Undergraduate Notes in Mathematics

Arkansas Tech University
Department of Mathematics

Introductory Notes in Discrete Mathematics

Marcel B. Finan

Last Updated

April 6, 2016

Preface

This book is designed for a one semester course in discrete mathematics for sophomore or junior level students. The text covers the mathematical concepts that students will encounter in many disciplines such as computer science, engineering, Business, and the sciences.
Besides reading the book, students are strongly encouraged to do all the exercises. Mathematics is a discipline in which working the problems is essential to the understanding of the material contained in this book.
Students are encouraged first to do the problems without referring to the solutions. Answers and Solutions to problems found at the end of this book can only be used when you are stuck. Exert a reasonable amount of efforts towards solving a problem before you look up the answer, and rework any problem you miss.
Students are strongly encouraged to keep up with the exercises and the sequel of concepts as they are going along, for mathematics builds on itself.
A solution guide to the text is available through email: mfinan@atu.edu

Marcel B. Finan
Russellville, Arkansas
August 2014

Contents

Set Numbers Notations

In this chapter, we introduce the set of numbers that we will use in this book.

- The set of all positive integers

$$\mathbb{N} = \{1, 2, 3, \cdots\}.$$

- The set of whole numbers

$$\mathbb{W} = \{0, 1, 2, \cdots\}.$$

- The set of all integers

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}.$$

- The set of all rational numbers

$$\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z} \text{ with } b \neq 0\}.$$

- The set of irrational numbers $\mathbb{I}$.
- The set $\mathbb{R}$ of all real numbers.

Also, when a number n belongs to a certain set, we will use the notation $\in$. For example, $-2 \in \mathbb{Z}$ and $-2 \notin \mathbb{N}$.

Fundamentals of Mathematical Logic

Logic is commonly known as the science of reasoning. This introductory chapter covers modern mathematical logic such as propositions and quantifiers.

1 Propositions and Related Concepts

A **proposition** is any meaningful statement that is either true or false, but not both. We will use lowercase letters, such as $p, q, r, \cdots$, to represent propositions. We will also use the notation

$$p : 1 + 1 = 3$$

to define p to be the proposition $1+1 = 3$. The **truth value** of a proposition is true, denoted by T, if it is a true statement and false, denoted by F, if it is a false statement. Statements that are not propositions include questions and commands.

Example 1.1
Which of the following are propositions? Give the truth value of the propositions.
(a) $2 + 3 = 7$.
(b) Julius Caesar was president of the United States.
(c) What time is it?
(d) Be quiet !

Solution.
(a) A proposition with truth value (F).
(b) A proposition with truth value (F).
(c) Not a proposition since no truth value can be assigned to this statement.
(d) Not a proposition ■

Example 1.2
Which of the following are propositions? Give the truth value of the propositions.
(a) The difference of two primes.
(b) $2 + 2 = 4$.
(c) Washington D.C. is the capital of New York.
(d) How are you?

Solution.
(a) Not a proposition.
(b) A proposition with truth value (T).
(c) A proposition with truth value (F).

(d) Not a proposition ■

New propositions called **compound propositions** or **propositional functions** can be obtained from old ones by using **symbolic connectives** which we discuss next. The propositions that form a propositional function are called the **propositional variables**.
Let p and q be propositions. The **conjunction** of p and q, denoted by $p \wedge q$ (read "p wedge q"), is the proposition: p *and* q. This proposition is defined to be true only when both p and q are true and it is false otherwise.
The **disjunction** of p and q, denoted by $p \vee q$ (read "p vee q"), is the proposition: p *or* q. The "or" is used in an inclusive way. This proposition is false only when both p and q are false, otherwise it is true.

Example 1.3
Let

$$p: \quad 5 < 9$$
$$q: \quad 9 < 7.$$

Construct the propositions $p \wedge q$ and $p \vee q$.

Solution.
The conjunction of the propositions p and q is the proposition

$$p \wedge q : 5 < 9 \text{ and } 9 < 7.$$

This proposition is false since the proposition $9 < 7$ has a truth value F.
The disjunction of the propositions p and q is the proposition

$$p \vee q : 5 < 9 \text{ or } 9 < 7$$

which is a true proposition ■

Example 1.4
Consider the following propositions

$$p: \quad \text{It is Friday}$$
$$q: \quad \text{It is raining.}$$

Construct the propositions $p \wedge q$ and $p \vee q$.

Solution.
The conjunction of the propositions p and q is the proposition

$$p \wedge q : \text{It is Friday and it is raining.}$$

The disjunction of the propositions p and q is the proposition

$$p \vee q : \text{It is Friday or It is raining} \blacksquare$$

A **truth table** displays the relationships between the truth values of propositions. Next, we display the truth tables of $p \wedge q$ and $p \vee q$.

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

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

Let p and q be two propositions. The **exclusive or** (or **exclusive disjunction**) of p and q, denoted $p \oplus q$, is the proposition that is true when exactly one of p and q is true and is false otherwise. The truth table of the exclusive "or" is displayed below

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Example 1.5
(a) Construct a truth table for $(p \oplus q) \oplus r$.
(b) Construct a truth table for $p \oplus p$.

Solution.
(a) The truth table is

p	q	r	$p \oplus q$	$(p \oplus q) \oplus r$
T	T	T	F	T
T	T	F	F	F
T	F	T	T	F
T	F	F	T	T
F	T	T	T	F
F	T	F	T	T
F	F	T	F	T
F	F	F	F	F

(b) The truth table is

p	$p \oplus p$
T	F
F	F

■

The final operation on a proposition p that we discuss is the **negation** of p. The negation of p, denoted $\sim p$, is the proposition not p. The truth table of $\sim p$ is displayed below

p	$\sim p$
T	F
F	T

Example 1.6
Consider the following propositions:
p: Today is Thursday.
q: $2 + 1 = 3$.
r: There is no pollution in New Jersey.
Construct the truth table of $[\sim (p \wedge q)] \vee r$.

Solution.

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

■

Example 1.7
Find the negation of the proposition $p : -5 < x \leq 0$.

Solution.
The negation of p is the proposition $\sim p : x > 0$ *or* $x \leq -5$ ■

A compound proposition is called a **tautology** if it is always true, regardless of the truth values of the propositional variables which comprise it.

Example 1.8
(a) Construct the truth table of the proposition $(p \wedge q) \vee (\sim p \vee \sim q)$. Determine if this proposition is a tautology.
(b) Show that $p \vee \sim p$ is a tautology.

Solution.
(a) The truth table is

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

Thus, the given proposition is a tautology.
(b) The truth table is

p	$\sim p$	$p \vee \sim p$
T	F	T
F	T	T

Again, this proposition is a tautology ■

Two propositions are **equivalent** if they have exactly the same truth values under all circumstances. We write $p \equiv q$.

Example 1.9
(a) Show that $\sim (p \vee q) \equiv \sim p \wedge \sim q$.
(b) Show that $\sim (p \wedge q) \equiv \sim p \vee \sim q$.
(c) Show that $\sim (\sim p) \equiv p$.
Parts (a) and (b) are known as DeMorgan's laws.

Solution.
(a) The truth table is

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

Note that the columns of $\sim (p \vee q)$ and $\sim p \wedge \sim q$ have the same truth values.
(b) The truth table is

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

Note that the columns of $\sim (p \wedge q)$ and $\sim p \vee \sim q$ have the same truth values.
(c) The truth table is

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

■

Example 1.10
(a) Show that $p \wedge q \equiv q \wedge p$ and $p \vee q \equiv q \vee p$.
(b) Show that $(p \vee q) \vee r \equiv p \vee (q \vee r)$ and $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$.
(c) Show that $(p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$ and $(p \vee q) \wedge r \equiv (p \wedge r) \vee (q \wedge r)$.

Solution.
(a) The truth table is

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

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

(b) The truth table is

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

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

(c) The truth table is

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

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

■

Example 1.11
Show that $\sim (p \wedge q) \not\equiv \sim p \wedge \sim q$

Solution.
We will use truth tables to prove the claim.

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

■

A compound proposition that has the value F for all possible values of the propositions in it is called a **contradiction**.

Example 1.12
Show that the proposition $p \wedge \sim p$ is a contradiction.

Solution.

p	$\sim p$	$p \wedge \sim p$
T	F	F
F	T	F

■

Review Problems

Problem 1.1
Indicate which of the following sentences are propositions.
(a) 1,024 is the smallest four-digit number that is a perfect square.
(b) She is a mathematics major.
(c) $128 = 2^6$.
(d) $x = 2^6$.

Problem 1.2
Consider the propositions:
p: Juan is a math major.
q: Juan is a computer science major.

Use symbolic connectives to represent the proposition "Juan is a math major but not a computer science major."

Problem 1.3
In the following sentence is the word "or" used in its inclusive or exclusive sense? "A team wins the playoffs if it wins two games in a row or a total of three games."

Problem 1.4
Write the truth table for the proposition: $(p \vee (\sim p \vee q)) \wedge \sim (q \wedge \sim r)$.

Problem 1.5
Let t be a tautology. Show that $p \vee t \equiv t$.

Problem 1.6
Let c be a contradiction. Show that $p \vee c \equiv p$.

Problem 1.7
Show that $(r \vee p) \wedge [(\sim r \vee (p \wedge q)) \wedge (r \vee q)] \equiv p \wedge q$.

Problem 1.8
Use De Morgan's laws to write the negation for the proposition: "This computer program has a logical error in the first ten lines or it is being run with an incomplete data set."

Problem 1.9
Use De Morgan's laws to write the negation for the proposition: "The dollar is at an all-time high and the stock market is at a record low."

Problem 1.10
Assume $x \in \mathbb{R}$. Use De Morgan's laws to write the negation for the proposition: $-5 < x \leq 0$.

Problem 1.11
Show that the proposition $s = (p \wedge q) \vee (\sim p \vee (p \wedge \sim q))$ is a tautology.

Problem 1.12
Show that the proposition $s = (p \wedge \sim q) \wedge (\sim p \vee q)$ is a contradiction.

Problem 1.13
(a) Find simpler proposition forms that are logically equivalent to $p \oplus p$ and $p \oplus (p \oplus p)$.
(b) Is $(p \oplus q) \oplus r \equiv p \oplus (q \oplus r)$? Justify your answer.
(c) Is $(p \oplus q) \wedge r \equiv (p \wedge r) \oplus (q \wedge r)$? Justify your answer.

Problem 1.14
Show the following:
(a) $p \wedge t \equiv p$, where t is a tautology.
(b) $p \wedge c \equiv c$, where c is a contradiction.
(c) $\sim t \equiv c$ and $\sim c \equiv t$, where t is a tautology and c is a contradcition.
(d) $p \vee p \equiv p$ and $p \wedge p \equiv p$.

Problem 1.15
Which of the following statements are propositions?
(a) The Earth is round.
(b) Do you know how to swim?
(c) Please leave the room.
(d) $x + 3 = 5$.
(e) Canada is in Asia.

Problem 1.16
Write the negation of the following propositions:
(a) $\sim p \wedge q$.
(b) John is not at work or Peter is at the gym.

Problem 1.17
Construct the truth table of the compound proposition $(p \wedge q) \vee (\sim p)$.

Problem 1.18
Show that $p \oplus q \equiv (p \vee q) \wedge \sim (p \wedge q)$.

Problem 1.19
Show that $p \vee \sim (p \wedge q)$ is a tautology.

Problem 1.20
Show that $\sim p \wedge (p \wedge q)$ is a contradiction.

2 Basics of Digital Logic Design

In this section we discuss the logic of digital circuits which are considered to be the basic components of most digital systems, such as electronic computers, electronic phones, traffic light controls, etc.
The purpose of digital systems is to manipulate discrete information which are represented by physical quantities such as voltages and current. The smallest representation unit is one **bit**, short for binary digit. Since electronic switches have two physical states, namely high voltage and low voltage we attribute the bit 1 to high voltage and the bit 0 for low voltage.
A **logic gate** is the smallest processing unit in a digital system. It takes one or few bits as input and generates one bit as an output.
A **circuit** is composed of a number of logic gates connected by wires. It takes a group of bits as input and generates one or more bits as output.
The six basic logic gates are the following:
(1) NOT gate (also called **inverter**): Takes an input of 0 to an output of 1 and an input of 1 to an output of 0. The corresponding logical symbol is $\sim P$.
(2) AND gate: Takes two bits, P and Q, and outputs 1 if P and Q are 1 and 0 otherwise. The logical symbol is $P \wedge Q$. In Boolean algebra notation, one uses $P \cdot Q$.
(3) OR gate: outputs 1 if either P or Q is 1 and 0 otherwise. The logical symbol is $P \vee Q$. The corresponding Boolean algebra notation is $P + Q$.
(4) NAND gate: outputs a 0 if both P and Q are 1 and 1 otherwise. The symbol is $\sim (P \wedge Q)$. Also, denoted by $P|Q$, where $|$ is called a **Scheffer stroke**.
(5) NOR gate: output a 0 if at least one of P or Q is 1 and 1 otherwise. The symbol is $\sim (P \vee Q)$ or $P \downarrow Q$, where $\downarrow$ is a **Pierce arrow**.
(6) XOR gate or the exclusive or: Outputs a 1 if exactly one of the inputs is 1 and 0 otherwise. The symbol is $P \oplus Q$.

Example 2.1
Construct the input/output tables of the gates discussed in this section.

Solution.
Table for NOT-gate:

P	$\sim P$
1	0
0	1

Table for AND-gate:

P	Q	$P \wedge Q$
1	1	1
1	0	0
0	1	0
0	0	0

Table for OR-gate:

P	Q	$P \vee Q$
1	1	1
1	0	1
0	1	1
0	0	0

Table for NAND-gate:

P	Q	$\sim (P \wedge Q)$
1	1	0
1	0	1
0	1	1
0	0	1

Table for NOR-gate:

P	Q	$\sim (P \vee Q)$
1	1	0
1	0	0
0	1	0
0	0	1

Table for XOR-gate:

P	Q	$P \oplus Q$
1	1	0
1	0	1
0	1	1
0	0	0

■

Graphical representations of the logic gates are shown in Figure 2.1.

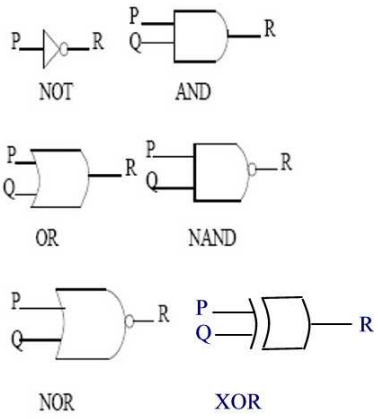
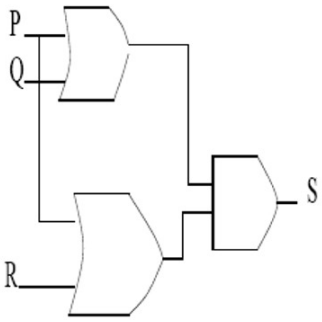


Figure 2.1

If you are given a set of input signals for a circuit, you can find its output by tracing through the circuit gate by gate.

Example 2.2
Give the output signal S for the following circuit, given that $P = 0, Q = 1$, and $R = 0$:



Solution.
The circuit is shown in Figure 2.2

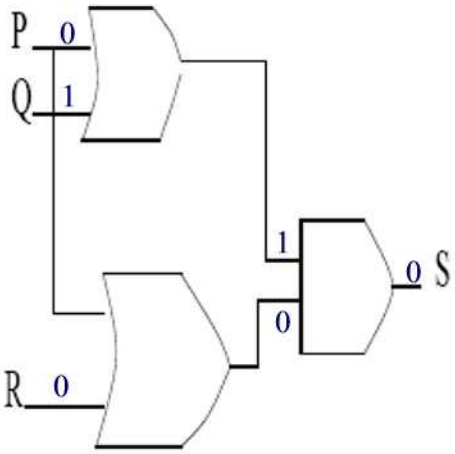


Figure 2.2

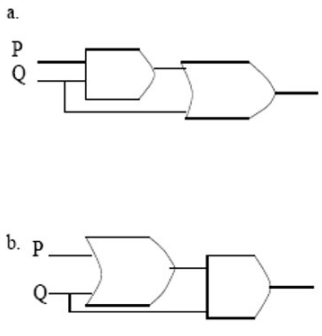
A variable with exactly two possible values is called a **Boolean variable**. A **Boolean expression** is an expression composed of Boolean variables and connectives (which are the gates in this section).

Example 2.3
Find the Boolean expression that corresponds to the circuit of Example 2.2.

Solution.
The Boolean expression is $(P \vee Q) \wedge (P \vee R)$ ■

Two digital logic circuits are **equivalent** if, and only if, their corresponding Boolean expressions are logically equivalent. Alternatively, the two Boolean expressions have the same truth table.

Example 2.4
Show that the following two circuits are equivalent:



Solution.
The Boolean expression corresponding to (a) is given by $(P \wedge Q) \vee Q$ and that corresponding to (b) is given by $(P \vee Q) \wedge Q$. These two expressions are logically equivalent:

$$\begin{aligned}(P \wedge Q) \vee Q &\equiv (P \vee Q) \wedge (Q \vee Q) \\ &\equiv (P \vee Q) \wedge Q \ \blacksquare\end{aligned}$$

In the next example, we describe the process of converting a number from base 10 to base 2 (binary) and vice versa.

Example 2.5
(a) Write the number $1,998_{10}$ in **base 2**.
(b) Write the number 11001_2 in **base 10**.

Solution.
(a) Let q denote the quotient of the division of a by b and r denote the remainder. We have

a	b	q	r
1,998	2	999	0
999	2	499	1
499	2	249	1
249	2	124	1
124	2	62	0
62	2	31	0
31	2	15	1
15	2	7	1
7	2	3	1
3	2	1	1
1	2	0	1.

Hence,

$$1,998_{10} = 11111001110_2.$$

(b) We have

$$11001_2 = 1 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 0 \times 2 + 1 = 25 \ \blacksquare$$

Integers Binary Representations

Several methods have been used for expressing negative integers in the computer. The most obvious way is to convert the number to binary and stick on another bit to indicate sign, 0 for positive and 1 for negative. Suppose that integers are stored using this signed-magnitude technique in 8 bits so that the leftmost bit holds the sign while the remaining bits represent the magnitude. Thus, $+41_{10} = 00101001$ and $-41_{10} = 10101001$.

The above procedure has a gap. How one would represent the bit 0? Well, there are two ways for storing 0. One way is 00000000 which represents $+0$ and a second way 10000000 represents -0. A method for representing numbers that avoid this problem is called the **two's complement**. Considering -41_{10} again, first, convert the absolute value to binary obtaining $41_{10} = 00101001$. Then take the complement of each bit obtaining 11010110. This is called the **one's complement** of 41. To complete the procedure, increment by 1 the one's complement to obtain $-41_{10} = 11010111$.

Conversion of $+41_{10}$ to two's complement consists merely of expressing the number in binary, i.e., $+41_{10} = 00101001$.

Example 2.6

(a) Represent the integer -6_{10} using one's complement.
(b) Represent the integer -6_{10} using two's complement.

Solution.

(a) We have $6_{10} = 0110_2$. The one's complement is $-6_{10} = 1001$.
(b) The two's complement is $-6_{10} = 1001 + 1 = 1010$ ■

Now, an algorithm to find the decimal representation of a negative integer with a given 8-bit two's complement is the following:

1. Find the two's complement of the given two's complement,
2. write the decimal equivalent of the result.

Example 2.7

(a) What is the decimal representation for the integer with 8-bit two's complement 10101001?
(b) What is the decimal representation for the integer with 8-bit two's complement 00101111?

Solution.

(a) The two's complement of 10101001 is $01010111 = 87_{10}$. Thus, the number

is -87_{10}.
(b) Since the integer is positive, $00101111 = 101111_2 = 1 \cdot 2^5 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 1 = 47_{10}$ ■

Review Problems

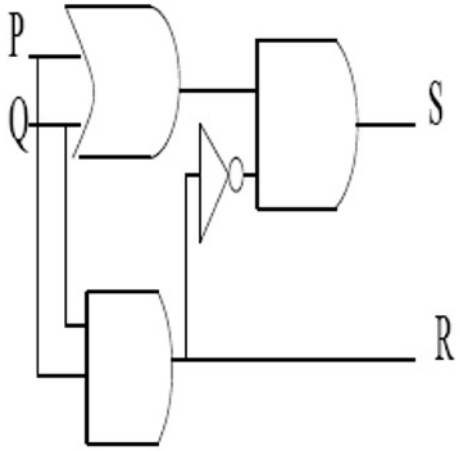
Problem 2.1
Write the input/output table for the circuit of Example 2.2 where P, Q, and R are any inputs.

Problem 2.2
Construct the circuit corresponding to the Boolean expression: $(P \wedge Q) \vee \sim R$.

Problem 2.3
For the following input/output table, construct (a) the corresponding Boolean expression and (b) the corresponding circuit:

P	Q	R	S
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	0

Problem 2.4
Consider the following circuit



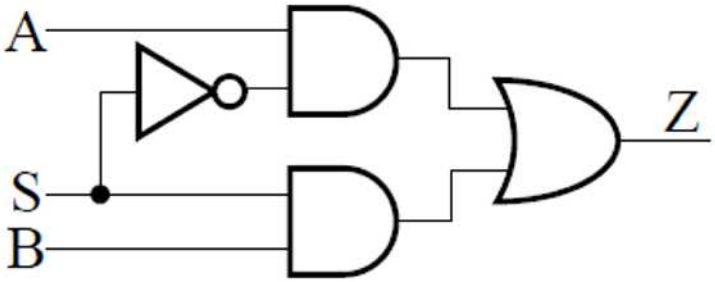
Complete the following table

P	Q	R	S
1	1		
1	0		
0	1		
0	0		

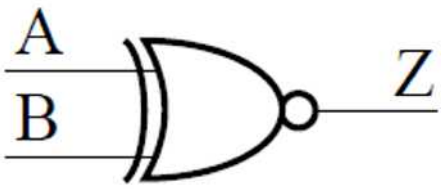
Problem 2.5
(a) Convert 1043_{10} to base 2.
(b) Convert 01101101_2 to base 10.

