $1^2 = 1$. Thus "$m^2 = m$" is true for a positive integer m, and so "$\exists m \in \mathbb{Z}^+$ such that $m^2 = m$" is true. ■

Example 1.39. Let $E = \{5, 6, 7, 8\}$ and consider the statement

$$\exists m \in E \text{ such that } m^2 = m.$$

Show that this statement is false.

Solution. Note that $m^2 = m$ is not true for any integers m from 5 through 8:

$$5^2 = 25 \neq 5,\ 6^2 = 36 \neq 6,\ 7^2 = 49 \neq 7,\ 8^2 = 64 \neq 8.$$

Thus "$\exists m \in E$ such that $m^2 = m$" is false. ■

Negation of Quantified Statements

Definition 16: Negation of a Universal Statement

The negation of a statement of the form

$$\forall x \in A, P(x)$$

is logically equivalent to a statement of the form

$$\exists x \in A \text{ such that } \sim P(x).$$

Symbolically,

$$\sim (\forall x \in A, P(x)) \equiv \exists x \in A \text{ such that } \sim P(x)$$

Thus

The negation of a universal statement ("all are") is logically equivalent to an existential statement ("some are not" or "there is at least one that is not").

Definition 17: Negation of an Existential Statement

The negation of a statement of the form

$$\exists x \in A, P(x)$$

is logically equivalent to a statement of the form

$$\forall x \in A \text{ such that } \sim P(x).$$

Symbolically,

$$\sim (\exists x \in A, P(x)) \equiv \forall x \in A \text{ such that } \sim P(x)$$

Thus

The negation of an existential statement ("some are") is logically equivalent to a universal statement ("none are" or "all are not").").

Example 1.40. Write formal negations for the following statements:

(a) $\forall$ primes p, p is odd.

(b) $\exists$ a triangle T such that the sum of the angles of T equals 200^o. ■

Solution. Exercises

Example 1.41. What are the negations of the statements $\forall x(x^2 > x)$ and $\exists x(x^2 = 2)$?

Solution. The negation of $\forall x(x^2 > x)$ is the statement $\sim (\forall x(x^2 > x))$, which is equivalent to $\exists x \sim (x^2 > x)$. This can be rewritten as $\exists x(x^2 \leq x)$. The negation of $\exists x(x^2 = 2)$ is the statement $\sim (\exists x(x^2 = 2))$, which is equivalent to $\forall x \sim (x^2 = 2)$. This can be rewritten as $\forall x(x^2 \neq 2)$. The truth values of these statements depend on the domain. ■

Counterexample

Example 1.42. Consider the statement $\forall x \in \mathbb{R}$, $|x| \neq 0$. The statement is false since 0 is a counterexample, that is, $|0| \neq 0$ is not true.

Example 1.43. Consider the statement $\forall x \in \mathbb{R}$, $x^2 \geq x$. The statement is not true since, for example, $\frac{1}{2}$ is a counterexample. Specifically, $(\frac{1}{2})^2 \geq \frac{1}{2}$ is not true, that is, $(\frac{1}{2})^2 < \frac{1}{2}$.

Propositional Functions with more than One Variable

A propositional function preceded by a quantifier for each variable, for example,

$$\forall x \exists y,\ p(x, y) \text{ or } \exists x \forall y \exists z,\ p(x, y, z)$$

denotes a statement and has a truth value.

Example 1.44. Let $B = \{1, 2, 3, ..., 9\}$ and let $p(x, y)$ denote "$x + y = 10$." Then $p(x, y)$ is a propositional function on $A = B^2 = B \times B$.

(a) The following is a statement since there is a quantifier for each variable:

$$\forall x \exists y,\ p(x, y), \text{ that is, "For every } x\text{, there exists a } y \text{ such that } x + y = 10\text{"}$$

This statement is true. For example, if $x = 1$, let $y = 9$; if $x = 2$, let $y = 8$, and so on.