Problem 2.6
Express the numbers 104 and -104 in two's complement representation with 8 bits.

Problem 2.7
Construct the input/output table of the circuit given below.



Problem 2.8
The negation of the exclusive or is the exclusive nor (abbreviated by XNOR) whose gate is shown below.

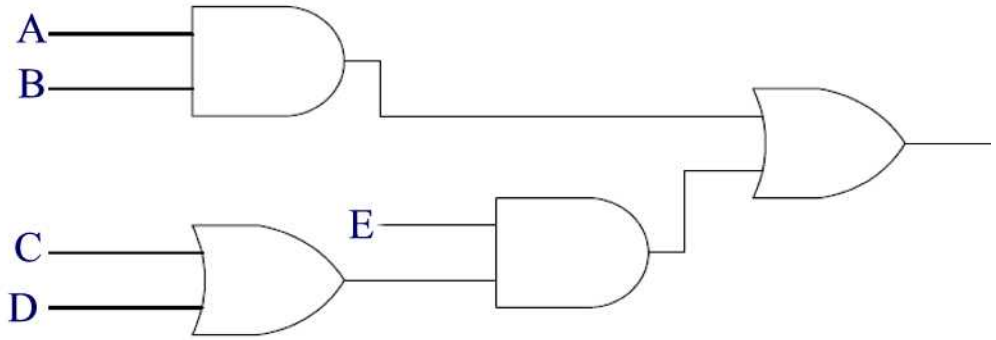


Contruct the input/output table of this gate.

Problem 2.9
Show that $A \oplus A$ and $A \oplus (\sim A)$ are constants.

Problem 2.10
Construct a circuit whose Boolean expression is $Q = (A \wedge B) \vee [(B \wedge C) \wedge (B \vee C)]$.

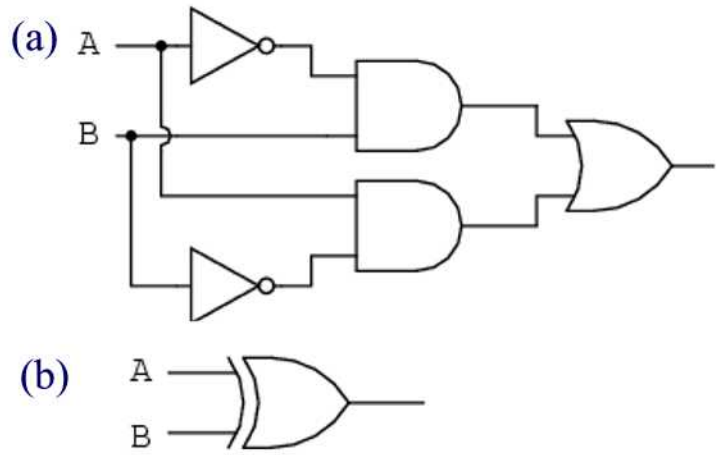
Problem 2.11
Find the Boolean expression that corresponds to the circuit.



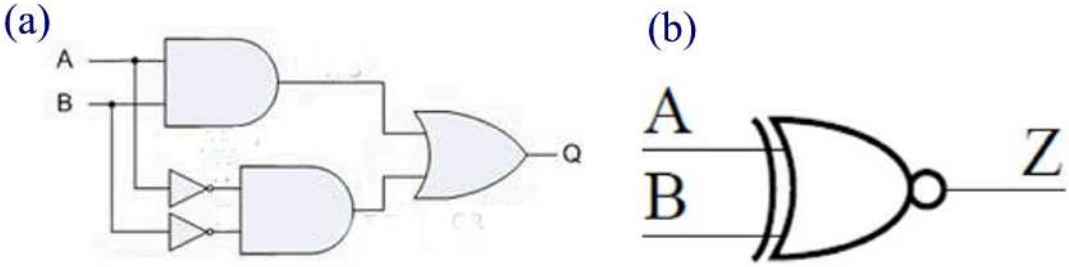
Problem 2.12
Find the Boolean expression S that corresponds to the input output table, where P, Q, and R are the Boolean variables.

P	Q	R	S
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	0

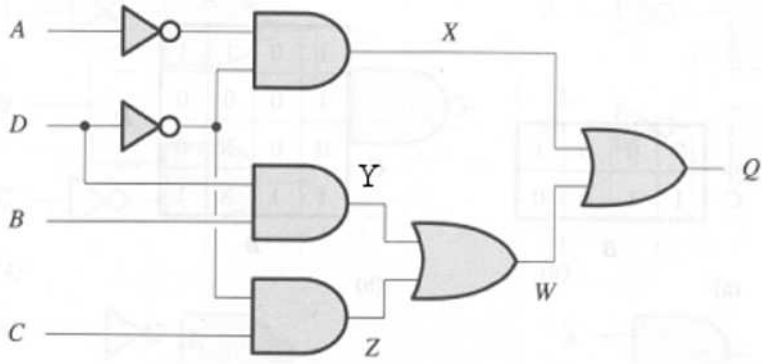
Problem 2.13
Show that the following two circuits are equivalent:



Problem 2.14
Show that the following two circuits are equivalent:



Problem 2.15
Let A, B, C and D be the Boolean variables of the circuit below. Find the Boolean Expressions: X, Y, Z, W, and Q.



Problem 2.16
(a) Write the number 513_{10} in base 2.
(b) Write the number 1110_2 in base 10.

Problem 2.17
Write the two's complement values of the numbers 7 and -2 in (a) 4-bit format (b) 8-bit format (c) 16-bit format.

Problem 2.18
Represent the integer -72_{10} as an 8-bit two's complement.

Problem 2.19
Convert 81_{10} to an 8-bit two's complememt.

Problem 2.20
What is the decimal representation for the integer with 8-bit two's complement 10010011?

Problem 2.21
What is the decimal representation for the integer with 8-bit two's complement 01001000?

3 Conditional and Biconditional Propositions

Let p and q be propositions. The **conditional proposition** $p \to q$ is the proposition that is false only when p is true and q is false; otherwise it is true. p is called the **hypothesis** and q is called the **conclusion.** The connective $\to$ is called the **conditional connective**.

Example 3.1
Construct the truth table of the implication $p \to q$.

Solution.
The truth table is

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

■

Example 3.2
Show that $p \to q \equiv (\sim p) \vee q$.

Solution.

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

■

It follows from the previous example that the proposition $p \to q$ is always true if the hypothesis p is false, regardless of the truth value of q. We say that $p \to q$ is **true by default** or **vacuously true**.
In terms of words the proposition $p \to q$ also reads:
(a) if p then q.
(b) p implies q.
(c) p is a sufficient condition for q.
(d) q is a necessary condition for p.
(e) p only if q.

Remark 3.1
In a purely logical sense, conditional sentences do not necessarily imply a cause and effect between the components p and q, although in mathematics and in general discourse they do. From a logical point of view the proposition "If $2+3=7$ then I $-1>0$" is a true proposition although there is no relationship between the component parts.

In propositional functions that involve the connectives $\sim, \wedge, \vee$, and $\rightarrow$ the order of operations is that $\sim$ is performed first and $\rightarrow$ is performed last.

Example 3.3
Show that $\sim (p \rightarrow q) \equiv p \wedge (\sim q)$.

Solution.
We use De Morgan's laws as follows.

$$\begin{aligned} \sim (p \rightarrow q) &\equiv \sim [(\sim p) \vee q) \\ &\equiv [\sim (\sim p)] \wedge (\sim q) \\ &\equiv p \wedge (\sim q) \ \blacksquare \end{aligned}$$

The converse of $p \rightarrow q$ is the proposition $q \rightarrow p$. The **opposite** or **inverse** of $p \rightarrow q$ is the proposition $\sim p \rightarrow \sim q$. The **contrapositive** of $p \rightarrow q$ is the proposition $\sim q \rightarrow \sim p$.

Example 3.4
Find the converse, opposite, and the contrapositive of the implication: " If $1+2=4$ then President Lincoln is from Illinois."

Solution.
The converse: If President Lincoln is from Illinois then $1+2=4$.
The opposite: If $1+2 \neq 4$ then President Lincoln is not from Illinois.
The contrapositive: If President Lincoln is not from Illinois then $1+2 \neq 4$ ■

Example 3.5
Show that $p \rightarrow q \equiv \sim q \rightarrow \sim p$.

Solution.
We use De Morgan's laws as follows.

$$\begin{aligned} p \to q \equiv & (\sim p) \vee q \\ \equiv & \sim [p \wedge (\sim q)] \\ \equiv & \sim [(\sim q) \wedge p] \\ \equiv & [\sim (\sim q)] \vee (\sim p) \\ \equiv & q \vee (\sim p) \\ \equiv & \sim q \to \sim p \ \blacksquare \end{aligned}$$

Example 3.6
Using truth tables show the following:
(a) $p \to q \not\equiv q \to p$.
(b) $p \to q \not\equiv \sim p \to \sim q$.

Solution.
(a) It suffices to show that $(\sim p) \vee q \not\equiv (\sim q) \vee p$.

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

(b) We will show that $(\sim p) \vee q \not\equiv p \vee (\sim q)$.

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

$\blacksquare$

The **biconditional proposition** of p and q, denoted by $p \leftrightarrow q$, is the propositional function that is true when both p and q have the same truth values and false if p and q have opposite truth values. Also reads, "p if and only if q" or "p is a necessary and sufficient condition for q."

Example 3.7
Construct the truth table for $p \leftrightarrow q$.

Solution.

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

■

Example 3.8
Show that the biconditional proposition of p and q is logically equivalent to the conjunction of the conditional propositions $p \rightarrow q$ and $q \rightarrow p$.

Solution.

p	q	$p \rightarrow q$	$q \rightarrow p$	$p \leftrightarrow q$	$(p \rightarrow q) \wedge (q \rightarrow p)$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

■

The order of operations for the five logical connectives is as follows:
1. $\sim$
2. $\wedge, \vee$ in any order.
3. $\rightarrow, \leftrightarrow$ in any order.

Review Problems

Problem 3.1
Construct the truth table for the proposition: $(\sim p) \vee q \rightarrow r$.

Problem 3.2
Construct the truth table for the proposition: $(p \rightarrow r) \leftrightarrow (q \rightarrow r)$.

Problem 3.3
Write negations for each of the following propositions.
(a) If $2 + 2 = 4$, then 2 is a prime number.
(b) If $1 = 0$ then $\sqrt{2}$ is rational.

Problem 3.4
Write the contrapositives for the propositions of Problem 3.3.

Problem 3.5
Write the converses for the propositions of problem 3.3

Problem 3.6
Write the inverses for the propositions of problem 3.3

Problem 3.7
Show that $p \vee q \equiv (p \rightarrow q) \rightarrow q$.

Problem 3.8
Show that $\sim (p \leftrightarrow q) \equiv (p \wedge \sim q) \vee (\sim p \wedge q)$.

Problem 3.9
Let $p : 2 > 3$ and $q : 0 < 5$. Find the truth value of $p \rightarrow q$ and $q \rightarrow p$.

Problem 3.10
Assuming that p is true, q is false, and r is true, find the truth value of each proposition.
(a) $p \wedge q \rightarrow r$.
(b) $p \vee q \rightarrow \sim r$.
(c) $p \vee (q \rightarrow r)$.

Problem 3.11
Show using a chain of logical equivalences that $(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$.

Problem 3.12
Show using a chain of logical equivalences that $p \leftrightarrow q \equiv (p \wedge q) \vee (\sim p \wedge \sim q)$.

Problem 3.13
(a) What are the truth values of p and q for which a conditional proposition and its inverse are both true?
(b) What are the truth values of p and q for which a conditional proposition and its inverse are both false?

Problem 3.14
Show that $p \leftrightarrow q \equiv \sim (p \oplus q)$.

Problem 3.15
Determine whether the following propostion is true or false: "If the moon is made of milk then I am smarter than Einstein."

Problem 3.16
Construct the truth table of $\sim p \wedge (p \to q)$.

Problem 3.17
Show that $(p \to q) \vee (q \to q)$ is a tautology.

Problem 3.18
Construct a truth table for $(p \to q) \wedge (q \to r)$.

Problem 3.19
Find the converse, inverse, and contrapositive of"It is raining is a necessary condition for me not going to town.

Problem 3.20
Show that $(p \wedge \sim q) \vee q \leftrightarrow p \vee q$ is a tautology.

4 Related Propositions: Inference Logic

The main concern of logic is how the truth of some propositions is connected with the truth of another. Thus, we will usually consider a group of related propositions.
An **argument** is a set of two or more propositions related to each other in such a way that all but one of them, the **premises**, are supposed to provide support for the remaining one, the **conclusion**.
The transition from premises to conclusion is the **inference** upon which the argument relies.

Example 4.1
Show that the propositions "The star is made of milk, and strawberries are red. My dog has fleas." do not form an argument.

Solution.
Indeed, the truth or falsity of each of the propositions has no bearing on that of the others ■

Example 4.2
Show that the propositions: "Mark is a lawyer. So Mark went to law school since all lawyers have gone to law school" form an argument.

Solution.
This is an argument. The truth of the conclusion, "Mark went to law school," is inferred or deduced from its premises, "Mark is a lawyer" and "all lawyers have gone to law school." ■

The above argument can be represented as follows: Let
p : Mark is a lawyer.
q : All lawyers have gone to law school.
r : Mark went to law school.
Then

$$\begin{array}{l} p \wedge q \\ \hline \therefore \quad r \end{array}$$

The symbol $\therefore$ is to indicate the inferrenced conclusion.

Now, suppose that the premises of an argument are all true. Then the conclusion may be either true or false. When the conclusion is true then the argument is said to be **valid.** When the conclusion is false then the argument is said to be **invalid.**
To test an argument for validity one proceeds as follows:
(1) Identify the premises and the conclusion of the argument.
(2) Construct a truth table including the premises and the conclusion.
(3) Find rows in which all premises are true.
(4) In each row of Step (3), if the conclusion is true then the argument is valid; otherwise the argument is invalid.

Example 4.3
Show that the argument

$$\begin{array}{l} p \to q \\ \underline{q \to p} \\ \therefore \quad p \vee q \end{array}$$

is invalid

Solution.
We construct the truth table as follows.

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

From the last row we see that the premises are true but the conclusion is false. The argument is then invalid ■

Next, we discuss some basic **rules of inference**.

Example 4.4 *(Modus Ponens or the method of affirmative)*
Show that the argument

$$\begin{array}{l} p \to q \\ p \\ \hline \therefore \quad q \end{array}$$

is valid.

Solution.
The truth table is as follows.

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

The first row shows that the argument is valid ■

Example 4.5 *(Modus Tollens or the method of denial)*
Show that the argument

$$\begin{array}{l} p \to q \\ \sim q \\ \hline \therefore \quad \sim p \end{array}$$

is valid.

Solution.
The truth table is as follows.

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

The last row shows that the argument is valid ■

Example 4.6 *(Disjunctive Addition)*
Show that the argument

$$\begin{array}{l} p \\ \hline \therefore \quad p \vee q \end{array}$$

is valid.

Solution.
The truth table is as follows.

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

The first and second rows show that the argument is valid ■

Example 4.7 *(Conjunctive addition)*
Show that

$$\begin{array}{l} p, q \\ \hline \therefore \quad p \wedge q \end{array}$$

is valid

Solution.
The truth table is as follows.

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

The first row shows that the argument is valid ■

Example 4.8 *(Conjunctive simplification)*
Show that the argument

$$\begin{array}{l} p \wedge q \\ \hline \therefore \quad p \end{array}$$

is valid.

Solution.
The truth table is as follows.

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

The first row shows that the argument is valid ■

Example 4.9 *(Disjunctive syllogism)*
Show that the argument

$$\begin{array}{l} p \vee q \\ \sim q \\ \hline \therefore \quad p \end{array}$$

is valid.

Solution.
The truth table is as follows.

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

The second row shows that the argument is valid ■

Example 4.10 *(Hypothetical syllogism)*
Show that the argument

$$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore \quad p \to r \end{array}$$

is valid.

Solution.
The truth table is as follows.

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

The first , fifth, seventh, and eighth rows show that the argument is valid ■

Example 4.11 *(Rule of contradiction)*
Show that if c is a contradiction then the following argument is valid for any p.

$$\begin{array}{l} \sim p \to c \\ \hline \therefore \quad p \end{array}$$

Solution.
Constructing the truth table we find

c	p	$\sim p \to c$
F	T	T
F	F	F

The first row shows that the argument is valid ■

Review Problems

Problem 4.1
Show that the propositions "Abraham Lincolm was the president of the United States, and blueberries are blue. My car is yellow" do not form an argument.

Problem 4.2
Show that the propositions: "Steve is a physician. So Steve went to medical school since all doctors have gone to medical school" form an argument. Identify the premises and the conclusion.

Problem 4.3
Show that the argument

$$\begin{array}{l} \sim p \vee q \rightarrow r \\ \sim p \vee q \\ \hline \therefore \quad r \end{array}$$

is valid.

Problem 4.4
Show that the argument

$$\begin{array}{l} p \rightarrow q \\ q \\ \hline \therefore \quad p \end{array}$$

is invalid.

Problem 4.5
Show that the argument

$$\begin{array}{l} p \rightarrow q \\ \sim p \\ \hline \therefore \quad \sim q \end{array}$$

is invalid.

Problem 4.6
Show that the argument

$$\begin{array}{l} q \\ \hline \therefore \quad p \vee q \end{array}$$

is valid.

Problem 4.7
Show that the argument

$$\begin{array}{l} p \wedge q \\ \hline \therefore \quad q \end{array}$$

is valid.

Problem 4.8
Show that the argument

$$\begin{array}{l} p \vee q \\ \sim p \\ \hline \therefore \quad q \end{array}$$

is valid.

Problem 4.9
Use modus ponens or modus tollens to fill in the blanks in the argument below so as to produce valid inferences.

If $\sqrt{2}$ is rational, then $\sqrt{2} = \frac{a}{b}$ for some integers a and b.
It is not true that $\sqrt{2} = \frac{a}{b}$ for some integers a and b.

$\therefore$ _____

Problem 4.10
Use modus ponens or modus tollens to fill in the blanks in the argument below so as to produce valid inferences.

If logic is easy, then I am a monkey's uncle.
I am not a monkey's uncle.
$\therefore$ _____

Problem 4.11
Use a truth table to determine whether the argument below is invalid.

$$p \to q$$
$$q \to p$$
$$\_\_\_\_\_$$
$$\therefore \quad p \wedge q$$

Problem 4.12
Use a truth table to determine whether the argument below is valid.

$$p$$
$$p \to q$$
$$\sim q \vee r$$
$$\_\_\_\_\_$$
$$\therefore \quad r$$

Problem 4.13
Use symbols to write the logical form of the given argument and then use a truth table to test the argument for validity.
If Tom is not on team A, then Hua is on team B.
If Hua is not on team B, then Tom is on team A.
$\therefore$ Tom is not on team A or Hua is not on team B.

Problem 4.14
Use symbols to write the logical form of the given argument and then use a truth table to test the argument for validity.
If Jules solved this problem correctly, then Jules obtained the answer 2.
Jules obtained the answer 2.
$\therefore$ Jules solved this problem correctly.

Problem 4.15
Use symbols to write the logical form of the given argument and then use a truth table to test the argument for validity.
If this number is larger than 2, then its square is larger than 4.
This number is not larger than 2.
$\therefore$ The square of this number is not larger than 4.

Problem 4.16
Use the valid argument forms of this section to deduce the conclusion from the premises.

$$\begin{array}{l} \sim p \vee q \rightarrow r \\ s \vee \sim q \\ \sim t \\ p \rightarrow t \\ \sim p \wedge r \rightarrow \sim s \\ \hline \therefore \quad \sim q \end{array}$$

Problem 4.17
Use the valid argument forms of this section to deduce the conclusion from the premises.

$$\begin{array}{l} \sim p \rightarrow r \wedge \sim s \\ t \rightarrow s \\ u \rightarrow \sim p \\ \sim w \\ u \vee w \\ \hline \therefore \quad \sim t \vee w \end{array}$$

Problem 4.18
Use the valid argument forms of this section to deduce the conclusion from

the premises.

$$\begin{array}{l} \sim (p \vee q) \rightarrow r \\ \sim p \\ \sim r \\ \hline \therefore \quad q \end{array}$$

Problem 4.19
Use the valid argument forms of this section to deduce the conclusion from the premises.

$$\begin{array}{l} p \wedge q \\ p \rightarrow \sim (q \wedge r) \\ s \rightarrow r \\ \hline \therefore \quad \sim s \end{array}$$

Problem 4.20
Show that

$$\begin{array}{l} p \rightarrow (q \rightarrow r) \\ \sim (q \rightarrow r) \\ \hline \therefore \quad \sim p \end{array}$$

5 Predicates and Quantifiers

Statements such as "$x > 3$" or "$x^2 + 4 \geq 4$" are often found in mathematical assertions and in computer programs. These statements are not propositions when the variables are not specified. However, one can produce propositions from such statements.

A **predicate** is an expression involving one or more variables defined on some domain, called the **domain of discourse**. Substitution of a particular value for the variable(s) produces a proposition which is either true or false. For instance, $P(n) : n \textit{ is prime}$ is a predicate on the set of natural numbers[1] $\mathbb{N}$. Observe that $P(1)$ is false, $P(2)$ is true. In the expression $P(x)$, x is called a **free variable**. As x varies the truth value of $P(x)$ varies as well. The set of true values of a predicate $P(x)$ is called the **truth set** and will be denoted by T_P.

Example 5.1
Let $Q(x, y) : x = y + 3$ with domain $\mathbb{Z}^+$. What are the truth values of the propositions $Q(1, 2)$ and $Q(3, 0)$?

Solution.
By substitution in the expression of Q we find: $Q(1, 2)$ is false since $1 = x \neq y + 3 = 5$. On the contrary, $Q(3, 0)$ is true since $x = 3 = 0 + 3 = y + 3$ ■

If $P(x)$ and $Q(x)$ are two predicates with a common domain D then the notation $P(x) \Rightarrow Q(x)$ means that every element in the truth set of $P(x)$ is also an element in the truth set of $Q(x)$. Same logical manipulations that were used with propositions can be used with predicates. For example, $P(x) \Rightarrow Q(x)$ is the same as $\sim P(x) \vee Q(x)$.

Example 5.2
Consider the two predicates $P(x) : x$ is a factor of 4 and $Q(x) : x$ is a factor of 8. Show that $P(x) \Rightarrow Q(x)$.

Solution.
Finding the truth set of each predicate we have: $T_P = \{1, 2, 4\}$ and $T_Q = \{1, 2, 4, 8\}$. Since every number appearing in T_P also appears in T_Q we have

[1] We define the set of **natural numbers** to be the set $\mathbb{N} = \{1, 2, 3, \cdots\}$. We will denote the set of all non-negative integers or the set of whole numbers by $\mathbb{W} = \mathbb{Z}^+ = \{0, 1, 2, \cdots\}$.

$P(x) \Rightarrow Q(x)$ ■

If two predicates $P(x)$ and $Q(x)$ with a common domain D are such that $T_P = T_Q$ then we use the notation $P(x) \Leftrightarrow Q(x)$.

Example 5.3
Let $D = \mathbb{R}$. Consider the two predicates $P(x) : -2 \leq x \leq 2$ and $Q(x) : |x| \leq 2$. Show that $P(x) \Leftrightarrow Q(x)$.

Solution.
Indeed, if x in T_P then the distance from x to the origin is at most 2. That is, $|x| \leq 2$ and hence x belongs to T_Q. Now, if x is an element in T_Q then $|x| \leq 2$, i.e. $(x-2)(x+2) \leq 0$. Solving this inequality we find that $-2 \leq x \leq 2$. That is, $x \in T_P$ ■

Quantifiers
A **quantifier** turns a predicate into a proposition without assigning specific values for the variable. There are primarily two quantifiers: Universal quantifier and existential quantifier. The **universal quantification** of a predicate $P(x)$ is the proposition $\forall x \in D, P(x)$ is true, where the symbol $\forall$ is the **universal quantifier**. For example, if k is a non-negative integer, then the predicate $P(k) : 2k \; is \; even$ is true for all $k \in \mathbb{Z}^+ = \mathbb{W}$. Using the universal quantifier $\forall$, we can write,

$$\forall k \in \mathbb{Z}^+, (2k \; is \; even).$$

The proposition $\forall x \in D, P(x)$ is false if $P(x)$ is false for at least one value of x. In this case, x is called a **counterexample**.

Example 5.4
Show that the proposition $[\forall x \in \mathbb{R}, x > \frac{1}{x}]$ is false.

Solution.
A counterexample is $x = \frac{1}{2}$. Clearly, $\frac{1}{2} < 2 = \frac{1}{\frac{1}{2}}$ ■

Example 5.5
Write in the form $\forall x \in D, P(x)$ the proposition : "Every real number is either positive, negative or 0."

Solution.
$\forall x \in \mathbb{R}, x > 0, x < 0, or\ x = 0$ ■

The **existential quantification** of the predicate $P(x)$ is the proposition $\exists x \in D, P(x)$ that is true if there is at least one value of $x \in D$ where $P(x)$ is true; otherwise it is false. The symbol $\exists$ is called the **existential quantifier**.

Example 5.6
Let $P(x)$ denote the statement "$x > 3$." What is the truth value of the proposition $\exists x \in \mathbb{R}, P(x)$.

Solution.
Since $4 \in \mathbb{R}$ and $4 > 3$, the given proposition is true ■

The proposition $\forall x \in D, P(x) \Longrightarrow Q(x)$ is called the **universal conditional proposition.** For example, the proposition $\forall x \in \mathbb{R}$, if $x > 2$ then $x^2 > 4$ is a universal conditional proposition.

Example 5.7
Rewrite the proposition "If a real number is an integer then it is a rational number" as a universal conditional proposition.

Solution.
$\forall x \in \mathbb{R}$, if x is an integer then x is a rational number ■

Example 5.8
(a) What is the negation of the proposition $\forall x \in D, P(x)$?
(b) What is the negation of the proposition $\exists x \in D, P(x)$?
(c) What is the negation of the proposition $\forall x \in D, P(x) \Longrightarrow Q(x)$?

Solution.
(a) $\exists x \in D, \sim P(x)$. That is, there is an $x \in D$ where $P(x)$ is false.
(b) $\forall x \in D, \sim P(x)$. That is, $P(x)$ is false for all $x \in D$.
(c) There is an $x \in D$ such that $\sim (\sim P(x) \vee Q(x)) = P(x) \wedge \sim Q(x)$. That is, $P(x)$ is true and $Q(x)$ is false ■

Example 5.9
Write the negation of each of the following propositions:

(a) $\forall x \in \mathbb{R}, x > 3 \Longrightarrow x^2 > 9$.
(b) Every polynomial function is continuous.
(c) There exists a triangle with the property that the sum of the interior angles is different from 180°.

Solution.
(a) $\exists x \in \mathbb{R}, x > 3$ and $x^2 \leq 9$.
(b) There exists a polynomial that is not continuous everywhere.
(c) For any triangle, the sum of the interior angles is equal to 180° ■

Nested Quantifiers
Next, we discuss predicates that contain multiple quantifiers. A typical example is the definition of a limit. We say that $L = \lim_{x \to a} f(x)$ if and only if $\forall \epsilon > 0, \exists$ a positive number δ such that if $|x - a| \leq \delta$ then $|f(x) - L| < \epsilon$.

Example 5.10
(a) Let $P(x, y)$ denote the statement "$x + y = y + x$." What is the truth value of the proposition $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R}), P(x, y)$?
(b) Let $Q(x, y)$ denote the statement "$x + y = 0$." What is the truth value of the proposition $(\exists y \in \mathbb{R})(\forall x \in \mathbb{R}), Q(x, y)$?

Solution.
(a) The given proposition is always true since addition of real numbers is commutative.
(b) The proposition is false. For otherwise, one can choose $x \neq -y$ to obtain $0 \neq x + y = 0$ which is impossible ■

Example 5.11
Find the negation of the following propositions:
(a) $\forall x \exists y, P(x, y)$.
(b) $\exists x \forall y, P(x, y)$.

Solution.
(a) $\exists x \forall y, \sim P(x, y)$.
(b) $\forall x \exists y, \sim P(x, y)$ ■

Example 5.12
The symbol $\exists!$ stands for the phrase "there exists a unique". Which of the following statements are true and which are false.
(a) $\exists! x \in \mathbb{R}, \forall y \in \mathbb{R}, xy = y$.
(b) $\exists!$ integer x such that $\frac{1}{x}$ is an integer.

Solution.
(a) True. Let $x = 1$.
(b) False since 1 and -1 are both integers with integer reciprocals ■

Review Problems

Problem 5.1
By finding a counterexample, show that the proposition: "For all positive integers n and $m, m.n \geq m + n$" is false.

Problem 5.2
Consider the statement

$$\exists x \in \mathbb{R} \text{ such that } x^2 = 2.$$

Which of the following are equivalent ways of expressing this statement?
(a) The square of each real number is 2.
(b) Some real numbers have square 2.
(c) The real number x has square 2.
(d) If x is a real number, then $x^2 = 2$.
(e) There is at least one real number whose square is 2.

Problem 5.3
Rewrite the following propositions informally in at least two different ways without using the symbols $\exists$ and $\forall$:
(a) $\forall$ squares x, x is a rectangle.
(b) $\exists$ a set A such that A has 16 subsets.

Problem 5.4
Rewrite each of the following statements in the form "$\exists$___x *such that*___":
(a) Some exercises have answers.
(b) Some real numbers are rational numbers.

Problem 5.5
Rewrite each of the following statements in the form "$\forall$___, if___$then$___.":
(a) All COBOL programs have at least 20 lines.
(b) Any valid argument with true premises has a true conclusion.
(c) The sum of any two even integers is even.
(d) The product of any two odd integers is odd.

Problem 5.6
Which of the following is a negation for "Every polynomial function is continuous"?

(a) No polynomial function is continuous.
(b) Some polynomial functions are discontinuous.
(c) Every polynomial function fails to be continuous.
(d) There is a non-continuous polynomial function.

Problem 5.7
Determine whether the proposed negation is correct. If it is not, write a correct negation.
Proposition : For all integers n, if n^2 is even then n is even.
Proposed negation : For all integers n, if n^2 is even then n is not even.

Problem 5.8
Let $D = \{-48, -14, -8, 0, 1, 3, 16, 23, 26, 32, 36\}$. Determine which of the following propositions are true and which are false. Provide counterexamples for those propositions that are false.
(a) $\forall x \in D$, if x is odd then $x > 0$.
(b) $\forall x \in D$, if x is less than 0 then x is even.
(c) $\forall x \in D$, if x is even then $x \leq 0$.
(d) $\forall x \in D$, if the ones digit of x is 2, then the tens digit is 3 or 4.
(e) $\forall x \in D$, if the ones digit of x is 6, then the tens digit is 1 or 2.

Problem 5.9
Write the negation of the proposition :$\forall x \in \mathbb{R}$, if $x(x+1) > 0$ then $x > 0$ or $x < -1$.

Problem 5.10
Write the negation of the proposition : If an integer is divisible by 2, then it is even.

Problem 5.11
Given the following true propostion: "$\forall$ real numbers x, $\exists$ an integer n such that $n > x$." For each x given below, find an n to make the predicate $n > x$ true.
(a) $x = 15.83$ (b) $x = 10^8$ (c) $x = 10^{10^{10}}$.

Problem 5.12
Given the proposition: $\forall x \in \mathbb{R}, \exists$ a real number y such that $x + y = 0$.
(a) Rewrite this proposition in English without the use of the quantifiers.
(b) Find the negation of the given proposition.

Problem 5.13
Given the proposition: $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}$, $x + y = 0$.
(a) Rewrite this proposition in English without the use of the quantifiers.
(b) Find the negation of the given proposition.

Problem 5.14
Consider the proposition "Somebody is older than everybody." Rewrite this proposition in the form "$\exists$ a person x such that $\forall$ _____."

Problem 5.15
Given the proposition: "There exists a program that gives the correct answer to every question that is posed to it."
(a) Rewrite this proposition using quantifiers and variables.
(b) Find a negation for the given proposition.

Problem 5.16
Given the proposition: $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ such that $x < y$.
(a) Write a proposition by interchanging the symbols $\forall$ and $\exists$.
(b) State which is true: the given proposition, the one in part (a), neither, or both.

Problem 5.17
Find the contrapositive, converse, and inverse of the proposition "$\forall x \in \mathbb{R}$, if $x(x + 1) > 0$ then $x > 0$ or $x < -1$."

Problem 5.18
Find the truth set of the predicate $P(x) : x + 2 = 2x$ where the domain of discourse is the set of real numbers.

Problem 5.19
Let $P(x)$ be the predicate $x + 2 = 2x$, where the domain of discourse is the set $\{1, 2, 3\}$. Which of the following statements are true?
(i) $\forall x, P(x)$ (ii) $\exists x, P(x)$.

Problem 5.20
Let $P(x, y)$ be the predicate $x + y = 10$ where x and y are any real numbers. Which of the following statements are true?
(a) $(\forall x)(\exists y), P(x, y)$.
(b) $(\exists y)(\forall x), P(x, y)$.

Fundamentals of Mathematical Proofs

In this chapter we discuss some common methods of proof and the standard terminology that accompanies them.

6 Methods of Direct Proof

A **mathematical system** consists of axioms, definitions, and undefined terms. An **axiom** is a statement that is assumed to be true. A **definition** is used to create new concepts in terms of existing ones. A **theorem** is a proposition that has been proved to be true. A **lemma** is a theorem that is usually not interesting in its own right but is useful in proving another theorem. A **corollary** is a theorem that follows quickly from a theorem.

Example 6.1
The Euclidean geometry furnishes an example of mathematical system:
• points and lines are examples of undefined terms.
• An example of a definition: Two angles are supplementary if the sum of their measures is $180°$.
• An example of an axiom: Given two distinct points, there is exactly one line that contains them.
• An example of a theorem: If two sides of a triangle are equal, then the angles opposite them are equal.
• An example of a corollary: If a triangle is equilateral, then it is equiangular.

An argument that establishes the truth of a theorem is called a **proof**. **Logic** is a tool for the analysis of proofs.

First we discuss methods for proving a theorem of the form "$\exists x$ such that $P(x)$." This theorem guarantees the existence of at least one x for which the predicate $P(x)$ is true. The proof of such a theorem is **constructive**: that is, the proof is either by finding a particular x that makes $P(x)$ true or by exhibiting an algorithm for finding x.

Example 6.2
Show that there exists a positive integer whose square can be written as the sum of the squares of two positive integers.

Solution.
Indeed, one example is $5^2 = 3^2 + 4^2$ ■

Example 6.3
Show that there exists an integer x such that $x^2 = 15,129$.

Solution.
We will use the well-known algorithm of extracting the square root as follows:
Step 1. Group the numbers in pairs starting from right to left. We obtain $\sqrt{01\ 51\ 29}$.
Step 2. Then, using the first pair, (01) find the largest positive integer whose square is less than or equal to 1. In this case, it is 1. Put 1 on top of the square root sign:

$$\begin{array}{l} \phantom{\sqrt{}}1 \\ \sqrt{1\ 51\ 29} \end{array}$$

Step 3. Subtract the square of the number on top, that is 1, from the first pair and then bring down the next pair of numbers (51):

$$\begin{array}{l} \phantom{\sqrt{}}1 \\ \sqrt{1\ 51\ 29} \\ 51 \end{array}$$

Step 4. Double 1 to get 2 and put 2 next to 51 on the left side:

$$\begin{array}{l} \phantom{\sqrt{}}1 \\ \sqrt{1\ 51\ 29} \\ 2\quad 51 \end{array}$$

Step 5: Find the largest digit z such that $2z \times z \leq 51$. In this case, $z = 2$. Put 2 next to 1 above the square root sign and then subtract 44 from 51:

$$\begin{array}{rl} & \phantom{\sqrt{}}12 \\ & \sqrt{1\ 51\ 29} \\ 22 \times 2 & \quad 51 \\ & \quad \underline{44} \\ & \quad\ 7 \end{array}$$

Step 6: Bring down the pair (29):

$$\begin{array}{rr} & 12 \\ & \sqrt{1\ 51\ 29} \\ 22 \times 2 & 51 \\ & \underline{44} \\ & 729 \end{array}$$

Step 7: Double 12 to get 24 and write it to the left of 729.

$$\begin{array}{rr} & 12 \\ & \sqrt{1\ 51\ 29} \\ 22 \times 2 & 51 \\ & \underline{44} \\ 24 & 729 \end{array}$$

Step 8: Find the largest digit z such that $24z \times z \leq 729$. In this case, $z = 3$. Put 3 next to 12 above the square root sign and then subtract 729 from 729 to obtain a zero remainder:

$$\begin{array}{rr} & 123 \\ & \sqrt{1\ 51\ 29} \\ 22 \times 2 & 51 \\ & \underline{44} \\ 243 \times 3 & 729 \\ & \underline{729} \\ & 0. \end{array}$$

Hence, $\sqrt{15129} = 123$ ■

In contrast to constructive existence proofs, a **non-constructive existence proof** uses known results to imply the existence of an x such that $P(x)$ is true without the need of knowing the actual value of x. We illustrate this method in the next example.

Example 6.4
In Calculus, the Intermediate Value Theorem states that if a function f is continuous in a closed interval $[a, b]$ and c is a number between $f(a)$ and $f(b)$ then the equation $f(x) = c$ has at least one solution in the open interval (a, b). Use the IVT to show that the equation $x^5 + 2x^3 + x - 5 = 0$ has a solution in the interval $(1, 2)$.

Solution.
Let $f(x) = x^5 + 2x^3 + x - 5$. Note that $f(1) = -1$ and $f(2) = 45$ so that $f(1) < 0 < f(2)$. Since f is continuous in $[1, 2]$, by the Intermediate Value Theorem, there is a number $1 < c < 2$ such that $f(c) = 0$. That is, $x^5 + 2x^3 + x - 5 = 0$ has a solution in the interval $(1, 2)$ ■

Next, we consider theorems of the form "$\forall x \in D,\ P(x)$." If D is a finite set, then one checks the truth value of $P(x)$ for each $x \in D$. This method is called the **method of exhaustion.**

Example 6.5
Show that for each positive integer $1 \leq n \leq 10$, $n^2 - n + 11$ is a prime number.

Solution.
In this example,

$$D = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

and $P(n) = n^2 - n + 11$ is a prime number. Using the method of exhaustion we see that

$$\begin{array}{llll} P(1) = 11 & ; \quad P(2) = 13 & ; \ P(3) = 17 & ; \ P(4) = 23 \\ P(5) = 31 & ; \quad P(6) = 41 & ; \ P(7) = 53 & ; \ P(8) = 67 \\ P(9) = 83 & ; \ P(10) = 101 & & \end{array}$$ ■

The proposition "$\forall x \in D,\ P(x)$" can be written in the form "$\forall x$ if $x \in D$ then $P(x)$." Thus, we consider propositions of the form "$\forall x \in D$ if $P(x)$ then $Q(x)$." We call $P(x)$ the **hypothesis** and $Q(x)$ the **conclusion**.

By a **direct method of proof** we mean a method that consists of showing that if $P(x)$ is true for $x \in D$ then $Q(x)$ is also true.

The following shows the format of the direct proof of a theorem.

Theorem 6.1
For all $n, m \in \mathbb{Z}$, if m and n are even then so is $m + n$.

Proof.
Let m and n be two even integers. Then there exist integers k_1 and k_2 such that $n = 2k_1$ and $m = 2k_2$. We must show that $m + n$ is even, that is, an integer multiple of 2. Indeed,

$$m + n = 2k_1 + 2k_2 = 2(k_1 + k_2) = 2k$$

where $k = k_1 + k_2 \in \mathbb{Z}$. Thus, by the definition of even, $m + n$ is even ■

Example 6.6
Prove the following theorem.

Theorem Every integer is a rational number. That is, for all n, if $n \in \mathbb{Z}$ then $n \in \mathbb{Q}$.

Solution.
Proof. Let n be an arbitrary integer. Then $n = \frac{n}{1}$. By the definition of rational numbers, n is rational ■

Example 6.7
Prove the following theorem.

Theorem If $a, b \in \mathbb{Q}$ then $a + b \in \mathbb{Q}$.

Solution.
Proof. Let a and b be two rational numbers. Then there exist integers $a_1, a_2, b_1 \neq 0$, and $b_2 \neq 0$ such that $a = \frac{a_1}{b_1}$ and $b = \frac{a_2}{b_2}$. By the property of addition of two fractions we have

$$\begin{aligned} a + b =& \frac{a_1}{b_1} + \frac{a_2}{b_2} \\ =& \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}. \end{aligned}$$

By letting $p = a_1 b_2 + a_2 b_1 \in \mathbb{Z}$ and $q = b_1 b_2 \in \mathbb{Z}^*$ we get $a + b = \frac{p}{q}$. That is, $a + b \in \mathbb{Q}$ ■

Example 6.8
Prove the following corollary.

Corollary The double of a rational number is rational.

Solution.
Proof. Let $a = b$ in the previous theorem we see that $2a = a+a = a+b \in \mathbb{Q}$ ■

Common mistakes when writing a mathematical proof
Next, we point out of some common mistakes that must be avoided in proving theorems.

• **Arguing from examples**. The validity of a general statement can not be proved by just using a particular example. For example, suppose that we want to show that the sum of two even integers is an even integer. The statement that 2 and 4 are even integers such that $2 + 4 = 6$ is also even is not a proof of our general statement. A complete proof is the one provided in Theorem 6.1.

• Using the same letters to mean two different things. For example, suppose that m and n are any two given even integers. Then by writing $m = 2k$ and $n = 2k$ this would imply that $m = n$ which is inconsistent with the statement that m and n are arbitrary and can be different.

• **Jumping to a conclusion**. Let us illustrate by an example. Suppose that we want to show that if the sum of two integers is even so is their difference. Consider the following proof: Suppose that $m + n$ is even. Then there is an integer k such that $m + n = 2k$. Then, $m = 2k - n$ and so $m - n$ is even.
The problem with this proof is that the crucial step $m - n = 2k - n - n = 2(k - n)$ is missing. The author of the proof has jumped prematurely to a conclusion.

• **Begging the question** or **circular reasoning**. By that we mean that the author of a proof uses in his argument a fact that he is supposed to prove. For example, suppose that we want to show $x + \frac{1}{x} \geq 2$ for any positive real number x. Multiplying through by x, we obtain $x^2 + 1 \geq 2x$. Subtract $2x$ from both sides, we find $x^2 - 2x + 1 = (x - 1)^2 \geq 0$. Since the square

of any real number is greater than or equal to 0, then $x+\frac{1}{x} \geq 2$ must be true.

We end this section, to mentioning that for a proposition of the form $\forall x \in D$, if $P(x)$ then $Q(x)$ to be false it suffices to find an element $x \in D$ where $P(x)$ is true but $Q(x)$ is false. Such an x is called a **counterexample.**

Example 6.9
Disprove the proposition $\forall a, b \in \mathbb{R}$, if $a < b$ then $a^2 < b^2$.

Solution.
A counterexample is the following. Let $a = -2$ and $b = -1$. Then $a < b$ but $a^2 > b^2$ ■

Review Problems

A real number r is called **rational** if there exist two integers a and $b \neq 0$ such that $r = \frac{a}{b}$. A real number that is not rational is called **irrational.**

Problem 6.1
Show that there exist integers m and n such that $3m + 4n = 25$.

Problem 6.2
Show that there is a positive integer x such that $x^4 + 2x^3 + x^2 - 2x - 2 = 0$. Hint: Use the rational zero test.

Problem 6.3
Show that there exist two prime numbers whose product is 143.