(b) The following is also a statement:

$$\exists y \forall x,\ p(x, y), \text{ that is, "There exists a } y \text{ such that, for every } x\text{, we have } x + y = 10\text{"}$$

No such y exists; hence this statement is false.

Negating Quantified Statements with more than One Variable

Quantified statements with more than one variable may be negated by successively applying the negation of quantified statements definitions above. Thus each $\forall$ is changed to $\exists$ and each $\exists$ is changed to $\forall$ as the negation symbol $\sim$ passes through the statement from left to right. For example,

$$\sim [\forall x \exists y \exists z,\ p(x, y, z)] \equiv \exists x \forall y \forall z,\ \sim p(x, y, z)$$

Example 1.45. Express the negation of the statement $\forall x \exists y(xy = 1)$ so that no negation precedes a quantifier.

Solution. We find that $\sim \forall x \exists y(xy = 1)$ is equivalent to $\exists x \sim \exists y(xy = 1)$, which is equivalent to $\exists x \forall y \sim (xy = 1)$. Because $\sim (xy = 1)$ can be expressed more simply as $xy \neq 1$, we conclude that our negated statement can be expressed as $\exists x \forall y(xy \neq 1)$. ■

2. Elementary Number theory and Methods of Proof

Direct Proof

A direct proof of a conditional statement $p \to q$ is constructed when the first step is the assumption that p is true; subsequent steps are constructed using rules of inference, with the final step showing that q must also be true.

Definition 18: Even and Odd Integers

An integer n is ***even*** if, and only if, n equals twice some integer. An integer n is ***odd*** if, and only if, n equals twice some integer plus 1.
Symbolically, for any integer, n

$$n \text{ is even} \leftrightarrow n = 2k \text{ for some integer } k$$

$$n \text{ is odd} \leftrightarrow n = 2k + 1 \text{ for some integer } k$$

Example 2.1. Use the definitions of even and odd to justify your answers to the following questions.

(a) Is 0 even?

(b) Is -301 odd?

(c) If a and b are integers, is $6a^2b$ even?

(d) If a and b are integers, is $10a + 8b + 1$ odd?

(e) Is every integer either even or odd?

Theorem 2.1. *The sum of any two even integers is even.*

Proof. Suppose m and n are any [particular but arbitrarily chosen] even integers. [We must show that $m + n$ is even.] By definition of even, $m + 2r$ and $n = 2s$ for some integers r and s. Then

$$\begin{aligned} m + n &= 2r + 2s \\ &= 2(r + s) \end{aligned}$$

Let $t = r + s$. Note that t is an integer because it is a sum of integers. Hence

$$m + n = 2t \text{ where } t \text{ is an integer.}$$

□

Example 2.2. Show that the difference of any odd integer and any even integer is odd.

Solution. Suppose a is any odd integer and b is any even integer.[*We must show that $a - b$ is odd.*] By definition of odd, $a = 2r + 1$ for some integer r, and $b = 2s$ for some integer s. Then

$$\begin{aligned} a - b &= (2r + 1) - 2s \\ &= 2r - 2s + 1 \\ &= 2(r - s) + 1 \\ &= 2t + 1 \text{ for some integer } t = r - s \end{aligned}$$

Hence $a - b$ is odd ■

Example 2.3. For every odd integer n, n^2 is odd

Solution. Suppose n is any odd integer. By definition of odd, $n = 2k + 1$ for some integer k. Then

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(k^2 + 2k) + 1 \\ &= 2r + 1 \text{ for some integer } r = k^2 + 2k \end{aligned}$$

Therefore n^2 is odd. ∎

Example 2.4. Show that for all integers r and s, if r is even and s is odd then $3r + 2s$ is even

Solution. Exercise ∎

Example 2.5. Deriving Additional Results about Even and Odd Integers

1. The sum, product, and difference of any two even integers are even.
2. The sum and difference of any two odd integers are even.
3. The product of any two odd integers is odd.
4. The product of any even integer and any odd integer is even.
5. The sum of any odd integer and any even integer is odd.
6. The difference of any odd integer minus any even integer is odd.
7. The difference of any even integer minus any odd integer is odd.