Problem 6.4
Show that there exists a point in the Cartesian system that is not on the line $y = 2x - 3$.

Problem 6.5
Using a constructive proof, show that the number $r = 6.32152152...$ is a rational number.

Problem 6.6
Show that the equation $x^3 - 3x^2 + 2x - 4 = 0$ has at least one solution in the interval $(2, 3)$.

Problem 6.7
Use a non-constructive proof to show that there exist irrational numbers a and b such that a^b is rational. Hint: Look at the number $q = \sqrt{2}^{\sqrt{2}}$. Consider the cases q is rational or q is irrational.

Problem 6.8
Use the method of exhaustion to show: $\forall n \in \mathbb{N}$, if n is even and $4 \leq n \leq 21$ then n can be written as the sum of two prime numbers.

Problem 6.9
Use the method of exhaustion to show: $\forall n \in \mathbb{N}$, if n is prime and $n < 7$ then $2n + 1$ is prime.

Problem 6.10
Prove the following theorem: The product of two rational numbers is a rational number.

Problem 6.11
Use the previous problem to prove the following corollary: The square of any rational number is rational.

Problem 6.12
Use the method of constructive proof to show that if r and s are two real numbers then there exists a real number x such that $r < x < s$.

Problem 6.13
Disprove the following statement by finding a counterexample: $\forall x, y, z \in \mathbb{R}$, if $x > y$ then $xz > yz$.

Problem 6.14
Disprove the following statement by finding a counterexample: $\forall x \in \mathbb{R}$, if $x > 0$ then $\frac{1}{x+2} = \frac{1}{x} + \frac{1}{2}$.

Problem 6.15
Show that for any even integer n, we have $(-1)^n = 1$.

Problem 6.16
Show that the product of two odd integers is odd.

Problem 6.17
Identify the error in the following proof:"For all positive integer n, the product $(n-1)n(n+2)$ is divisible by 3 since $3(4)(5)$ is divisible by 3."

Problem 6.18
Identify the error in the following proof:" If n amd m are two different odd integers then there exists an integer k such that $n = 2k+1$ and $m = 2k+1$."

Problem 6.19
Identify the error in the following proof:"Suppose that m and n are integers such that $n + m$ is even. We want to show that $n - m$ is even. For $n + m$ to be even, n and m must be even. Hence, $n = 2k_1$ and $m = 2k_2$ so that $n - m = 2(k_1 - k_2)$ which is even."

Problem 6.20
Identify the error in proving that if a product of two integers x and y is divisible by 5 then x is divisible by 5 or y is divisible by 5:" Since xy is divisible by 5, there is an integer k such that $xy = 5k$. Hence, $x = 5k_1$ for some k_1 or $y = 5k_2$ for some k_2. Thus, either x is divisible by 5 or y is divisible by 5."

Problem 6.21
Consider the system of integers where the numbers are considered as the undefined terms of the mathematical system. Examples of axioms are the arithmetic properties of addition such as commutativity, associativity, etc. In this system, consider the following definitions:
Definition 1: "A number is **even** if it can be written as an integer multiple of 2."
Definition 2: "A number is **odd** if it can be written as $2k + 1$ for some unique integer k."
Prove each of the following:
(a) Lemma: The product of two odd integers is always odd.
(b) Theorem: If the product of two integers m and n is even, then either m is even or n is even.
(c) Corollary: If n^2 is even then n is even.

7 More Methods of Proof

A **vacuous proof** is a proof of an implication $p \to q$ in which it is shown that p is false. Thus, if p is false then the implication is true regardless of the truth value of q.

Example 7.1
Use the method of vacuous proof to show that if $x \in \emptyset$ then 2 is an odd number.

Solution.
Since the proposition $x \in \emptyset$ is always false, the given proposition is vacuously true ■

Example 7.2
Show that if 4 is a prime number then $-4 = 4$.

Solution.
The hypothesis is false, therefore the implication is vacuously true (even though the conclusion is also false) ■

A **trivial proof** of an implication $p \to q$ is one in which q is shown to be true without any reference to p.

Example 7.3
Use the method of trivial proof to show that if n is an even integer then n is divisible by 1.

Solution.
Since the proposition n is divisible by 1 is always true, the given implication is trivially true. Notice that the hypothesis n is an even integer did not play a role in the proof ■

The method of **proof by cases** is a direct method of proving the conditional proposition $p_1 \vee p_2 \vee \cdots \vee p_n \to q$. The method consists of proving the conditional propositions $p_1 \to q, p_2 \to q, \cdots, p_n \to q$.

Example 7.4
Show that if n is a positive integer then $n^3 + n$ is even.

Solution.
We use the method of proof by cases.

Case 1. Suppose that n is even. Then there is $k \in \mathbb{N}$ such that $n = 2k$. In this case, $n^3 + n = 8k^3 + 2k = 2(4k^3 + k)$ which is even.

Case 2. Suppose that n is odd. Then there is a $k \in \mathbb{N}$ such that $n = 2k + 1$. So, $n^3 + n = 2(4k^3 + 6k^2 + 4k + 1)$ which is even ■

Example 7.5
Use the proof by cases to prove the triangle inequality: $|x + y| \leq |x| + |y|$.

Solution.
Case 1. $x \geq 0$ and $y \geq 0$. Then $x + y \geq 0$ and so $|x + y| = x + y = |x| + |y|$.
Case 2. $x \geq 0$ and $y < 0$. Then $x + y < x + 0 = |x| \leq |x| + |y|$. On the other hand, $-(x + y) = -x + (-y) \leq 0 + (-y) = |y| \leq |x| + |y|$. Thus, if $|x + y| = x + y$ then $|x + y| < |x| + |y|$ and if $|x + y| = -(x + y)$ then $|x + y| \leq |x| + |y|$.
Case 3. The case $x < 0$ and $y \geq 0$ is similar to case 2.
Case 4. Suppose $x < 0$ and $y < 0$. Then $x + y < 0$ and therefore $|x + y| = -(x + y) = (-x) + (-y) = |x| + |y|$.
So in all four cases $|x + y| \leq |x| + |y|$ ■

Now, given a real number x, the largest integer n less than or equal to x is called the **floor of** x and is denoted by $\lfloor x \rfloor$. The smallest integer n greater than or equal to x is called the **ceiling of** x and is denoted by $\lceil x \rceil$.

Example 7.6
Compute $\lfloor x \rfloor$ and $\lceil x \rceil$ for the following values of x :
(a) 37.999 (b) $-\frac{57}{2}$ (c) -14.001

Solution.
(a) $\lfloor 37.999 \rfloor = 37, \lceil 37.999 \rceil = 38$.
(b) $\lfloor -\frac{57}{2} \rfloor = -29, \lceil -\frac{57}{2} \rceil = -28$.
(c) $\lfloor -14.001 \rfloor = -15, \lceil -14.001 \rceil = -14$ ■

Remark 7.1
Note that if n is an integer than $\lfloor n \rfloor = \lceil n \rceil = n$.

Example 7.7
Use the proof by a counterexample to show that the proposition "$\forall x, y \in \mathbb{R}, \lfloor x+y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$" is false.

Solution.
Let $x = y = 0.5$. Then $\lfloor x+y \rfloor = 1$ and $\lfloor x \rfloor + \lfloor y \rfloor = 0$ ■

The following gives another example of the method of proof by cases.

Theorem 7.1
For any integer n,

$$\lfloor \frac{n}{2} \rfloor = \begin{cases} \frac{n}{2}, & \text{if } n \text{ is even} \\ \frac{n-1}{2}, & \text{if } n \text{ is odd} \end{cases}$$

Proof.
Let n be any integer. Then we consider the following two cases.

Case 1. n is odd. In this case, there is an integer k such that $n = 2k+1$. Hence,

$$\lfloor \frac{n}{2} \rfloor = \lfloor \frac{2k+1}{2} \rfloor = \lfloor k + \frac{1}{2} \rfloor = k.$$

Since $n = 2k+1$, solving this equation for k we find $k = \frac{n-1}{2}$. It follows that

$$\lfloor \frac{n}{2} \rfloor = k = \frac{n-1}{2}.$$

Case 2. Suppose n is even. Then there is an integer k such that $n = 2k$. Hence, $\lfloor \frac{n}{2} \rfloor = \lfloor k \rfloor = k = \frac{n}{2}$ ■

Proof of Many Equivalent Statements
In future math courses you will sometimes encounter a certain kind of theorem that is neither a conditional nor a biconditional statement. Instead, it asserts that a list of statements is "equivalent."
To say that statements $p_1, p_2, \cdots, p_n$ are all equivalent means that either they are all true or all false. To prove that they are equivalent, one assumes p_1 to be true and proves that p_2 is true, then assumes p_2 to be true and proves that p_3 is true, continuing in this fashion, assume that p_{n-1} is true and prove that p_n is true and finally, assume that p_n is true and prove that p_1 is true. This is known as the **proof by circular argument**. The logical equivalence of the above process is shown in Problem 7.20.

Example 7.8
Show that all the following statements are equivalent:
(i) $ad = bc$.
(ii) $\frac{a}{b} = \frac{c}{d}$.
(iii) $\frac{a+b}{b} = \frac{c+d}{d}$.
(iv) $\frac{a}{c} = \frac{b}{d}$
where a, b, c, and d are non-zero numbers.

Solution.
(i) $\Longrightarrow$ (ii): Suppose $ad = bc$. Divide both sides by bd to obtain $\frac{a}{b} = \frac{c}{d}$.
(ii) $\Longrightarrow$ (iii): Suppose $\frac{a}{b} = \frac{c}{d}$. Add 1 to both sides to obtain $\frac{a}{b} + 1 = \frac{c}{d} + 1$. Hence, $\frac{a+b}{b} = \frac{c+d}{d}$.
(iii) $\Longrightarrow$ (iv): Suppose $\frac{a+b}{b} = \frac{c+d}{d}$. Then $\frac{a}{b} + 1 = \frac{c}{d} + 1$. Subtract 1 from both sides to obtain $\frac{a}{b} = \frac{c}{d} = m$. Hence, $a = bm$ and $c = dm$. Thus, $\frac{a}{c} = \frac{bm}{dm} = \frac{b}{d}$.
(iv) $\Longrightarrow$ (i): Suppose that $\frac{a}{c} = \frac{b}{d} = m$. Then $a = cm$ and $ad = dcm$. Likewise, $b = dm$ and $bc = dcm$. It follows that $ad = bc$ ■

Review Problems

Problem 7.1
Using the method of vacuous proof, show that if n is a positive integer and $n = -n$ then $n^2 = n$.

Problem 7.2
Show that for all $x \in \mathbb{R}$, $x^2 + 1 < 0$ implies $x^2 \geq 4$.

Problem 7.3
Let $x \in \mathbb{R}$. Show that if $x^2 - 2x + 5 < 0$ then $x^2 + 1 < 0$.

Problem 7.4
Use the method of trivial proof to show that if $x \in \mathbb{R}$ and $x > 0$ then $x^2 + 1 > 0$.

Problem 7.5
Show that if 6 is a prime number then $6^2 = 36$.

Problem 7.6
Use the method of proof by cases to prove that for any integer n the product $n(n + 1)$ is even.

Problem 7.7
Use the method of proof by cases to prove that the square of any integer has the form $4k$ or $4k' + 1$ for some integers k and k'

Problem 7.8
Use the method of proof by cases to to prove that for any integer n, $n(n^2 - 1)(n + 2)$ is divisible by 4.

Problem 7.9
State a necessary and sufficient condition for the floor function of a real number to equal that number

Problem 7.10
Prove that if n is an even integer then $\lceil \frac{n}{2} \rceil = \frac{n}{2}$.

Problem 7.11
Show that the equality $\lfloor x - y \rfloor = \lfloor x \rfloor - \lfloor y \rfloor$ is not valid for all real numbers x and y.

Problem 7.12
Show that the equality $\lceil x+y \rceil = \lceil x \rceil + \lceil y \rceil$ is not valid for all real numbers x and y.

Problem 7.13
Prove that for all real numbers x and all integers m, $\lceil x+m \rceil = \lceil x \rceil + m$.

Problem 7.14
Show that if n is an odd integer then $\lceil \frac{n}{2} \rceil = \frac{n+1}{2}$.

Problem 7.15
Prove that all of the following statements are equivalent:
(i) $x^2 - 4 = 0$.
(ii) $(x-2)(x+2) = 0$.
(iii) $x = -2$ or $x = 2$.

Problem 7.16
Let x and y be two real numbers. Show that all the following are equivalent:
(a) $x < y$ (b) $\frac{x+y}{2} > x$ (c) $\frac{x+y}{2} < y$.

Problem 7.17
Show that all the following are equivalent:
(a) $x^2 - 5x + 6 = 0$.
(b) $(x-2)(x-3) = 0$.
(c) $x - 2 = 0$ or $x - 3 = 0$.
(d) $x = 2$ or $x = 3$.

Problem 7.18
Use the method of proof by cases to show that for all $x \in \mathbb{R}$, we have $-5 \leq |x+2| - |x-3| \leq 5$.

Problem 7.19
Use the method of proof by cases to show that $\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$ for all $a, b \in \mathbb{R}$ with $b \neq 0$.

Problem 7.20
Using truth tables, show that $(p \leftrightarrow q) \wedge (q \leftrightarrow r) \wedge (r \leftrightarrow p) \equiv (p \rightarrow q) \wedge (q \rightarrow r) \wedge (r \rightarrow p)$.

8 Methods of Indirect Proofs: Contradiction and Contraposition

Recall that in a direct proof one starts with the hypothesis of an implication $p \to q$ and then proves that the conclusion is true. Any other method of proof will be referred to as an **indirect proof**. In this section we study two methods of indirect proofs, namely, the proof by contradiction and the proof by contrapositive.

Proof by contradiction

We want to show that q is true. Instead, we assume it is not, i.e., $\sim q$ is true, and derive that a proposition of the form $r \wedge \sim r$ is true. But $r \wedge \sim r$ is a contradiction which is always false (See Example 1.12). Hence, the assumption $\sim q$ must be false, so the original proposition q must be true.

Theorem 8.1
If n^2 is an even integer so is n.

Proof.
Suppose the contrary. That is suppose that n is odd. Then there is an integer k such that $n = 2k + 1$. In this case, $n^2 = 2(2k^2 + 2k) + 1$ is odd and this contradicts the assumption that n^2 is even. Hence, n must be even ■

The method of proof by contradiction is not limited to just proving conditional propositions of the form $p \to q$, it can be used to prove any kind of statement whatsoever. We illustrate this point in the next example.

Theorem 8.2
The number $\sqrt{2}$ is irrational.

Proof.
Suppose not. That is, suppose that $\sqrt{2}$ is rational. Then there exist two integers m and n with no common divisors such that $\sqrt{2} = \frac{m}{n}$. Squaring both sides of this equality we find that $2n^2 = m^2$. Thus, m^2 is even. By Theorem 8.1, m is even. That is, 2 divides m. But then $m = 2k$ for some integer k. Taking the square we find that $2n^2 = m^2 = 4k^2$, that is $n^2 = 2k^2$. This says that n^2 is even and by Theorem 8.1, n is even. We conclude that 2 divides both m and n and this contradicts our assumption that m and n have no common divisors. Hence, $\sqrt{2}$ must be irrational ■

Example 8.1
Use the proof by contradiction to show that there are no positive integers n and m such that $n^2 - m^2 = 1$.

Solution.
Suppose the contrary. Then $(n-m)(n+m) = 1$ implies the system of equation

$$\begin{cases} n - m = & 1 \\ n + m = & 1. \end{cases}$$

Solving this system we find $n = 1$ and $m = 0$, contradicting our assumption that n and m are positive integers ■

Proof by contrapositive
We already know that $p \to q \equiv \sim q \to \sim p$. So to prove $p \to q$ we sometimes instead prove $\sim q \to \sim p$.

Theorem 8.3
If n is an integer such that n^2 is odd then n is also odd.

Proof.
Suppose that n is an integer that is even. Then there exists an integer k such that $n = 2k$. But then $n^2 = 2(2k^2)$ which is even ■

Remark 8.1
How is the proof by contrapositive different from the proof by contradicton? Let's examine how the two methods work when trying to prove $p \to q$. Using the method by contradiction, we assume that p and $\sim q$ and derive a contradiction. Using the method of contrapositive, we assume $\sim q$ and prove $\sim p$. Hence, the method of contrapositive has the advantage that your goal is clear: Prove $\sim p$. In the method of contradiction, your goal is to prove a contradiction, but it is not always clear what the contradiction is going to be at the start.

Example 8.2
Prove by the method of contrapositive: If a and b are two integers such that $a \cdot b$ is even then at least one the two must be even.

Solution.
Suppose that a and b are both odd. Then there exist integers m and n such that $a = 2m + 1$ and $b = 2n + 1$. Thus, $a \cdot b = (2m + 1)(2n + 1) = 2(2mn + m + n) + 1 = 2k + 1$ where $k = 2mn + m + n \in \mathbb{Z}$. Hence, $a \cdot b$ is odd ■

Example 8.3 *(Perfect squares test)*
Prove by the method of contrapositive: If n is a positive integer such that the remainder of the division of n by 4 is either 2 or 3, then n is not a perfect square.

Solution.
Suppose that n is a perfect square. Then $n = k^2$ for some $k \in \mathbb{Z}$.
• If the remainder of the division of k by 4 is 0 then $k = 4m_1$ and $n = 16m_1^2 = 4(4m_1^2)$ so that the remainder of the division of n by 4 is 0.
• If the remainder of the division of k by 4 is 1 then $k = 4m_2 + 1$ and $n = 4(4m_2^2 + 2m_2) + 1$ so that the remainder of the division of n by 4 is 1.
• If the remainder of the division of k by 4 is 2 then $k = 4m_3 + 2$ and $n = 4(4m_3^2 + 4m_3 + 1)$ so that the remainder of the division of n by 4 is 0.
• If the remainder of the division of k by 4 is 3 then $k = 4m_4 + 3$ and $n = 4(4m_4^2 + 6m_4 + 2) + 1$ so that the remainder of the division of n by 4 is 1 ■

Review Problems

Problem 8.1
Use the proof by contradiction to prove the proposition "There is no greatest even integer."

Problem 8.2
Prove by contradiction that the difference of any rational number and any irrational number is irrational.

Problem 8.3
Use the proof by contraposition to show that if a product of two positive real numbers is greater than 100, then at least one of the numbers is greater than 10.

Problem 8.4
Use the proof by contradiction to show that the product of any nonzero rational number and any irrational number is irrational.

Problem 8.5
Show that if n is an integer and n^2 is divisible by 3 then n is also divisible by 3.

Problem 8.6
Show that the number $\sqrt{3}$ is irrational.

Problem 8.7
Use the proof by contrapositive to show that if n and m are two integers for which $n + m$ is even then either both n and m are even or both are odd.

Problem 8.8
Use the proof by contrapositive to show that for any integer n, if $3n + 1$ is even then n is odd.

Problem 8.9
Use the proof by contradiction to show that there are no positive integers n and m such that $n^2 - m^2 = 2$.

Problem 8.10
Use the proof by contradiction to show that for any integers n and m, we have $n^2 - 4m \neq 2$.

Problem 8.11
Prove by contrapositive: If n is a positive integer such that the remainder of the division of n by 3 is 2 then n is not a perfect square.

Problem 8.12
Prove by contrapositive: Suppose that $a, b \in \mathbb{Z}$. If $a \cdot b$ is not divisible by 5 then both a and b are not divisible by 5.

Problem 8.13
Prove by contradiction: Suppose that $n \in \mathbb{Z}$. If $n^3 + 5$ is odd then n is even.

Problem 8.14
Prove by contradiction: There exist no integers a and b such that $18a+6b = 1$.

Problem 8.15
Prove by contrapositive: If a and b are two integers such that $a \cdot b$ is not divisible by n then a and b are not divisible by n.

Problem 8.16
Prove by contradiction: Suppose that a, b, and c are positive real numbers. Show that if $ab = c$ then $a \leq \sqrt{c}$ or $b \leq \sqrt{c}$.

Problem 8.17
Prove by contrapositive: Let $n \in \mathbb{Z}$. If $n^2 - 6n + 5$ is even then n is odd.

Problem 8.18
Prove by contradiction: There is no largest even integer.

Problem 8.19
Prove by contrapositive: Let $a, b \in \mathbb{Z}$. If $a + b \geq 15$ then $a \geq 8$ or $b \geq 8$.

Problem 8.20
Prove by contradiction: Let $a \in \mathbb{Z}$. If p is a prime number that divides a then p does not divide $a + 1$.

9 Method of Proof by Induction

With the emphasis on structured programming has come the development of an area called **program verification,** which means your program is correct as you are writing it.
One technique essential to program verification is **mathematical induction**, a method of proof that has been useful in every area of mathematics as well.
Consider an arbitrary loop in Pascal starting with the statement

$$FOR\ I\ := 1\ TO\ N\ DO$$

If you want to verify that the loop does something regardless of the particular integral value of N, you need mathematical induction.
Also, sums of the form

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

are very useful in analysis of algorithms and a proof of this formula is mathematical induction.
Next we examine this method. We want to prove that a predicate $P(n)$ is true for any nonnegative integer $n \geq n_0$. The steps of mathematical induction are as follows:
(i) (Basis of induction) Show that $P(n_0)$ is true.
(ii) (Induction hypothesis) Assume $P(k)$ is true for $n_0 \leq k \leq n$.
(iii) (Induction step) Show that $P(n+1)$ is true.

Example 9.1
Use the technique of mathematical induction to show that

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}, \quad n \geq 1.$$

Solution.
Let $P(n) : 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. Then
(i) (Basis of induction) $P(1) : 1 = \frac{1(1+1)}{2}$. That is, $P(1)$is true.
(ii) (Induction hypothesis) Assume $P(k)$ is true for $1 \leq k \leq n$.
(iii) (Induction step) We must show that $P(n+1) : 1+2+3+\cdots+n+1 =$

$\frac{(n+1)(n+2)}{2}$. Indeed,

$$\begin{aligned}1+2+\cdots+n+(n+1) =&(1+2+\cdots+n)+n+1\\ =&\frac{n(n+1)}{2}+(n+1)\\ =&\frac{(n+1)(n+2)}{2}\ \blacksquare\end{aligned}$$

Example 9.2 *(Geometric progression)*
(a) Use induction to show $P(n):\sum_{i=0}^{n} ar^i = \frac{a(1-r^{n+1})}{1-r},\ n\geq 0$ where $r\neq 1$.
(b) Show that $1+\frac{1}{2}+\cdots+\frac{1}{2^{n-1}}\leq 2$, for all $n\geq 1$.

Solution.
(a) We use the method of proof by mathematical induction.
(i) (Basis of induction) $a = a\frac{1-r^{0+1}}{1-r} = \sum_{k=0}^{0} ar^k$. That is, $P(0)$is true.
(ii) (Induction hypothesis) Assume $P(k)$ is true for $0\leq k\leq n$.
(iii) (Induction step) We must show that $P(n+1)$ is true. That is, $\sum_{k=0}^{n+1} ar^k = \frac{a(1-r^{n+2})}{1-r}$. Indeed,

$$\begin{aligned}\sum_{i=0}^{n+1} ar^i =&\sum_{i=0}^{n} ar^i + ar^{n+1}\\ =&a\frac{1-r^{n+1}}{1-r}+ar^{n+1}\frac{1-r}{1-r}\\ =&a\frac{1-r^{n+1}+r^{n+1}-r^{n+2}}{1-r}\\ =&a\frac{1-r^{n+2}}{1-r}.\end{aligned}$$

(b) By (a) we have

$$\begin{aligned}1+\frac{1}{2}+\frac{1}{2^2}+\cdots+\frac{1}{2^{n-1}} =&\frac{1-(\frac{1}{2})^n}{1-\frac{1}{2}}\\ =&2(1-(\frac{1}{2})^n)\\ =&2-\frac{1}{2^{n-1}}\\ \leq&2\ \blacksquare\end{aligned}$$

Example 9.3 *(Arithmetic progression)*
Use induction to show that $P(n) : \sum_{i=1}^{n}(a+(i-1)r) = \frac{n}{2}[2a+(n-1)r],\ n \geq 1$.

Solution.
We use the method of proof by mathematical induction.
(i) (Basis of induction) $a = \frac{1}{2}[2a + (1-1)r] = \sum_{i=1}^{1}(a + (i-1)r)$. That is, $P(1)$is true.
(ii) (Induction hypothesis) Assume $P(k)$ is true for $1 \leq k \leq n$.
(iii) (Induction step) We must show that $P(n+1)$ is true. That is, $\sum_{i=1}^{n+1}(a + (i-1)r) = \frac{(n+1)}{2}[2a + nr]$. Indeed,

$$\begin{aligned}\sum_{i=1}^{n+1}(a + (i-1)r) =& \sum_{i=1}^{n}(a + (i-1)r) + a + (n+1-1)r \\ =& \frac{n}{2}[2a + (n-1)r] + a + nr \\ =& \frac{2an + n^2r - nr + 2a + 2nr}{2} \\ =& \frac{2a(n+1) + n(n+1)r}{2} \\ =& \frac{n+1}{2}[2a + nr] \ \blacksquare\end{aligned}$$

Example 9.4
(a) Use induction to prove that $n < 2^n$ for all non-negative integers n.
(b) Use induction to prove that $2^n < n!$ for all non-negative integers $n \geq 4$.

Solution.
(a) Let $P(n) : n < 2^n$. We want to show that $P(n)$ is valid for all $n \geq 0$. We use the method of mathematical induction.
(i) (Basis of induction) We have $0 < 2^0 = 1$. Thus, $P(0)$is true.
(ii) (Induction hypothesis) Assume $P(k)$ is true for $0 \leq k \leq n$.
(iii) (Induction step) We must show that $P(n+1)$ is also true. That is, $n + 1 < 2^{n+1}$. Indeed,

$$\begin{aligned}n + 1 <& 2^n + 1 \\ \leq& 2^n + n \\ <& 2^n + 2^n \\ =& 2 \cdot 2^n = 2^{n+1}\end{aligned}$$

where we used the fact that $n < 2^n$ twice.
(b) Let $P(n) : 2^n < n!$. We want to show that $P(n)$ is valid for all $n \geq 4$. By the method of mathematical induction we have
(i) (Basis of induction) $16 = 2^4 < 24 = 4!$. That is, $P(4)$is true.
(ii) (Induction hypothesis) Assume $P(k)$ is true for $4 \leq k \leq n$.
(iii) (Induction step) We must show that $P(n+1)$ is true. That is, $2^{n+1} < (n+1)!$. Indeed,

$$\begin{aligned} 2^{n+1} =& 2^n + 2^n \\ <& 2n! \\ <& (n+1)n! = (n+1)! \end{aligned}$$

where we have used the fact that if $n + 1 \geq 5 > 2$ ■

Example 9.5 *(Bernoulli's inequality)*
Let $h > -1$. Use induction to show that

$$(1 + nh) \leq (1 + h)^n, \quad n \geq 0.$$

Solution.
Let $P(n) : (1 + nh) \leq (1 + h)^n$. We want to show that $P(n)$ is valid for all nonnegative integers.
(i) (Basis of induction) $1 + 0h = 1 \leq 1 = (1 + h)^0$. That is, $P(0)$is true.
(ii) (Induction hypothesis) Assume $P(k)$ is true for $0 \leq k \leq n$.
(iii) (Induction step) We must show that $P(n+1)$ is true. That is, $(1 + (n + 1)h) \leq (1 + h)^{n+1}$. Indeed,

$$\begin{aligned} (1 + nh) \leq& (1 + h)^n \\ (1 + h)(1 + nh) \leq& (1 + h)^{n+1} \\ 1 + (n + 1)h + nh^2 \leq& (1 + h)^{n+1}. \end{aligned}$$

But $nh^2 \geq 0$ so that $1 + (n + 1)h \leq 1 + (n + 1)h + nh^2 \leq (1 + h)^{n+1}$ ■

Review Problems

Problem 9.1
Use the method of induction to show that

$$2 + 4 + 6 + \cdots + 2n = n^2 + n$$

for all integers $n \geq 1$.

Problem 9.2
Use mathematical induction to prove that

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$$

for all integers $n \geq 0$.

Problem 9.3
Use mathematical induction to show that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

for all integers $n \geq 1$.

Problem 9.4
Use mathematical induction to show that

$$1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$$

for all integers $n \geq 1$.

Problem 9.5
Use mathematical induction to show that

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

for all integers $n \geq 1$.

Problem 9.6
Use the formula

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

to find the value of the sum

$$3 + 4 + \cdots + 1,000.$$

Problem 9.7
Find the value of the geometric sum

$$1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^n}.$$

Problem 9.8
Let $S(n) = \sum_{k=1}^{n} \frac{k}{(k+1)!}$. Evaluate $S(1), S(2), S(3), S(4)$, and $S(5)$. Make a conjecture about a formula for this sum for general n, and prove your conjecture by mathematical induction.

Problem 9.9
For each positive integer n let $P(n)$ be the proposition $4^n - 1$ is divisible by 3.
(a) Write $P(1)$. Is $P(1)$ true?
(b) Write $P(k)$.
(c) Write $P(k+1)$.
(d) In a proof by mathematical induction that this divisibility property holds for all integers $n \geq 1$, what must be shown in the induction step?

Problem 9.10
For each positive integer n let $P(n)$ be the proposition $2^{3n} - 1$ is divisible by 7. Prove this property by mathematical induction.

Problem 9.11
Show that $2^n < (n+2)!$ for all integers $n \geq 0$.

Problem 9.12
(a) Use mathematical induction to show that $n^3 > 2n + 1$ for all integers $n \geq 2$.
(b) Use mathematical induction to show that $n! > n^2$ for all integers $n \geq 4$.

Problem 9.13
A sequence $a_1, a_2, \cdots$ is defined recursively by $a_1 = 3$ and $a_n = 7a_{n-1}$ for $n \geq 2$. Show that $a_n = 3 \cdot 7^{n-1}$ for all integers $n \geq 1$.

Problem 9.14
Show by using mathematical induction: For all integers $n \geq 1$, $2^{2n} - 1$ is divisible by 3.

Problem 9.15
Define the following sequence of numbers: $a_1 = 2$ and for $n \geq 2$, $a_n = 5a_{n-1}$. Find a formula for a_n and then prove its validity by mathematical induction.

Problem 9.16
Prove by mathematical induction that $n^3 + 5n$ is divisible by 6 for all positive integer n.

Problem 9.17
Use mathematical induction to show that the sum of the first n odd positive integers is equal to n^2.

Problem 9.18
Use mathematical induction to show that $23^n - 1$ is divisible by 11 for all positive integer n.

Problem 9.19
Define the following sequence of numbers: $a_1 = 1$, $a_2 = 8$ and for $n \geq 3$, $a_n = a_{n-1} + 2a_{n-2}$. Use induction to show that $a_n = 3 \cdot 2^{n-1} + 2(-1)^n$ for all positive integers n.

Problem 9.20
Consider the sequence of real numbers defined by the relations $a_1 = 1$ and $a_{n+1} = \sqrt{1 + 2a_n}$ for all $n \geq 1$. Use mathematical induction to show that $a_n < 4$ for all $n \geq 1$.

Number Theory and Mathematical Proofs

In this chapter, we look at the applications of mathematical proofs to number theory.

10 Divisibility. The Division Algorithm

In this section we study the divisibility of integers. Our main goal is to obtain the **Division Algorithm**. This is achieved by applying the well-ordering principle which we prove next.

Theorem 10.1 *(The Well-Ordering Principle)*
If S is a nonempty subset of $\mathbb{N}$ then there is $m \in S$ such that $m \leq x$ for all $x \in S$. That is, S has a smallest or least element.

Proof.
We will use contraposition to prove the theorem. That is, by assuming that S has no smallest element we will prove that $S = \emptyset$.
We will prove that $n \notin S$ for all $n \in \mathbb{N}$. We do this by induction on n. Since S has no smallest element, we have $1 \notin S$. Asuume that we have proved that $1, 2, \cdots, n \notin S$. We will show that $n + 1 \notin S$. If $n + 1 \in S$ then $n + 1$ would be the smallest element of S since $1, 2, 3, \cdots, n \notin S$, and this contradicts the assumption that S has no smallest element. Thus, we must have $n + 1 \notin S$. Hence, by the principle of mathematical induction, $n \notin S$ for all $n \in \mathbb{N}$. But this leads to $S = \emptyset$. This establishes a proof of the theorem ■

Remark 10.1
The above theorem is false if $\mathbb{N}$ is replaced by $\mathbb{Z}, \mathbb{Q}$, or $\mathbb{R}$. For example, the set of even integers is nonempty subset of $\mathbb{Z}$ with no smallest element.

Example 10.1
Prove that there is no positive integer between 0 and 1.

Solution.
Suppose the contrary. Let $n \in \mathbb{N}$ such that $0 < n < 1$. Define the set $S = \{a \in \mathbb{N} : 0 < a < 1\}$. Since $n \in S$, S is non-empty. By Theorem 10.1, S has a smallest element b where $b \in \mathbb{N}$ and $0 < b < 1$. Multiply this last inequality by b to obtain $0 < b^2 < b < 1$. But then $b^2 \in S$ and $b^2 < b$ which contradicts the fact that b is the smallest element of S. By the method of proof by contradiction, we conclude that there is no positive integer between 0 and 1 ■

With the Well-Ordering Principle we can establish the following theorem.

Theorem 10.2 *(Division Algorithm)*
If a and b are integers with $b \geq 1$ then there exist unique integers q and r such that

$$a = bq + r, \quad 0 \leq r < b.$$

Proof.
The proof consists of two parts: existence and uniqueness.

Existence
Consider the sets

$$S = \{a - bt : t \in \mathbb{Z}\}, \qquad S' = \{x \in S : x \geq 0\}.$$

The set S' is nonempty. To see this, if $a \geq 0$ then $a - 0t \in S$ and $a - 0t \geq 0$. That is, $a \in S'$. If $a < 0$ then since $a - ba \in S$ and $a - ba = a(1 - b) \geq 0$ so that $a - ba \in S'$.
Now, if $0 \in S'$ then $a - qb = 0$ for some $q \in \mathbb{Z}$ and so $r = 0$ and in this case the theorem holds. So, assume that $0 \notin S'$. By Theorem 10.1, there exists a smallest element $r \in S'$. That is,

$$a - qb = r, \quad \text{for some } q \in \mathbb{Z}.$$

Since $r \in S'$, we have $r > 0$ since $0 \notin S'$. It remains to show that $r < b$. If we assume the contrary, i.e., $r \geq b$, then

$$a - b(q + 1) = a - bq - b = r - b \geq 0$$

and this implies that $a - b(q + 1) \in S'$. But $b \geq 1 > 0$ so that

$$a - b(q + 1) = a - bq - b < a - bq = r$$

and this contradicts the definition of r as being the smallest element of S'. Thus, for the given a and b we can find integers q and r such that

$$a = bq + r, \quad 0 \leq r < b.$$

Uniqueness
Suppose that

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b$$

and

$$a = bq_2 + r_2, \quad 0 \leq r_2 < b.$$

We must show that $r_1 = r_2$ and $q_1 = q_2$. Indeed, $bq_1 + r_1 = bq_2 + r_2$ implies $b(q_1 - q_2) = r_2 - r_1$. This says that $b|(r_2 - r_1)$. But $0 \leq r_1 < b$ and $0 \leq r_2 < b$ so that $-b < -r_1 < r_2 - r_1 < r_2 < b$. That is, $-b < r_2 - r_1 < b$. Hence, $-b < b(q_2 - q_1) < b$ which by dividing through by b we find $-1 < q_2 - q_1 < 1$. Now, $q_2 - q_1$ is an integer strictly between -1 and 1. Thus, $q_2 - q_1 = 0$ or $q_1 = q_2$. But then $r_2 - r_1 = b(q_1 - q_2) = 0$ and this implies $r_1 = r_2$ ■

Example 10.2
Find q and r when $a = 11$ and $b = 4$.

Solution
By long division of numbers, we find $q = 2$ and $r = 3$ ■

Next, we introduce the concept of divisibility and derive some of its properties.
An integer m is **divisible** by a nonzero integer n if and only if $m = nq$ for some integer q. We also say that n **divides** m, n is a **divisor** of m, m is a **multiple** of n, or n is a **factor** of m. We write $n|m$. If n does not divide m we write $n \nmid m$. For example, $2|\ 8$ and $4|\ 8$. However, $4 \nmid 6$.

The following theorem discusses some of the properties of divisibility.

Theorem 10.3
(a) If $n|m$ then $n|(-m)$.
(b) If $n|a$ and $n|b$ then $n|(a \pm b)$
(c) If $n|m$ and $m|p$ then $n|p$.
(d) If $n|m$ and $m|n$ then either $n = m$ or $n = -m$.

A positive integer $n > 1$ with only divisors 1 and n is called **prime.** An integer greater than 1 that is not prime is called **composite**. That is, a composite number is a positive integer that has at least one positive divisor other than one or the number itself. For example, 2 is the first prime number whereas 4 is first composite number.

If a positive number p is composite then one can always write p as the product of primes, where the prime factors are written in increasing order. This result is known as the **Fundamental Theorem of Arithmetic** or **the Unique Factorization Theorem**.

Theorem 10.4
Every positive integer $n > 1$ is either a prime or can be written as a product of prime integers, and this product is unique except for the order of the factors.

Example 10.3
Write the prime factorization of 180.

Solution.
The prime factorization is $180 = 2^2 \times 3^2 \times 5$ ■

The following important theorem shows that if a number is not divisible by any prime less than or equal to its square root then the number must be prime.

Theorem 10.5
If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Proof.
Since n is composite, there is a divisor a of n such that $1 < a < n$. Write $n = ab$ where b is a positive integer. Note that b is also a divisor of n. If $a > \sqrt{n}$ and $b > \sqrt{n}$ then $n = ab > \sqrt{n}\sqrt{n} = n$, a false conclusion. Thus, either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Hence, n has a positive divisor which is less than or equal to $\sqrt{n}$. If the divisor, say a, is a prime then we are done. If a is not a prime then by the Fundamental Theorem of Arithmetic there is a prime number p that divides a.That is, $a = pk$. But then $n = pqb$ so that p divides n and $p < a \leq \sqrt{n}$. In either case, n has a prime divisor less than or equal to $\sqrt{n}$ ■

Example 10.4
Use the previous theorem to show that the number 101 is prime.

Solution.
The prime numbers less than or equal to $\sqrt{101}$ are: $2, 3, 5, 7$. Since none of them divides 101, by the previous theorem, 101 is prime ■

Let a and b be two integers, not both zero. The largest positive integer d that divides both a and b is called the **greatest common divisor** of a

and b. We write $d = (a, b)$ or $d = gcd(a, b)$. If $gcd(a, b) = 1$ then we say that a and b are **relatively prime**. For example, the numbers 2 and 3 are relatively prime.

Example 10.5
Find the greatest common divisor of 42 and 56.

Solution.
Since

$$D_{42} = \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42\}$$

and

$$D_{56} = \{\pm 1, \pm 2, \pm 4, \pm 7, \pm 8, \pm 14, \pm 28, \pm 56\},$$

we have $gcd(42, 56) = 14$ ■

Example 10.6
Find the greatest common divisor of 15 and 28.

Solution.
Since

$$D_{15} = \{\pm 1, \pm 3, \pm 5, \pm 15\}$$

and

$$D_{28} = \{\pm 1, \pm 2, \pm 4, \pm 7, \pm 14, \pm 28\},$$

we have $gcd(15, 28) = 1$ so that 15 and 28 are relatively prime ■

The greatest common divisor is useful for writing fractions in lowest term. For example, $-\frac{42}{56} = -\frac{3}{4}$ where we cancelled $14 = gcd(42, 56)$.

Remark 10.2
In the next section we will establish the existence and uniqueness of the greatest common divisor and provide an algorithm of how to find it.

Review Problems

Problem 10.1
Show that the set of all positive real numbers does not have a least element.

Problem 10.2
Use the well-ordering principle to show that every positive integer $n \geq 8$ can be written as sums of 3's and 5's.

Problem 10.3
Let a and b be positive integers such that $\frac{a}{b} = \sqrt{2}$. Let $S = \{n \in \mathbb{N} : \sqrt{2}n \in \mathbb{N}\}$. Show that S is the empty set. Hence, concluding that $\sqrt{2}$ is irrational.

Problem 10.4
Let n and m be integers such that $n|m$ where $n \neq 0$. Show that $n|(-m)$.

Problem 10.5
Let n, a and b be integers such that $n|a$ and $n|b$ where $n \neq 0$. Show that $n|(a \pm b)$.

Problem 10.6
Let n, m and p be integers such that $n|m$ and $m|p$ where $n, m \neq 0$. Show that $n|p$.

Problem 10.7
Let n and m be integers such that $n|m$ and $m|n$ where $n, m \neq 0$. Show that either $n = m$ or $n = -m$.

Problem 10.8
Write the first 7 prime numbers.

Problem 10.9
Show that 227 is a prime number.

Problem 10.10
Write the prime factorization of 42 and 105.

Problem 10.11
Find the greatest common divisor of 42 and 105.

Problem 10.12
Are the numbers 27 and 35 relatively prime?

Problem 10.13
We say that an integer n is **even** if and only if there exists an integer k such that $n = 2k$. An integer n is said to be **odd** if and only if there exists an integer k such that $n = 2k + 1$.
Let m and n be two integers.
(a) Is $6m + 8n$ an even integer?
(b) Is $6m + 4n^2 + 3$ odd?

Problem 10.14
Let a, b, and c be integers such that $a|b$ where $a \neq 0$. Show that $a|(bc)$.

Problem 10.15
Let m and n be positive integers with $m > n$. Is $m^2 - n^2$ composite?

Problem 10.16
Show that if $a|b$ and $a|c$ then $a|(mb + nc)$ for all integers m and n.

Problem 10.17
If two integers a and b have the property that their difference $a-b$ is divisible by an integer n, i.e., $a - b = nq$ for some integer q, we say that a and b are **congruent modulo** n. Symbolically, we write $a \equiv b(mod\ n)$. Show that if $a \equiv b(mod\ n)$ and $c \equiv d(mod\ n)$ then $a + c \equiv (b + d)(mod\ n)$.

Problem 10.18
Show that if $a \equiv b(mod\ n)$ and $c \equiv d(mod\ n)$ then $ac \equiv bd(mod\ n)$.

Problem 10.19
Show that if $a \equiv a(mod\ n)$ for all integer a.

Problem 10.20
Show that if $a \equiv b(mod\ n)$ then $b \equiv a(mod\ n)$.

Problem 10.21
Show that if $a \equiv b(mod\ n)$ and $b \equiv c(mod\ n)$ then $a \equiv c(mod\ n)$.

Problem 10.22
What are the solutions of the linear congruences $3x \equiv 4(mod\ 7)$?

Problem 10.23
Solve $2x + 11 \equiv 7(mod\ 3)$?

11 The Euclidean Algorithm

In this section, we discuss the question of existence of the gcd of two integers, in which one the integers is non-zero, and develop a systematic procedure for finding it, known as the **Euclid's Algorithm.**. For that purpose, we need the following result.

Theorem 11.1
If a, b, q, and r are integers such that $a = bq + r$ then $gcd(a, b) = gcd(b, r)$.

Proof.
Let $d_1 = gcd(a, b)$ and $d_2 = gcd(b, r)$. We will show that $d_1 = d_2$. Since $d_2|bq$ and $d_2|r$, we have $d_2|(bq + r)$ (Problem 10.5). Hence, $d_2|a$. Thus, by the definition of gcd, we have $d_2 \leq d_1$. Now, since $d_1|b$, we have $d_1|bq$ (Problem 10.7). Since $d_1|a$, we have $d_1|(a - bq)$ (Problem 10.5). Hence, $d_1|r$. From the definition of d_2, we have $d_1 \leq d_2$. Thus, $d_1 \leq d_2$ and $d_2 \leq d_1$. We conclude $d_1 = d_2$ ■

Example 11.1
Find $gcd(998, 996)$ using Theorem 11.1.