Remark: Direct proofs lead from the premises of a theorem to the conclusion. They begin with the premises, continue with a sequence of deductions, and end with the conclusion.

Proof by Contraposition

In some cases we will see that attempts at direct proofs often reach dead ends. We need other methods of proving theorems of the form $\forall x(P(x) \rightarrow Q(x))$. Proofs of theorems of this type that are not direct proofs, that is, that do not start with the premises and end with the conclusion, are called indirect proofs.

Proofs by contraposition make use of the fact that the conditional statement $p \rightarrow q$ is equivalent to its contrapositive, $\sim q \rightarrow \sim p$. This means that the conditional statement $p \rightarrow q$ can be proved by showing that its contrapositive, $\sim q \rightarrow \sim p$, is true. In a proof by contraposition of $p \rightarrow q$, we take $\sim q$ as a premise, and using axioms, definitions, and previously proven theorems, together with rules of inference, we show that $\sim p$ must follow.

Example 2.6. Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

Solution. Let the conditional statement "If $3n + 2$ is odd, then n is odd" be false.
i.e. assume that n is even. Then, by the definition of an even integer, $n = 2k$ for some integer k.

$$\begin{aligned} 3n + 2 &= 3(2k) + 2 \\ &= 6k + 2 \\ &= 2(3k + 1) \end{aligned}$$

This tells us that 3n + 2 is even (because it is a multiple of 2), and therefore not odd. This is the negation of the premise of the example. Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, the original conditional statement is true. ∎

Example 2.7. Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Solution. Because there is no obvious way of showing that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ directly from the equation $n = ab$, where a and b are positive integers, we attempt a proof by contraposition.
Let the conditional statement "If $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$" be false.

$$\text{i.e. } (a \leq \sqrt{n}) \vee (b \leq \sqrt{n}) \text{ is false.}$$

$$\begin{aligned} \sim ((a \leq \sqrt{n}) \vee (b \leq \sqrt{n})) &\equiv \sim (a \leq \sqrt{n}) \wedge \sim (b \leq \sqrt{n}) \\ &\equiv (a > \sqrt{n}) \wedge (b > \sqrt{n}) \end{aligned}$$

This implies that $a > \sqrt{n}$ and $b > \sqrt{n}$. Multiply these inequalities together we obtained

$$\begin{aligned} ab &> \sqrt{n}\sqrt{n} = n \\ &> n \end{aligned}$$

This shows that $ab \neq n$, which contradicts the statement $n = ab$.
Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, the original conditional statement is true. ■

Example 2.8. Prove that if n is an integer and n^2 is odd, then n is odd.

Solution. Exercise ■

Example 2.9. Show that the proposition $P(0)$ is true, where $P(n)$ is "If $n > 1$, then $n^2 > n$" and the domain consists of all integers.

Solution. Note that $P(0)$ is "If $0 > 1$, then $0^2 > 0$." We can show $P(0)$ using a vacuous proof. Indeed, the hypothesis $0 > 1$ is false. This tells us that $P(0)$ is automatically true. ■

Example 2.10. Prove that if n is an integer with $10 \leq n \leq 15$ which is a perfect square, then n is also a perfect cube.

Solution. Note that there are no perfect squares n with $10 \leq n \leq 15$, because $3^2 = 9$ and $4^2 = 16$. Hence, the statement that n is an integer with $10 \leq n \leq 15$ which is a perfect square is false for all integers n. Consequently, the statement to be proved is true for all integers n. ■

We can also quickly prove a conditional statement $p \to q$ if we know that the conclusion q is true. By showing that q is true, it follows that $p \to q$ must also be true. A proof of $p \to q$ that uses the fact that q is true is called a **trivial proof**.

Example 2.11. Let $P(n)$ be "If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$," where the domain consists of all nonnegative integers. Show that $P(0)$ is true.