Solution.
Using Theorem 11.1, we have that $gcd(bq + r, b) = gcd(r, b)$ for any integer q. Thus, $gcd(998, 996) = gcd(998 - 996, 996) = gcd(2, 996)$. Since $gcd(2, 996)|2$, $gcd(2, 996) - 1$ or $gcd(2, 996) = 2$. Since $2|996$, we conclude that $gcd(998, 996) = 2$ ■

The following theorem, establishes the existence and uniqueness of the greatest common divisor and provides an algorithm of how to find it.

Theorem 11.2 *(The Euclidean Algorithm)*
If a and b are two integers with $b > 0$, then there exists a unique largest positive integer d that divide both numbers.

Proof.
Uniqueness: Suppose that d_1 and d_2 are two greatest common divisors of a and b. In this case, we can write $d_1 \leq d_2$ and $d_2 \leq d_1$. Hence, $d_1 = d_2$.
Existence: If $a = 0$ then $d = b$. So assume that $a \neq 0$. By the Division Algorithm (Theorem 10.2) there exist unique integers q_1 and r_1 such that

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b.$$

If $r_1 = 0$ then $d = b$. So assume $r_1 > 0$. Using the Division Algorithm for a second time to find unique integers q_2 and r_2 such that

$$b = r_1 q_2 + r_2 \quad 0 \leq r_2 < r_1.$$

If $r_2 = 0$ then by Theorem 11.1, $r_1 = gcd(b, r_1) = gcd(a, b)$. If $r_2 > 0$, we find integers q_3 and r_3 such that

$$r_1 = r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2.$$

If $r_3 = 0$, then $r_2 = gcd(r_1, r_2) = gcd(b, r_1) = gcd(a, b)$. We keep this process going and eventually we will find integers r_{n-2}, r_{n-1} and r_n such that

$$r_{n-2} = r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1}$$

and

$$r_{n-1} = r_n q_{n+1}$$

with $r_n = gcd(r_n, r_{n-1}) = gcd(r_{n-1}, r_{n-2}) = \cdots = gcd(a, b)$. Note that r_n is the last nonzero remainder in the process ■

Example 11.2
Find gcd(1776,1492).

Solution.
Performing the arithmetic for the Euclidean algorithm we have

$$\begin{aligned} 1776 &= (1)(1492) + 284 \\ 1492 &= (5)(284) + 72 \\ 284 &= (3)(72) + 68 \\ 72 &= (1)(68) + 4 \\ 68 &= 4(17). \end{aligned}$$

So $gcd(1776, 1492) = 4$ ■

Theorem 11.3 *(Bezout)*
If a and b are two integers with $b > 0$, then there exist integers m and n such that $gcd(a, b) = ma + nb$.

Proof.
From the proof of Theorem 11.2, we have

$$\begin{aligned} gcd(a,b) = r_n =& r_{n-2} - r_{n-1}q_n \\ =& m_1 r_{n-1} + n_1 r_{n-2} \\ =& m_1(r_{n-3} - r_{n-2}q_{n-1}) + n_1 r_{n-2} \\ =& m_2 r_{n-2} + n_2 r_{n-3} \\ =& m_2(r_{n-4} - r_{n-3}q_{n-2}) + n_2 r_{n-3} \\ =& m_3 r_{n-3} + n_3 r_{n-4} \\ & \vdots \\ =& m r_1 + n' b \\ =& m(a - bq_1) + n' b \\ =& ma + nb \ \blacksquare \end{aligned}$$

Review Problems

Problem 11.1
(i) Find $gcd(120, 500)$.
(ii) Show that 17 and 22 are relatively prime.

Problem 11.2
Use the Euclidean algorithm to find $gcd(414, 662)$.

Problem 11.3
Use the Euclidean algorithm to find $gcd(287, 91)$.

Problem 11.4
Use the Euclidean algorithm to find $gcd(-24, 25)$.

Problem 11.5
Use the Euclidean algorithm to find $gcd(-6, -15)$.

Problem 11.6
Prove that if $n \in Z$, then $gcd(3n + 4, n + 1) = 1$.

Problem 11.7
Show that $gcd(a, b) = gcd(|a|, |b|)$.

Problem 11.8
Show that if $d = gcd(a, b)$ then $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime.

Problem 11.9
Show that if $a|bc$ and $gcd(a, b) = 1$ then $a|c$.

Problem 11.10
Show that if $a|c$ and $b|c$ and $gcd(a, b) = 1$ then $ab|c$.

Problem 11.11
Show that if $gcd(a, c) = 1$ and $gcd(b, c) = 1$ then $gcd(ab, c) = 1$.

Problem 11.12
Show that there are integers m and n such that $121m + 38n = 1$.

Problem 11.13
Find integers m and n such that $121m + 38n = 1$.

Problem 11.14
Show that $gcd(ma, na) = a \cdot gcd(m, n)$, where a is a positive integer.

Problem 11.15
Show that $gcd(a, bc)|gcd(a, b)gcd(a, c)$.

Problem 11.16
Give an example where $ma + nb = d$ but $d \neq gcd(a, b)$.

Problem 11.17
Let p be a prime number. Find $gcd(a, p)$ where $a \in \mathbb{Z}$.

Problem 11.18
Show that if $gcd(a, b) = 1$ then $xa \equiv 1 (\text{mod } b)$ has a solution.

Problem 11.19
Show that if $ma + nb = d$ then d is a multiple of $gcd(a, b)$.

Problem 11.20
Let p be a prime number such that $p|ab$. Show that $p|a$ or $p|b$.

Fundamentals of Set Theory

Set is the most basic term in mathematics and computer science. Hardly any discussion in either subject can proceed without **set** or some synonym such as **class** or **collection**. In this chapter we introduce the concept of sets and its various operations and then study the properties of these operations.

12 Basic Definitions

We first consider an example of a **paradox** known as the **barber paradox**: "Terry is a barber in an army captain who was ordered to shave all members of the company who do not shave themselves. Does the barber shave himself? If he shaves himself then being the barber of the company he disobeyed the captain's order. If he does not shave himself, then by the captain's order he is supposed to shave himself." Obviously, to resolve the above paradox one has to take the barber out of the company.

Naive set theory defines a set to be any definable collection. Such a definition leads to the following paradox:

Russell's Paradox. Consider the set $A = \{X : X \text{ is a set}, X \notin X\}$. Since A is itself a set, either $A \in A$ or $A \notin A$. Saying that $A \in A$ will imply that $A \notin A$ by the definition of A. Saying that $A \notin A$ means that $A \in A$ by the definition of A. Thus, in either case the assumption that A is a set leads to the paradox: $A \in A$ and $A \notin A$.

Such a paradox indicated the necessity of a formal **axiomatization** of set theory.

We define a **set** A as a collection of well-defined objects (called **elements** or **members** of A) such that for any given object x either one (but not both) of the following holds:

- x belongs to A and we write $x \in A$.
- x does not belong to A, and in this case we write $x \notin A$.

With this definition, the A in Russell's paradox is not a set.

We denote sets by capital letters $A, B, C, \cdots$ and elements by lowercase letters $a, b, c, \cdots$ Sets consisting of sets will be denoted by script letters.

There are different ways to represent a set. The first one is to list, without repetition, the elements of the set. We say that the set is given in **tabular form**. Another way is to describe a property characterizing the members of the set. Such a representation is referred to as the **descriptive form** of a set. The third way is to write in symbolic form the common characteristic shared by all the elements of the set such as

$$A = \{x \in \mathbb{Z} | x^2 - 4 = 0\}.$$

We refer to such a form as the **set-builder form**.

We define the **empty set**, denoted by $\emptyset$, to be the set with no elements.

Example 12.1
In what form are the following sets are defined?
(a) A is the vowel of the English alphabet.
(b) $A = \{1, 2, 3\}$.
(c) $A = \{x \in \mathbb{R} | x^2 - 1 = 0\}$.

Solution.
(a) Descriptive form.
(b) Tabular form.
(c) Set-builder form ■

Example 12.2
List the elements of the following sets:
(a) $\{x \in \mathbb{R} | x^2 = 1\}$.
(b) $\{x \in \mathbb{Z} | x^2 - 3 = 0\}$.

Solution.
(a) $\{-1, 1\}$.
(b) $\emptyset$ ■

Example 12.3
Write the set-builder form of each of the following sets.
(a) $\{a, e, i, o, u\}$.
(b) $\{1, 3, 5, 7, 9\}$.

Solution.
(a) $\{x$ is a letter of the English alphabet$|x$ *is a vowel*$\}$.
(b) $\{n \in \mathbb{N} | n$is odd and less than 10$\}$ ■

Let A and B be two sets. We say that A is a **subset** of B, denoted by $A \subseteq B$, if and only if every element of A is also an element of B. Symbolically:

$$[A \subseteq B] \Leftrightarrow [x \in A \Longrightarrow x \in B].$$

If there exists an element of A which is not in B then we write $A \nsubseteq B$.
Now, for any set A, the proposition $x \in \emptyset \Longrightarrow x \in A$ is vacuously true since $x \in \emptyset$ is always false. Hence $\emptyset \subseteq A$.

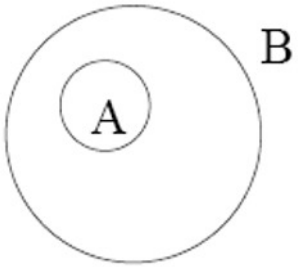
Example 12.4
Suppose that $A = \{2, 4, 6\}$, $B = \{2, 6\}$, and $C = \{4, 6\}$. Determine which of these sets are subsets of which other(s) of these sets.

Solution.
$B \subseteq A$ and $C \subseteq A$ ■

If sets A and B are represented as regions in the plane, relationships between A and B can be represented by pictures, called **Venn diagrams.**

Example 12.5
Represent $A \subseteq B$ using a Venn diagram.

Solution.



■

Two sets A and B are said to be **equal** if and only if $A \subseteq B$ and $B \subseteq A$. We write $A = B$. Thus, to show that $A = B$ it suffices to show the double inclusions mentioned in the definition. For non-equal sets we write $A \neq B$.

Example 12.6
Determine whether each of the following pairs of sets are equal.
(a) $\{1, 3, 5\}$ and $\{5, 3, 1\}$.
(b) $\{\{1\}\}$ and $\{1, \{1\}\}$.

Solution.
(a) $\{1, 3, 5\} = \{5, 3, 1\}$.
(b) $\{\{1\}\} \neq \{1, \{1\}\}$ since $1 \notin \{\{1\}\}$ ■

Let A and B be two sets. We say that A is a **proper subset** of B, denoted by $A \subset B$, if $A \subseteq B$ and $A \neq B$. Thus, to show that A is a proper subset of B we must show that every element of A is an element of B and there is an element of B which is not in A.

Example 12.7
Order the sets of numbers: $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{N}$ using $\subset$

Solution.
$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ ■

Example 12.8
Determine whether each of the following statements is true or false.
(a) $x \in \{x\}$ (b) $\{x\} \subseteq \{x\}$ (c) $\{x\} \in \{x\}$
(d) $\{x\} \in \{\{x\}\}$ (e) $\emptyset \subseteq \{x\}$ (f) $\emptyset \in \{x\}$

Solution.
(a) True (b) True (c) False (d) True (e) True (f) False ■

If U is a given set whose subsets are under consideration, then we call U a **universal set.**
Let U be a universal set and A, B be two subsets of U. The **absolute complement** of A is the set

$$A^c = \{x \in U | x \notin A\}.$$

The **relative complement** of A with respect to B is the set

$$B \backslash A = \{x \in U | x \in B \; and \; x \notin A\}.$$

Example 12.9
Let $U = \mathbb{R}$. Consider the sets $A = \{x \in \mathbb{R} | x < -1 \; or \; x > 1\}$ and $B = \{x \in \mathbb{R} | x \leq 0\}$. Find
(a) A^c.
(b) $B \backslash A$.

Solution.
(a) $A^c = [-1, 1]$.
(b) $B \backslash A = [-1, 0]$ ■

Let A and B be two sets. The **union** of A and B is the set

$$A \cup B = \{x | x \in A \; or \; x \in B\}.$$

where the "or" is inclusive. This definition can be extended to more than two sets. More precisely, if $A_1, A_2, \cdots$, are sets then

$$\cup_{n=1}^{\infty} A_n = \{x | x \in A_i \; for \; some \; i\}.$$

Let A and B be two sets. The **intersection** of A and B is the set

$$A \cap B = \{x | x \in A \; and \; x \in B\}.$$

If $A \cap B = \emptyset$ we say that A and B are **disjoint sets**. Given the sets $A_1, A_2, \cdots$, we define

$$\cap_{n=1}^{\infty} A_n = \{x | x \in A_i \; for \; all \; i\}.$$

Example 12.10
Let $A = \{a, b, c\}, B = \{b, c, d\}$, and $C = \{b, c, e\}$.
(a) Find $A \cup (B \cap C), (A \cup B) \cap C$, and $(A \cup B) \cap (A \cup C)$. Which of these sets are equal?
(b) Find $A \cap (B \cup C), (A \cap B) \cup C$, and $(A \cap B) \cup (A \cap C)$. Which of these sets are equal?
(c) Find $A \backslash (B \backslash C)$ and $(A \backslash B) \backslash C$. Are these sets equal?

Solution.
(a) $A \cup (B \cap C) = A, (A \cup B) \cap C = \{b, c\}, (A \cup B) \cap (A \cup C) = \{b, c\} = (A \cup B) \cap C$.
(b) $A \cap (B \cup C) = \{b, c\}, (A \cap B) \cup C = C, (A \cap B) \cup (A \cap C) = \{b, c\} = A \cap (B \cup C)$.
(c) $A \backslash (B \backslash C) = A$ and $(A \backslash B) \backslash C = \{a\} \neq A \backslash (B \backslash C)$ ■

Example 12.11
For each $n \geq 1$, let $A_n = \{x \in \mathbb{R} : x < 1 + \frac{1}{n}\}$. Show that

$$\cap_{n=1}^{\infty} A_n = \{x \in \mathbb{R} : x \leq 1\}.$$

Solution.
The proof is by double inclusions method. Let $y \in \{x \in \mathbb{R} : x \leq 1\}$. Then for all positive integer n we have $y \leq 1 < 1 + \frac{1}{n}$. That is, $y \in \cap_{n=1}^{\infty} A_n$. This shows that $\{x \in \mathbb{R} : x \leq 1\} \subseteq \cap_{n=1}^{\infty} A_n$.
Conversely, let $y \in \cap_{n=1}^{\infty} A_n$. Then $y < 1 + \frac{1}{n}$ for all $n \geq 1$. Now take the limit of both sides as $n \to \infty$ to obtain $y \leq 1$. That is, $y \in \{x \in \mathbb{R} : x \leq 1\}$. This shows that $\cap_{n=1}^{\infty} A_n \subseteq \{x \in \mathbb{R} : x \leq 1\}$ ■

Example 12.12
The **symmetric difference** of A and B, denoted by $A \Delta B$, is the set containing those elements in either A or B but not both. Find $A \Delta B$ if $A = \{1, 3, 5\}$ and $B = \{1, 2, 3\}$.

Solution.
$A\Delta B = \{2, 5\}$ ■

The notation $(a_1, a_2, \cdots, a_n)$ is called an **ordered n-tuples**. We say that two $n-$tuples $(a_1, a_2, \cdots, a_n)$ and $(b_1, b_2, \cdots, b_n)$ are equal if and only if $a_1 = b_1, a_2 = b_2, \cdots, a_n = b_n$.
Given n sets $A_1, A_2, \cdots, A_n$ the **Cartesian product** of these sets is the set

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \cdots, a_n) | a_1 \in A_1, a_2 \in A_2, \cdots, a_n \in A_n\}$$

Example 12.13
Let $A = \{x, y\}, B = \{1, 2, 3\}$, and $C = \{a, b\}$. Find
(a) $A \times B \times C$.
(b) $(A \times B) \times C$.

Solution.
(a)

$$\begin{aligned} A \times B \times C = &\{(x,1,a),(x,2,a),(x,3,a),(y,1,a),(y,2,a),\\ &(y,3,a),(x,1,b),(x,2,b),(x,3,b),(y,1,b)\\ &(y,2,b),(y,3,b)\} \end{aligned}$$

(b)

$$\begin{aligned} (A \times B) \times C = &\{((x,1),a),((x,2),a),((x,3),a),((y,1),a),((y,2),a),\\ &((y,3),a),((x,1),b),((x,2),b),((x,3),b),((y,1),b)\\ &((y,2),b),((y,3),b)\} \blacksquare \end{aligned}$$

Review Problems

Problem 12.1
Write each the following sets in tabular form.
(a) $A = \{x \in N | x > 0\}$.
(b) A consists of the first five prime number.
(c) $A = \{x \in \mathbb{Z} | 2x^2 + x - 1 = 0\}$.

Problem 12.2
Write each the following sets in set-builder notation.
(a) $A = \{1, 2, 3, 4, 5\}$.
(b) $A = \{4, 6, 8, 9, 10\}$.

Problem 12.3
Which of the following sets are equal?
(a) $\{a, b, c, d\}$
(b) $\{d, e, a, c\}$
(c) $\{d, b, a, c\}$
(d) $\{a, a, d, e, c, e\}$

Problem 12.4
Let $A = \{c, d, f, g\}, B = \{f, j\}$, and $C = \{d, g\}$. Answer each of the following questions. Give reasons for your answers.
(a) Is $B \subseteq A$?
(b) Is $C \subseteq A$?
(c) Is $C \subseteq C$?
(d) Is C a proper subset of A?

Problem 12.5
(a) Is $3 \in \{1, 2, 3\}$?
(b) Is $1 \subseteq \{1\}$?
(c) Is $\{2\} \in \{1, 2\}$?
(d) Is $\{3\} \in \{1, \{2\}, \{3\}\}$?
(e) Is $1 \in \{1\}$?
(f) Is $\{2\} \subseteq \{1, \{2\}, \{3\}\}$?
(g) Is $\{1\} \subseteq \{1, 2\}$?
(h) Is $1 \in \{\{1\}, 2\}$?
(i) Is $\{1\} \subseteq \{1, \{2\}\}$?
(j) Is $\{1\} \subseteq \{1\}$?

Problem 12.6
Let $A = \{b, c, d, f, g\}$ and $B = \{a, b, c\}$. Find each of the following:
(a) $A \cup B$.
(b) $A \cap B$.
(c) $A \backslash B$.
(d) $B \backslash A$.

Problem 12.7
Indicate which of the following relationships are true and which are false:
(a) $\mathbb{Z}^+ \subseteq \mathbb{Q}$.
(b) $\mathbb{R}^- \subset \mathbb{Q}$.
(c) $\mathbb{Q} \subset \mathbb{Z}$.
(d) $\mathbb{Z}^+ \cup \mathbb{Z}^- = \mathbb{Z}$.
(e) $\mathbb{Q} \cap \mathbb{R} = \mathbb{Q}$.
(f) $\mathbb{Q} \cup \mathbb{Z} = \mathbb{Z}$.
(g) $\mathbb{Z}^+ \cap \mathbb{R} = \mathbb{Z}^+$
(h) $\mathbb{Z} \cup \mathbb{Q} = \mathbb{Q}$.

Problem 12.8
Let $A = \{x, y, z, w\}$ and $B = \{a, b\}$. List the elements of each of the following sets:
(a) $A \times B$
(b) $B \times A$
(c) $A \times A$
(d) $B \times B$.

Problem 12.9
(a) Find all possible subsets of the set $A = \{a, b, c\}$.
(b) How many proper subsets are there?

Problem 12.10
Subway prepared 60 4-inch sandwiches for a birthday party. Among these sandwiches, 45 of them had tomatoes, 30 had both tomatoes and onions, and 5 had neither tomatoes nor onions. Using a Venn diagram, how many sandwiches did he make with
(a) tomatoes or onions?
(b) onions?
(c) onions but not tomatoes?

Problem 12.11
A camp of international students has 110 students. Among these students,

75	speak english,
52	speak spanish,
50	speak french,
33	speak english and spanish,
30	speak english and french,
22	speak spanish and french,
13	speak all three languages.

How many students speak
(a) english and spanish, but not french,
(b) neither english, spanish, nor french,
(c) french, but neither english nor spanish,
(d) english, but not spanish,
(e) only one of the three languages,
(f) exactly two of the three languages.

Problem 12.12
Let A be the set of the first five composite numbers and B be the set of positive integers less than or equal to 8. Find $A\backslash B$ and $B\backslash A$.

Problem 12.13
Let U be a universal set. Find U^c and $\emptyset^c$.

Problem 12.14
Let A be the set of natural numbers less than 0 and $B = \{1, 3, 7\}$. Find $A \cup B$ and $A \cap B$.

Problem 12.15
Let

$$A = \{x \in \mathbb{N} | 4 \leq x \leq 8\}$$
$$B = \{x \in \mathbb{N} | x \text{ even and } x \leq 10\}.$$

Find $A \cup B$ and $A \cap B$.

Problem 12.16
Using a Venn diagram, show that $A \Delta B = (A\backslash B) \cup (B\backslash A) = (A \cap B^c) \cup (B \cap A^c)$.

Problem 12.17
Let $A = \{a, b, c\}$. Find $A \times A$.

Problem 12.18
Find the symmetric difference of the two sets $A = \{1, 3, 5\}$ and $B = \{1, 2, 3\}$.

Problem 12.19
Let $A = \{1, 2, 3\}$ and $B = \{2, 5\}$ be two subsets of a universal set $U = \{1, 2, 3, 4, 5\}$. Compare $(A \cup B)^c$ and $A^c \cap B^c$.

Problem 12.20
Let A and B be two subsets of a universal set U. Compare $A \backslash B$ and $A \cap B^c$.

13 Properties of Sets

In this section, we derive some properties of the set theory operations introduced in the previous section. The following example shows that the operation $\subseteq$ is reflexive and transitive, concepts that will be discussed in the next chapter.

Example 13.1
(a) Show that $A \subseteq A$.
(b) Suppose that A, B, C are sets such that $A \subseteq B$ and $B \subseteq C$. Show that $A \subseteq C$.

Solution.
(a) The proposition if $x \in A$ then $x \in A$ is always true. Thus, $A \subseteq A$.
(b) We need to show that every element of A is an element of C. Let $x \in A$. Since $A \subseteq B$, we have $x \in B$. But $B \subseteq C$ so that $x \in C$ ■

Theorem 13.1
Let A and B be two sets. Then
(a) $A \cap B \subseteq A$ and $A \cap B \subseteq B$.
(b) $A \subseteq A \cup B$ and $B \subseteq A \cup B$.

Proof.
(a) If $x \in A \cap B$ then $x \in A$ and $x \in B$. This still imply that $x \in A$. Hence, $A \cap B \subseteq A$. A similar argument holds for $A \cap B \subseteq B$.
(b) The proposition "if $x \in A$ then $x \in A \cup B$" is always true. Hence, $A \subseteq A \cup B$. A similar argument holds for $B \subseteq A \cup B$ ■

Theorem 13.2
Let A be a subset of a universal set U. Then
(a) $\emptyset^c = U$.
(b) $U^c = \emptyset$.
(c) $(A^c)^c = A$.
(d) $A \cup A^c = U$.
(e) $A \cap A^c = \emptyset$.

Proof.
(a) If $x \in U$ then $x \in U$ and $x \notin \emptyset$. Thus, $U \subseteq \emptyset^c$. Conversely, suppose that

$x \in \emptyset^c$. Then $x \in U$ and $x \notin \emptyset$. This implies that $x \in U$. Hence, $\emptyset^c \subseteq U$.
(b) It is always true that $\emptyset \subseteq U^c$. Conversely, the proposition "$x \in U$ and $x \notin U$ implies $x \in \emptyset$" is vacuously true since the hypothesis is false. This says that $U^c \subseteq \emptyset$.
(c) Let $x \in (A^c)^c$. Then $x \in U$ and $x \notin A^c$. That is, $x \in U$ and ($x \notin U$ or $x \in A$). Since $x \in U$, we have $x \in A$. Hence, $(A^c)^c \subseteq A$. Conversely, suppose that $x \in A$. Then $x \in U$ and $x \in A$. That is, $x \in U$ and $x \notin A^c$. Thus, $x \in (A^c)^c$. This shows that $A \subseteq (A^c)^c$.
(d) and (e) See Problem 13.17 ■

Theorem 13.3
If A and B are subsets of U then
(a) $A \cup U = U$.
(b) $A \cup A = A$.
(c) $A \cup \emptyset = A$.
(d) $A \cup B = B \cup A$.
(e) $(A \cup B) \cup C = A \cup (B \cup C)$.

Proof.
(a) Clearly, $A \cup U \subseteq U$. Conversely, let $x \in U$. Then definitely, $x \in A \cup U$. That is, $U \subseteq A \cup U$.
(b) If $x \in A$ then $x \in A$ or $x \in A$. That is, $x \in A \cup A$ and consequently $A \subseteq A \cup A$. Conversely, if $x \in A \cup A$ then $x \in A$. Hence, $A \cup A \subseteq A$.
(c) If $x \in A \cup \emptyset$ then $x \in A$ since $x \notin \emptyset$. Thus, $A \cup \emptyset \subseteq A$. Conversely, if $x \in A$ then $x \in A$ or $x \in \emptyset$. Hence, $A \subseteq A \cup \emptyset$.
(d) and (e) See Problem 13.18 ■

Theorem 13.4
Let A and B be subsets of U. Then
(a) $A \cap U = A$.
(b) $A \cap A = A$.
(c) $A \cap \emptyset = \emptyset$.
(d) $A \cap B = B \cap A$.
(e) $(A \cap B) \cap C = A \cap (B \cap C)$.

Proof.
(a) If $x \in A \cap U$ then $x \in A$. That is , $A \cap U \subseteq A$. Conversely, let $x \in A$. Then definitely, $x \in A$ and $x \in U$. That is, $x \in A \cap U$. Hence, $A \subseteq A \cap U$.

(b) If $x \in A$ then $x \in A$ and $x \in A$. That is, $A \subseteq A \cap A$. Conversely, if $x \in A \cap A$ then $x \in A$. Hence, $A \cap A \subseteq A$.
(c) Clearly $\emptyset \subseteq A \cap \emptyset$. Conversely, if $x \in A \cap \emptyset$ then $x \in \emptyset$. Hence, $A \cap \emptyset \subseteq \emptyset$.
(d) If $x \in A \cap B$ then $x \in A$ and $x \in B$. But this is the same thing as saying $x \in B$ and $x \in A$. That is, $x \in B \cap A$. Now interchange the roles of A and B to show that $B \cap A \subseteq A \cap B$.
(e) Let $x \in (A \cap B) \cap C$. Then $x \in (A \cap B)$ and $x \in C$. Thus, ($x \in A$ and $x \in B$) and $x \in C$. This implies $x \in A$ and ($x \in B$ and $x \in C$). Hence, $x \in A \cap (B \cap C)$. The converse is similar ■

Theorem 13.5
If A, B, and C are subsets of U then
(a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
(b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Proof.
(a) Let $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$. Thus, $x \in A$ and ($x \in B$ or $x \in C$). This implies that ($x \in A$ and $x \in B$) or ($x \in A$ and $x \in C$). Hence, $x \in A \cap B$ or $x \in A \cap C$, i.e. $x \in (A \cap B) \cup (A \cap C)$. The converse is similar.
(b) See Problem 13.19 ■

Theorem 13.6 *(De Morgan's Laws)*
Let A and B be subsets of U then
(a) $(A \cup B)^c = A^c \cap B^c$.
(b) $(A \cap B)^c = A^c \cup B^c$.

Proof.
(a) Let $x \in (A \cup B)^c$. Then $x \in U$ and $x \notin A \cup B$. Hence, $x \in U$ and ($x \notin A$ and $x \notin B$). This implies that ($x \in U$ and $x \notin A$) and ($x \in U$ and $x \notin B$). It follows that $x \in A^c \cap B^c$. Now, go backward for the converse.
(b) Let $x \in (A \cap B)^c$. Then $x \in U$ and $x \notin A \cap B$. Hence, $x \in U$ and ($x \notin A$ or $x \notin B$). This implies that ($x \in U$ and $x \notin B$) or ($x \in U$ and $x \notin A$). It follows that $x \in A^c \cup B^c$. The converse is similar ■

Theorem 13.7
Suppose that $A \subseteq B$. Then
(a) $A \cap B = A$.
(b) $A \cup B = B$.

Proof.
See Problem 13.20 ■

Example 13.2
Let A and B be arbitrary sets. Show that $(A\backslash B) \cap B = \emptyset$.

Solution.
Suppose not. That is, suppose $(A\backslash B) \cap B \neq \emptyset$. Then there is an element x that belongs to both $A\backslash B$ and B. By the definition of $A\backslash B$ we have that $x \notin B$. Thus, $x \in B$ and $x \notin B$ which is a contradiction ■

A collection of nonempty subsets $\{A_1, A_2, \cdots, A_n\}$ of A is said to be a **partition** of A if and only if
(i) $A = \cup_{k=1}^{n} A_k$.
(ii) $A_i \cap A_j = \emptyset$ for all $i \neq j$.

Example 13.3
Let $A = \{1, 2, 3, 4, 5, 6\}, A_1 = \{1, 2\}, A_2 = \{3, 4\}, A_3 = \{5, 6\}$. Show that $\{A_1, A_2, A_3\}$ is a partition of A.

Solution.
(i) $A_1 \cup A_2 \cup A_3 = A$.
(ii) $A_1 \cap A_2 = A_1 \cap A_3 = A_2 \cap A_3 = \emptyset$ ■

The number of elements of a set is called the **cardinality** of the set. We write $|A|$ to denote the cardinality of the set A. If A has a finite cardinality we say that A is a **finite** set. Otherwise, it is called **infinite**.

Example 13.4
What is the cardinality of each of the following sets?
(a) $\emptyset$.
(b) $\{\emptyset\}$.
(c) $\{a, \{a\}, \{a, \{a\}\}\}$.

Solution.
(a) $|\emptyset| = 0$
(b) $|\{\emptyset\}| = 1$
(c) $|\{a, \{a\}, \{a, \{a\}\}\}| = 3$ ■

Let A be a set. The **power set** of A, denoted by $\mathcal{P}$(A), is the empty set together with all possible subsets of A.

Example 13.5
Find the power set of $A = \{a, b, c\}$.

Solution.

$$\mathcal{P}(\mathrm{A}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

Theorem 13.8
If $A \subseteq B$ then $\mathcal{P}(\mathrm{A}) \subseteq \mathcal{P}(\mathrm{B})$.

Proof.
Let $X \in \mathcal{P}(\mathrm{A})$. Then $X \subseteq A$. Since $A \subseteq B$, we have $X \subseteq B$. Hence, $X \in \mathcal{P}(\mathrm{B})$ ■

Example 13.6
(a) Use induction to show that if $|A| = n$ then $|\mathcal{P}(\mathrm{A})| = 2^n$.
(b) If $\mathcal{P}(\mathrm{A})$ has 256 elements, how many elements are there in A?

Solution.
(a) If $n = 0$ then $A = \emptyset$ and in this case $\mathcal{P}(\mathrm{A}) = \{\emptyset\}$. Thus $|\mathcal{P}(\mathrm{A})| = 1$. As induction hypothesis, suppose that if $|A| = n$ then $|\mathcal{P}(\mathrm{A})| = 2^n$. Let $B = A \cup \{a_{n+1}\}$. Then $\mathcal{P}(\mathrm{B})$ consists of all subsets of A and all subsets of A with the element a_{n+1} added to them. Hence, $|\mathcal{P}(\mathrm{B})| = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$.
(b) Since $|\mathcal{P}(\mathrm{A})| = 256 = 2^8$, we have $|A| = 8$ ■

Review Problems

Problem 13.1
Let A, B, and C be sets. Prove that if $A \subseteq B$ then $A \cap C \subseteq B \cap C$.

Problem 13.2
Find sets A, B, and C such that $A \cap C = B \cap C$ but $A \neq B$.

Problem 13.3
Find sets A, B, and C such that $A \cap C \subseteq B \cap C$ and $A \cup C \subseteq B \cup C$ but $A \neq B$.

Problem 13.4
Let A and B be two sets. Prove that if $A \subseteq B$ then $B^c \subseteq A^c$.

Problem 13.5
Let A, B, and C be sets. Prove that if $A \subseteq C$ and $B \subseteq C$ then $A \cup B \subseteq C$.

Problem 13.6
Let A, B, and C be sets. Show that $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Problem 13.7
Let A, B, and C be sets. Show that $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Problem 13.8
(a) Is the number 0 in $\emptyset$? Why?
(b) Is $\emptyset = \{\emptyset\}$? Why?
(c) Is $\emptyset \in \{\emptyset\}$? Why?

Problem 13.9
Let A and B be two sets. Prove that $(A \backslash B) \cap (A \cap B) = \emptyset$.

Problem 13.10
Let A and B be two sets. Show that if $A \subseteq B$ then $A \cap B^c = \emptyset$.

Problem 13.11
Let A, B and C be three sets. Prove that if $A \subseteq B$ and $B \cap C = \emptyset$ then $A \cap C = \emptyset$.

Problem 13.12
Find two sets A and B such that $A \cap B = \emptyset$ but $A \times B \neq \emptyset$.

Problem 13.13
Suppose that $A = \{1, 2\}$ and $B = \{2, 3\}$. Find each of the following:
(a) $\mathcal{P}(\mathrm{A} \cap \mathrm{B})$.
(b) $\mathcal{P}(\mathrm{A})$.
(c) $\mathcal{P}(\mathrm{A} \cup \mathrm{B})$.
(d) $\mathcal{P}(\mathrm{A} \times \mathrm{B})$.

Problem 13.14
(a) Find $\mathcal{P}(\emptyset)$.
(b) Find $\mathcal{P}(\mathcal{P}(\emptyset))$.
(c) Find $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$.

Problem 13.15
Determine which of the following statements are true and which are false. Prove each statement that is true and give a counterexample for each statement that is false.
(a) $\mathcal{P}(\mathrm{A} \cup \mathrm{B}) = \mathcal{P}(\mathrm{A}) \cup \mathcal{P}(\mathrm{B})$.
(b) $\mathcal{P}(\mathrm{A} \cap \mathrm{B}) = \mathcal{P}(\mathrm{A}) \cap \mathcal{P}(\mathrm{B})$.
(c) $\mathcal{P}(\mathrm{A}) \cup \mathcal{P}(\mathrm{B}) \subseteq \mathcal{P}(\mathrm{A} \cup \mathrm{B})$.
(d) $\mathcal{P}(\mathrm{A} \times \mathrm{B}) = \mathcal{P}(\mathrm{A}) \times \mathcal{P}(\mathrm{B})$.

Problem 13.16
Find two sets A and B such that $A \in B$ and $A \subseteq B$.

Problem 13.17
Let A be a subset of a universal set U. Prove:
(a) $A \cup A^c = U$.
(b) $A \cap A^c = \emptyset$.

Problem 13.18
Let A and B be subsets of U. Prove:
(a) $A \cup B = B \cup A$.
(b) $(A \cup B) \cup C = A \cup (B \cup C)$.

Problem 13.19
Let A, B, and C b subsets of U. Prove $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Problem 13.20
Suppose that $A \subseteq B$. Prove:
(a) $A \cap B = A$.
(b) $A \cup B = B$.

14 Boolean Algebra

Logic circuits are the basis for modern digital computer systems. To appreciate how computer systems operate you will need to understand digital logic and boolean algebra. This Chapter provides only a basic introduction to boolean algebra.
A **Boolean algebra** is a nonempty set S together with two operations $\oplus$ and $\odot$ that satisfy the following axioms:

• **Closure:** $a \oplus b \in S$ and $a \odot b \in S$ for all $a, b \in S$.
• **Cummutative law**: $a \oplus b = b \oplus a$ and $a \odot b = b \odot a$, $\forall a, b \in S$.
• **Associative law**: $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ and $a \odot (b \odot c) = (a \odot b) \odot c)$, $\forall a, b, c \in S$.
• **Distributive law**: $a \oplus (b \odot c) = (a \oplus b) \odot (a \oplus c)$ and $a \odot (b \oplus c) = a \odot b \oplus a \odot c$ $\forall a, b, c \in S$.
• **Identity element**: There exist distinct elements 0 and 1 in S such that $a \oplus 0 = a$ and $a \odot 1 = a$ $\forall a \in S$.
• **Inverse element**: For each $a \in S$ there exists an element $\overline{a}$ such that $a \oplus \overline{a} = 1$ and $a \odot \overline{a} = 0$. We call $\overline{a}$ the **complement** or the **negation** of a.

We write $(S, \oplus, \odot)$.

Example 14.1
Show that if S is a collection of propositions with finite propositional variables then $(S, \vee, \wedge)$ is a Boolean algebra.

Solution.
Let $p, q, r \in S$. Then
(1) $p \vee q \in S$ and $p \wedge q \in S$.
(2) $p \vee q \equiv q \vee p$ and $p \wedge q \equiv q \wedge p$.
(3) $p \vee (q \vee r) \equiv (p \vee q) \vee r$ and $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$.
(4) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ and $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$.
(5) Let c be a contradiction and t a tautology then $p \vee c \equiv p$ and $p \wedge t \equiv p$.
(6) If $p \in S$ then $\sim p \in S$ is such that $p \vee \sim p \equiv t$ and $p \wedge \sim p \equiv c$ ■

Example 14.2
Show that for a given nonempty set S, $(\mathcal{P}(\mathrm{S}), \cup, \cap)$ is a Boolean algebra.

Solution.
Let $A, B, C \in \mathcal{P}(\mathrm{S})$. Then
(1) $A \cup B \in \mathcal{P}(\mathrm{S})$ and $A \cap B \in \mathcal{P}(\mathrm{S})$.
(2) $A \cup B = B \cup A$ and $A \cap B = B \cap A$.
(3) $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$.
(4) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
(5) $A \cup \emptyset = A$ and $A \cap S = A$.
(6) $A \cup A^c = S$ and $A \cap A^c = \emptyset$ ■

Example 14.3 *(Idempotent law)*
Show that $x \oplus x = x$.

Solution.
We have

$$\begin{aligned} x \oplus x =& (x \oplus x) \odot 1 = (x \oplus x) \odot (x \oplus \overline{x}) \\ =& x \oplus (x \odot \overline{x}) \\ =& x \oplus 0 = x \end{aligned}$$ ■

Example 14.4 *(Domination law)*
Show that $x \oplus 1 = 1$.

Solution.
We have

$$\begin{aligned} x \oplus 1 =& x \oplus (x \oplus \overline{x}) \\ =& (x \oplus x) \oplus \overline{x} \\ =& x \oplus \overline{x} = 1 \end{aligned}$$ ■

Example 14.5 *(Absorption law)*
Show that $(x \odot y) \oplus x = x$.

Solution.
We have

$$\begin{aligned} (x \odot y) \oplus x =& x \odot y \oplus x \odot 1 \\ =& x \odot (y \oplus 1) \\ =& x \odot 1 = x \end{aligned}$$ ■

Example 14.6
Show that if $x \oplus y = 1$ and $x \odot y = 0$ then $y = \overline{x}$.

Solution.
We have

$$\begin{aligned} y =& y \odot 1 \\ =& y \odot (x \oplus \overline{x}) \\ =& y \odot x \oplus y \odot \overline{x} \\ =& 0 \oplus y \odot \overline{x} \\ =& y \odot \overline{x}. \end{aligned}$$

Likewise, we have

$$\begin{aligned} \overline{x} =& \overline{x} \odot 1 \\ =& \overline{x} \odot (x \oplus y) \\ =& \overline{x} \odot x \oplus \overline{x} \odot y \\ =& 0 \oplus \overline{x} \odot y \\ =& \overline{x} \odot y = y \odot \overline{x}. \end{aligned}$$

Hence, $y = \overline{x}$ ■

Example 14.7 *(Double Complement)*
Show that $\overline{\overline{x}} = x$.

Solution.
Since $\overline{x} \oplus x = 1$ and $\overline{x} \odot x = 0$, the previous example implies that $\overline{\overline{x}} = x$ ■

Example 14.8
Let $u \in S$ such that $x \oplus u = x$ for all $x \in S$. Show that $u = 0$.

Solution.
Since $x \oplus u = x$ for all $x \in S$, by choosing $x = 0$ we have $0 = 0 \oplus u = u$ ■

Example 14.9 *(DeMorgan's law)*
Show that $\overline{x \odot y} = \overline{x} \oplus \overline{y}$.

Solution.
We have

$$\begin{aligned}(x \odot y) \oplus (\overline{x} \oplus \overline{y}) =& (\overline{x} \oplus \overline{y}) \oplus (x \odot y) \\ =& [(\overline{x} \oplus \overline{y}) \oplus x] \odot [(\overline{x} \oplus \overline{y}) \oplus y] \\ =& [\overline{y} \oplus (\overline{x} \oplus x] \odot [\overline{x} \oplus (\overline{y} \oplus y)] \\ =& (\overline{y} \oplus 1) \odot (\overline{x} \oplus 1) \\ =& 1 \odot 1 = 1\end{aligned}$$

and

$$\begin{aligned}(x \odot y) \odot (\overline{x} \oplus \overline{y}) =& [(x \odot y) \odot \overline{x}] \oplus [(x \odot y) \odot \overline{y}] \\ =& [(x \odot \overline{x}) \odot y] \oplus [x \odot (y \odot \overline{y})] \\ =& (0 \odot y) \oplus (x \odot 0) \\ =& = \qquad\qquad 0.\end{aligned}$$

Note that $0 \odot x = 0 \odot y = 0$ by Problem 14.2. Hence, by Example 14.6, we have $\overline{x \odot y} = \overline{x} \oplus \overline{y}$ ■

Example 14.10
In Chapter 2, we denote the logical gate AND by $\cdot$, the logical gate OR by $+$, and the logical gate $\sim P$ by $\overline{P}$. Simplify the circuit given in Figure 14.1.

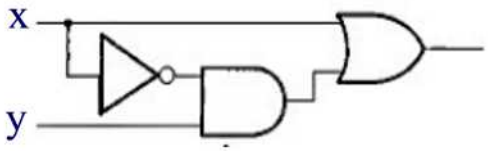


Figure 14.1

Solution.
From Problem 14.4, we have $x + \overline{x} \cdot y = x + y$. Hence, the resulting circuit simplification is shown in Figure 14.2 ■

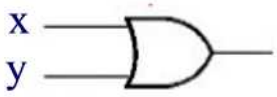


Figure 14.2

Review Problems

Problem 14.1
Show that $x \odot x = x$.

Problem 14.2
Show that $x \odot 0 = 0$.

Problem 14.3
Show that $(x \oplus y) \odot x = x$.

Problem 14.4
Show that $x \oplus (\overline{x} \odot y) = x \oplus y$.

Problem 14.5
Let $v \in S$ such that $x \odot v = x$ for all $x \in S$. Show that $v = 1$.

Problem 14.6
Show that $\overline{x \oplus y} = \overline{x} \odot \overline{y}$.

Problem 14.7
Show that $\overline{1} = 0$ and $\overline{0} = 1$.

Problem 14.8
Show that $x \odot (\overline{x} \oplus y) = x \odot y$.

Problem 14.9
Show that $\overline{\overline{x} \odot \overline{y}} = x \oplus y$.

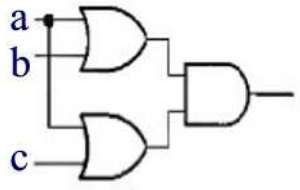
Problem 14.10
Simplify $[(x \oplus y \oplus z) \odot \overline{s \oplus t}] \oplus [(x \oplus y \oplus z) \odot (s \oplus t)]$.