Solution. The proposition $P(0)$ is "If $a \geq b$, then $a^0 \geq b^0$." Because $a^0 = b^0 = 1$, the conclusion of the conditional statement "If $a \geq b$, then$a^0 \geq b^0$" is true. Hence, this conditional statement, which is $P(0)$, is true. This is an example of a trivial proof. Note that the hypothesis, which is the statement "$a \geq b$," was not needed in this proof. ■

Definition 19

The real number r is **rational** if there exist integers p and q with $q \neq 0$ such that $r = \frac{p}{q}$. A real number that is not rational is called **irrational.**

Example 2.12. Determining whether Numbers Are Rational or Irrational

(a) Is $\frac{10}{3}$ a rational number?

(b) Is $-\frac{5}{39}$ a rational number?

(c) Is 0.281 a rational number?

(d) Is 7 a rational number?

(e) Is 0 a rational number?

(f) Is $\frac{2}{0}$ a rational number?

(g) Is $\frac{2}{0}$ a irrational number?

(h) Is 0.12121212 A a rational number (where the digits 12 are assumed to repeat forever)?

(i) If m and n are integers and neither m nor n is zero, is $\frac{(m+n)}{mn}$ a rational number?

Solution. Exercise ∎

Theorem 2.2. *Every integer is a rational number.*

Example 2.13. Any Sum of Rational Numbers Is Rational

Solution. Suppose r and s are any rational numbers.
By definition $r = \frac{a}{b}$ and $s = \frac{c}{d}$ for some integers a, b, c, and d where $b \neq 0$ and $d \neq 0$.
It follows by substitution that

$$\begin{aligned} r + s &= \frac{a}{b} + \frac{c}{d} \\ &= \frac{ad}{bd} + \frac{bc}{bd} \\ &= \frac{ad+bc}{bd} \\ &= \frac{p}{q} \text{ where } p = ad + bc \text{ and } q = bd \text{ are integers and } q \neq 0. \end{aligned}$$

This means that $r + s$ is rational ∎

Example 2.14. Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

Solution. Suppose $\sqrt{2}$ is rational. Then

$$\begin{aligned} \sqrt{2} &= \frac{p}{q} \text{ for some integer } p \text{ and } q \neq 0. \\ 2 &= \frac{p^2}{q^2} \\ 2q^2 &= p^2 \end{aligned}$$

p^2 must be even. Since p^2 is even, then p is also even. Since p is even, it can be written as $2m$ where m is an integer.
Substituting $p = 2m$ in the above equation:

$$2q^2 = (2m)^2$$
$$2q^2 = 4m^2$$
$$q^2 = 2m^2$$

q^2 is an even number. So q is an even number. Since q is even, it can be written as $2n$ where n is an integer.
Now we have $p = 2m$ and $q = 2n$ and remember we assumed that $\sqrt{2} = \frac{p}{q}$:

$$\sqrt{2} = \frac{p}{q}$$
$$\sqrt{2} = \frac{2m}{2n}$$
$$\sqrt{2} = \frac{m}{n}$$

We now have a fraction m/n that is simpler than p/q.
Hence $\sqrt{2}$ cannot be rational and so must be irrational. ■

Exhaustive Proof

Some theorems can be proved by examining a relatively small number of examples. Such proofs are called exhaustive proofs, or proofs by exhaustion because these proofs proceed by exhausting all possibilities. An exhaustive proof is a special type of proof by cases where each case involves checking a single example.

Example 2.15. Prove that $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

Solution. We use a proof by exhaustion.We only need verify the inequality $(n+1)^3 \geq 3^n$ when $n = 1, 2, 3,$ and 4. ■

Example 2.16. Prove that the only consecutive positive integers not exceeding 100 that are perfect powers are 8 and 9. (An integer n is a **perfect power** if it equals m^a, where m is an integer and a is an integer greater than 1.)

Solution. We use a proof by exhaustion. In particular, we can prove this fact by examining positive integers n not exceeding 100, first checking whether n is a perfect power, and if it is, checking whether $n+1$ is also a perfect power. A quicker way to do this is simply to look at all perfect powers not exceeding 100 and checking whether the next largest integer is also a perfect power. The squares of positive integers not exceeding 100 are 1, 4, 9, 16, 25, 36, 49, 64, 81, and 100. The cubes of positive integers not exceeding 100 are 1, 8, 27, and 64. The fourth powers of positive integers not exceeding 100 are 1, 16, and 81. The fifth powers of positive integers not exceeding 100 are 1 and 32. The sixth powers of positive integers not exceeding 100 are 1 and 64. There are no powers of positive integers higher than the sixth power not exceeding 100, other than 1. Looking at this list of perfect powers not exceeding 100, we see that $n = 8$ is the only perfect power n for which $n+1$ is also a perfect power. That is, $2^3 = 8$ and $3^2 = 9$ are the only two consecutive perfect powers not exceeding 100. ■

Proof by Cases

A proof by cases must cover all possible cases that arise in a theorem. We illustrate proof by cases with a couple of examples. In each example, you should check that all possible cases are covered.

Example 2.17. Prove that if n is an integer, then $n^2 \geq n$.

Solution. We can prove that $n^2 \geq n$ for every integer by considering three cases, when $n = 0$, when $n \geq 1$, and when $n \leq -1$. We split the proof into three cases because it is straightforward to prove the result by considering zero, positive integers, and negative integers separately.
Case (i): When $n = 0$, because $0^2 = 0$, we see that $0^2 \geq 0$. It follows that $n^2 \geq n$ is true in this case.
Case (ii): When $n \geq 1$, when we multiply both sides of the inequality $n \geq 1$ by the positive integer n, we obtain $n.n \geq n.1$. This implies that $n^2 \geq n$ for $n \geq 1$.
Case (iii): In this case $n \leq -1$. However, $n^2 \geq 0$. It follows that $n^2 \geq n$. ∎

Because the inequality $n^2 \geq n$ holds in all three cases, we can conclude that if n is an integer, then $n^2 \geq n$. ∎

Example 2.18. Use a proof by cases to show that $|xy| = |x||y|$, where x and y are real numbers. (**Recall** that $|a|$, the absolute value of a, equals a when $a \geq 0$ and equals $-a$ when $a \leq 0$.) ∎

Solution. Exercise

Example 2.19. Show that there are no solutions in integers x and y of $x^2 + 3y^2 = 8$. ∎

Solution. Exercise

Uniqueness Proofs

Some theorems assert the existence of a unique element with a particular property. In other words, these theorems assert that there is exactly one element with this property. To prove a statement of this type we need to show that an element with this property exists and that no other element has this property. The two parts of a **uniqueness proof** are:

Existence: We show that an element x with the desired property exists.

Uniqueness: We show that if x and y both have the desired property, then $x = y$.

Example 2.20. Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Solution. First, note that the real number $r = -b/a$ is a solution of $ar + b = 0$ because

$$a(-b/a) + b = -b + b = 0$$

Consequently, a real number r exists for which $ar + b = 0$. This is the existence part of the proof.

Second, suppose that s is a real number such that $as + b = 0$. Then $ar + b = as + b$, where $r = -b/a$. Subtracting b from both sides, we find that $ar = as$. Dividing both sides of this last equation by a, which is nonzero, we see that $r = s$. This establishes the uniqueness part of the proof. ∎

2.1 Prime and Composite Numbers

Definition 20: Prime and Composite Numbers

An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n. An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$. In symbols: For each integer n with $n > 1$,

$$n \text{ is prime } \leftrightarrow \forall \text{ positive integers } r \text{ and } s, \text{ if } n = rs \text{ then either } r = 1 \text{ and } s = n \text{ or } r = n \text{ and } s = 1.$$

$$n \text{ is composite } \leftrightarrow \exists \text{ positive integers } r \text{ and } s, \text{ such that } n = rs \text{ and } 1 < r < n \text{ and } 1 < s < n.$$