Problem 14.11
Simplify $x \oplus \overline{x \odot y}$.

Problem 14.12
Simplify $\overline{x \odot y} \odot (\overline{x} \oplus y) \odot (\overline{y} \oplus y)$.

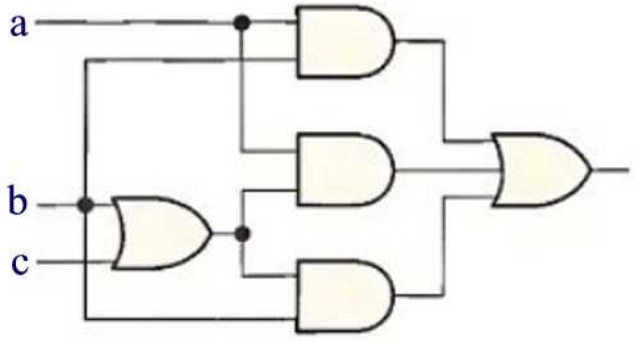
Problem 14.13
Simplify $(a \oplus b) \odot (a \oplus c)$.

Problem 14.14
Find the resulting circuit simplification of the circuit below.



Problem 14.15
Simplify $(a \odot b) \oplus [a \odot (b \oplus c)] \oplus [b \odot (b \oplus c)]$.

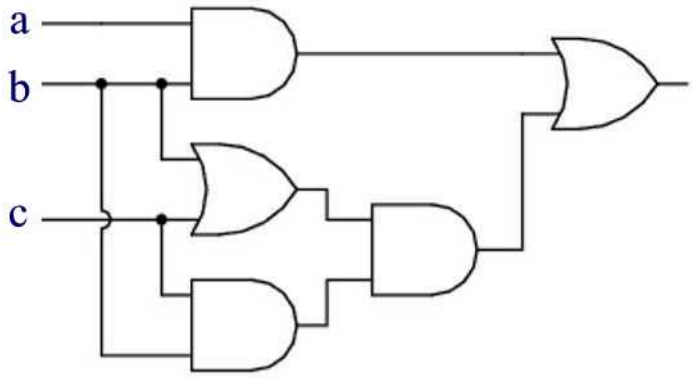
Problem 14.16
Find the resulting circuit simplification of the circuit below.



Problem 14.17
Simplify $a \oplus (a \odot b) \oplus [\overline{a} \odot (\overline{a} \oplus c)]$.

Problem 14.18
Simplify $a \cdot b + b \cdot c \cdot (b + c)$.

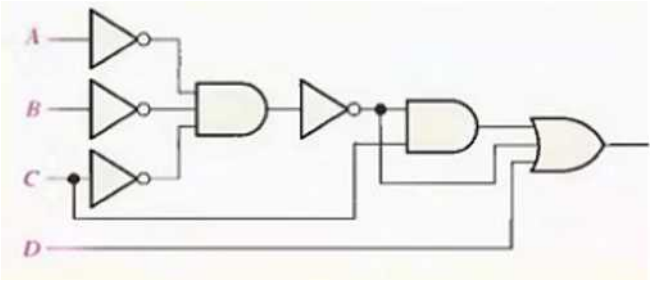
Problem 14.19
Find the resulting circuit simplification of the circuit below.



Problem 14.20
Simplify $\overline{(\overline{a} \odot b) \oplus (\overline{a} \odot \overline{b}) \oplus \overline{b}}$.

Problem 14.21
Simplify: $(\overline{\overline{A} \cdot \overline{B} \cdot \overline{C}}) \cdot C + \overline{\overline{A} \cdot \overline{B} \cdot \overline{C}} + D$.

Problem 14.22
Reduce the following logic circuit with a simple logic circuit.



Relations and Functions

The reader is familiar with many relations which are used in mathematics and computer science, i.e. “is a subset of”, “ is less than” and so on.
One frequently wants to compare or contrast various members of a set, perhaps to arrange them in some appropriate order or to group together those with similar properties. The mathematical framework to describe this kind of organization of sets is the theory of relations.
There are two kinds of relations which we discuss in this chapter: (i) equivalence relations, and (ii) order relations.

15 Binary Relations

Let A and B be two given sets. An **ordered pair** (a, b), where $a \in A$ and $b \in B$, is defined to be the set $\{a, \{a, b\}\}$. The element a (resp. b) is called the **first** (resp. **second**) **component**.

Example 15.1
(a) Show that if $a \neq b$ then $(a, b) \neq (b, a)$.
(b) Show that $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.

Solution.
(a) If $a \neq b$ then $\{a, \{a, b\}\} \neq \{b, \{a, b\}\}$. That is, $(a, b) \neq (b, a)$.
(b) $(a, b) = (c, d)$ if and only if $\{a, \{a, b\}\} = \{c, \{c, d\}\}$ and this is equivalent to $a = c$ and $\{a, b\} = \{c, d\}$ by the definition of equality of sets. Thus, $a = c$ and $b = d$ ■

Example 15.2
Find x and y such that $(x + y, 0) = (1, x - y)$.

Solution.
We have the system

$$\begin{cases} x + y = 1 \\ x - y = 0. \end{cases}$$

Solving by the method of elimination one finds $x = \frac{1}{2}$ and $y = \frac{1}{2}$ ■

The collection of all ordered pairs (a, b) where $a \in A$ and $b \in B$ is denoted by $A \times B$. We call $A \times B$ the **Cartesian product** of A and B.

Example 15.3
(a) Show that if A is a set with m elements and B is a set of n elements then $A \times B$ is a set of mn elements.
(b) Show that if $A \times B = \emptyset$ then $A = \emptyset$ or $B = \emptyset$.

Solution.
(a) Suppose that $A = \{a_1, a_2, \cdots, a_m\}$ and $B = \{b_1, b_2, \cdots, b_n\}$. Then

$$\begin{aligned} A \times B = \{&(a_1, b_1), (a_1, b_2), \cdots, (a_1, b_n), \\ &(a_2, b_1), (a_2, b_2), \cdots, (a_2, b_n), \\ &(a_3, b_1), (a_3, b_2), \cdots, (a_3, b_n), \\ &\vdots \\ &(a_m, b_1), (a_m, b_2), \cdots, (a_m, b_n)\} \end{aligned}$$

Thus, $|A \times B| = m \cdot n = |A| \cdot |B|$.
(b) We use the proof by contrapositive. Suppose that $A \neq \emptyset$ and $B \neq \emptyset$. Then there is at least an $a \in A$ and an element $b \in B$. That is, $(a, b) \in A \times B$ and this shows that $A \times B \neq \emptyset$ ■

Example 15.4
Let $A = \{1, 2\}, B = \{1\}$. Show that $A \times B \neq B \times A$.

Solution.
We have $A \times B = \{(1, 1), (2, 1)\} \neq \{(1, 1), (1, 2)\} = B \times A$ ■

A **binary relation** R from a set A to a set B is a subset of $A \times B$. If $(a, b) \in R$ we write aRb and we say that a is related to b. If a is not related to b we write $a \not R b$. In case $A = B$ we call R a **binary relation** on A.
The set

$$\text{Dom}(R) = \{a \in A | (a, b) \in R \text{ for some b} \in B\}$$

is called the **domain** of R. The set

$$\text{Range}(R) = \{b \in B | (a, b) \in R \text{ for some a} \in A\}$$

is called the **range** of R.

Example 15.5
(a) Let $A = \{2, 3, 4\}$ and $B = \{3, 4, 5, 6, 7\}$. Define the relation R by aRb if and only if a *divides* b. Find, $R, \text{Dom}(R), \text{Range}(R)$.
(b) Let $A = \{1, 2, 3, 4\}$. Define the relation R by aRb if and only if $a \leq b$. Find, $R, \text{Dom}(R), \text{Range}(R)$.

Solution.
(a) $R = \{(2,4),(2,6),(3,3),(3,6),(4,4)\}$, $\text{Dom}(R) = \{2,3,4\}$, and $\text{Range}(R) = \{3,4,6\}$.
(b) $R = \{(1,1),(1,2),(1,3),(1,4),(2,2),(2,3),(2,4),(3,3),(3,4),(4,4)\}$, $\text{Dom}(R) = A$, $\text{Range}(R) = A$ ■

A **function** is a special case of a relation. A function from A to B, denoted by $f : A \to B$, is a relation from A to B such that for every $x \in A$ there is a unique $y \in B$ such that $(x, y) \in f$. The element y is called the **image** of x and we write $y = f(x)$. The set A is called the **domain** of f and the set of all images of f is called the **range** of f.

Example 15.6
(a) Show that the relation

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

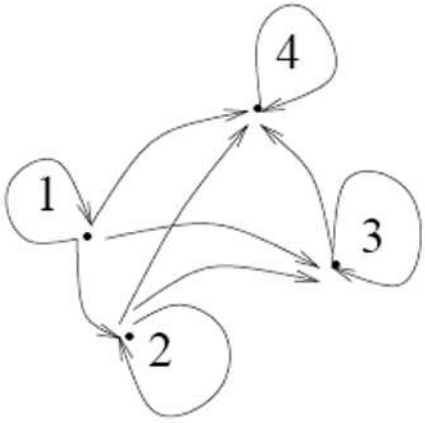
defines a function from $A = \{1,2,3\}$ to $B = \{a,b,c\}$. Find its range.
(b) Show that the relation $f = \{(1,a),(2,b),(3,c),(1,b)\}$ does not define a function from $A = \{1,2,3\}$ to $B = \{a,b,c\}$.

Solution.
(a) Note that each element of A has exactly one image. Hence, f is a function with domain A and range $\text{Range}(f) = \{a,b\}$.
(b) The relation f does not define a function since the element 1 has two images, namely a and b ■

An informative way to picture a relation on a set is to draw its **digraph.** To draw a digraph of a relation on a set A, we first draw dots or **vertices** to represent the elements of A. Next, if $(a,b) \in R$ we draw an arrow (called a **directed edge**) from a to b. Finally, if $(a,a) \in R$ then the directed edge is simply a **loop**.

Example 15.7
Draw the directed graph of the relation in part (b) of Example 15.5.

Solution.



■

Next we discuss three ways of building new relations from given ones. Let R be a relation from a set A to a set B. The **inverse** of R is the relation R^{-1} from Range(R) to Dom(R) such that

$$R^{-1} = \{(b, a) \in B \times A : (a, b) \in R\}.$$

Example 15.8
Let $R = \{(1, y), (1, z), (3, y)\}$ be a relation from $A = \{1, 2, 3\}$ to $B = \{x, y, z\}$.
(a) Find R^{-1}.
(b) Compare $(R^{-1})^{-1}$ and R.

Solution.
(a) $R^{-1} = \{(y, 1), (z, 1), (y, 3)\}$.
(b) $(R^{-1})^{-1} = R$ ■

Let R and S be two relations from a set A to a set B. Then we define the relations $R \cup S$ and $R \cap S$ by

$$R \cup S = \{(a, b) \in A \times B | (a, b) \in R \text{ or } (a, b) \in S\},$$

and

$$R \cap S = \{(a, b) \in A \times B | (a, b) \in R \text{ and } (a, b) \in S\}.$$

Example 15.9
Given the following two relations from $A = \{1, 2, 4\}$ to $B = \{2, 6, 8, 10\}$:

$$aRb \text{ if and only if } a|b.$$
$$aSb \text{ if and only if } b-4=a.$$

List the elements of $R, S, R \cup S$, and $R \cap S$.

Solution.
We have

$$\begin{aligned} R =& \{(1,2),(1,6),(1,8),(1,10),(2,2),(2,6),(2,8),(2,10),(4,8)\} \\ S =& \{(2,6),(4,8)\} \\ R \cup S =& R \\ R \cap S =& S \end{aligned}$$ ■

Now, if we have a relation R from A to B and a relation S from B to C we can define the relation $S \circ R$, called the **composition** relation[2], to be the relation from A to C defined by

$$S \circ R = \{(a,c) | (a,b) \in R \textit{ and } (b,c) \in S \text{ for some } b \in B\}.$$

Example 15.10
Let

$$\begin{aligned} R =& \{(1,2),(1,6),(2,4),(3,4),(3,6),(3,8)\} \\ S =& \{(2,u),(4,s),(4,t),(6,t),(8,u)\} \end{aligned}$$

Find $S \circ R$.

Solution.

$$S \circ R = \{(1,u),(1,t),(2,s),(2,t),(3,s),(3,t),(3,u)\}$$ ■

[2]Some authors prefer the notation $R \circ S$ instead of $S \circ R$. We rather prefer the notation $S \circ R$ so that we are consistent with the case when R and S are functions. That is, if R and S are functions then the composition of R and S is $S \circ R$.

Review Problems

Problem 15.1
Suppose that $|A| = 3$ and $|A \times B| = 24$. What is $|B|$?

Problem 15.2
Let $A = \{1, 2, 3\}$. Find $A \times A$.

Problem 15.3
Find x and y so that $(3x - y, 2x + 3y) = (7, 1)$.

Problem 15.4
Find the domain and range of the relation $R = \{(5, 6), (-12, 4), (8, 6), (-6, -6), (5, 4)\}$.

Problem 15.5
Let $A = \{1, 2, 3\}$ and $B = \{a, b, c, d\}$.
(a) Is the relation $f = \{(1, d), (2, d), (3, a)\}$ a function from A to B? If so, find its range.
(b) Is the relation $f = \{(1, a), (2, b), (2, c), (3, d)\}$ a function from A to B? If so, find its range.

Problem 15.6
Let R be the divisibility relation on the set $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Construct the digraph of R.

Problem 15.7
Find the inverse relation of $R = \{(a, 1), (b, 5), (c, 2), (d, 1)\}$. Is the inverse relation a function?

Problem 15.8
Let

$$\begin{aligned} A =& \{1, 2, 3, 4\} \\ B =& \{1, 2, 3\} \\ R =& \{(1, 2), (1, 3), (1, 4), (2, 2), (3, 4), (4, 1), (4, 2)\} \\ S =& \{(1, 1), (1, 2), (1, 3), (2, 3)\}. \end{aligned}$$

Find (a) $R \cup S$ (b) $R \cap S$ (c) $R \backslash S$ and (d) $S \backslash R$.

Problem 15.9
Let

$$\begin{aligned} A =& \{a, b, c\} \\ B =& \{1, 2\} \\ C =& \{a, b, g\} \\ R =& \{(a, 1), (a, 2), (b, 2), (c, 1)\} \\ S =& \{(1, a), (2, b), (2, g)\}. \end{aligned}$$

Find $S \circ R$.

Problem 15.10
Let $X = \{a, b, c\}$. Recall that $\mathcal{P}(X)$ is the power set of X. Define a binary relation $\mathcal{R}$ on $\mathcal{P}(X)$ as follows:

$$A, B \in \mathcal{P}(x),\ A\ \mathcal{R}\ B \Leftrightarrow |A| = |B|.$$

(a) Is $\{a, b\}\mathcal{R}\{b, c\}$?
(b) Is $\{a\}\mathcal{R}\{a, b\}$?
(c) Is $\{c\}\mathcal{R}\{b\}$?

Problem 15.11
Let $A = \{4, 5, 6\}$ and $B = \{5, 6, 7\}$ and define the binary relations R, S, and T from A to B as follows:

$$(x, y) \in A \times B, (x, y) \in R \Leftrightarrow x \geq y.$$

$$(x, y) \in A \times B, x\ S\ y \Leftrightarrow 2|(x - y).$$

$$T = \{(4, 7), (6, 5), (6, 7)\}.$$

(a) Draw arrow diagrams for R, S, and T.
(b) Indicate whether any of the relations S, R, or T are functions.

Problem 15.12
Let $A = \{3, 4, 5\}$ and $B = \{4, 5, 6\}$ and define the binary relation R as follows:

$$(x, y) \in A \times B, (x, y) \in R \Leftrightarrow x < y.$$

List the elements of the sets R and R^{-1}.

Problem 15.13
Let $A = \{2, 4\}$ and $B = \{6, 8, 10\}$ and define the binary relations R and S from A to B as follows:

$$(x, y) \in A \times B, (x, y) \in R \Leftrightarrow x|y.$$

$$(x, y) \in A \times B, x \ S \ y \Leftrightarrow y - 4 = x.$$

List the elements of $A \times B, R, S, R \cup S$, and $R \cap S$.

Problem 15.14
A couple is planning their wedding. They have four nieces (Sara, Cindy, Brooke, and Nadia) and three nephews (Mike, John, and Derik). How many different pairings are possible to have one boy and one girl as a ring bearer and flower girl? List the possible choices as a Cartesian product.

Problem 15.15
Let R be a relation on a set A. We define the **complement** of R to be the relation $\sim R = (A \times A) \backslash R$. Let $A = \{1, 2, 3\}$ and R be the relation xRy if and only if $x \leq y$. Find $\sim R$.

Problem 15.16
Let $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = x^2\}$ and $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = -x\}$. Find $R \cap S$.

Problem 15.17
Consider a family A with five children, Amy, Bob, Charlie, Debbie, and Eric. We abbreviate the names to their first letters so that

$$A = \{a, b, c, d, e\}.$$

Let R be the brother-sister relation on A. Find R and draw the directed graph.

Problem 15.18
If $|A| = n$, where n is a positive integer, then how many binary relations are there on the set A?

Problem 15.19
Let $R = \{(a, b), (b, a), (b, c)\}$ be a relation on the set $A = \{a, b, c\}$. Find $R \circ R$.

Problem 15.20
Let $A = \{1\}$ and $B = \{4, 3, 2\}$. Find all the binary relations from A to B.

Problem 15.21
Let f be the relation on $\mathbb{R}$ defined by $x\ f\ y$ if and only $f(x) = -4x + 9$. Let g be the relation on $\mathbb{R}$ defined by $x\ g\ y$ if and only $g(x) = 2x - 7$. Find $f \circ g$ and $g \circ f$.

16 Equivalence Relations

In this section, we define four types of binary relations. A relation R on a set A is called **reflexive** if $(a, a) \in R$ for all $a \in A$. In this case, the digraph of R has a loop at each vertex.

Example 16.1
(a) Show that the relation $a \leq b$ on the set $A = \{1, 2, 3, 4\}$ is reflexive.
(b) Show that the relation on $\mathbb{R}$ defined by aRb if and only if $a < b$ is not reflexive.

Solution.
(a) Since $1 \leq 1, 2 \leq 2, 3 \leq 3$, and $4 \leq 4$, the given relation is reflexive.
(b) Indeed, for any real number a we have $a - a = 0$ and not $a - a < 0$ ■

A relation R on A is called **symmetric** if whenever $(a, b) \in R$ then we must have $(b, a) \in R$. The digraph of a symmetric relation has the property that whenever there is a directed edge from a to b, there is also a directed edge from b to a.

Example 16.2
(a) Let $A = \{a, b, c, d\}$ and $R = \{(a, a), (b, c), (c, b), (d, d)\}$. Show that R is symmetric.
(b) Let $\mathbb{R}$ be the set of real numbers and R be the relation aRb if and only if $a < b$. Show that R is not symmetric.

Solution.
(a) bRc and cRb so R is symmetric.
(b) $2 < 4$ but $4 \not< 2$ ■

A relation R on a set A is called **antisymmetric** if whenever $(a, b) \in R$ and $a \neq b$ then $(b, a) \notin R$. The digraph of an antisymmetric relation has the property that between any two vertices there is at most one directed edge.

Example 16.3
(a) Let $\mathbb{N}$ be the set of positive integers and R the relation aRb if and only if a divides b. Show that R is antisymmetric.
(b) Let $A = \{a, b, c, d\}$ and $R = \{(a, a), (b, c), (c, b), (d, d)\}$. Show that R is not antisymmetric.

Solution.
(a) Suppose that $a|b$ and $b|a$. We must show that $a = b$. Indeed, by the definition of division, there exist positive integers k_1 and k_2 such that $b = k_1 a$ and $a = k_2 b$. This implies that $a = k_2 k_1 a$ and hence $k_1 k_2 = 1$. Since k_1 and k_2 are positive integers, we must have $k_1 = k_2 = 1$. Hence, $a = b$.
(b) bRc and cRb with $b \neq c$ ■

A relation R on a set A is called **transitive** if whenever $(a, b) \in R$ and $(b, c) \in R$ then $(a, c) \in R$. The digraph of a transitive relation has the property that whenever there are directed edges from a to b and from b to c then there is also a directed edge from a to c.

Example 16.4
(a) Let $A = \{a, b, c, d\}$ and $R = \{(a, a), (b, c), (c, b), (d, d)\}$. Show that R is not transitive.
(b) Let $\mathbb{Z}$ be the set of integers and R the relation aRb if a divides b. Show that R is transitive.

Solution.
(a) $(b, c) \in R$ and $(c, b) \in R$ but $(b, b) \notin R$.
(b) Suppose that $a|b$ and $b|c$. Then there exist integers k_1 and k_2 such that $b = k_1 a$ and $c = k_2 b$. Thus, $c = (k_1 k_2)a$ which means that $a|c$ ■

Now, let $A_1, A_2, \cdots, A_n$ be a partition of a set A. That is, the $A_i's$ are subsets of A that satisfy
(i) $\cup_{i=1}^{n} A_i = A$
(ii) $A_i \cap A_j = \emptyset$ for $i \neq j$.
Define on A the binary relation $x\ R\ y$ if and only if x and y belongs to the same set A_i for some $1 \leq i \leq n$.

Theorem 16.1
The relation R defined above is reflexive, symmetric, and transitive.

Proof.
See Problem 16.9 ■

A relation that is reflexive, symmetric, and transitive on a set A is called an **equivalence relation on A.** For example, the relation "=" is an equivalence relation on $\mathbb{R}$.

Example 16.5
Let $\mathbb{Z}$ be the set of integers and $n \in \mathbb{Z}$. Let R be the relation on $\mathbb{Z}$ defined by aRb if $a - b$ is a multiple of n. We denote this relation by $a \equiv b \ (mod\ n)$ read "a congruent to b modulo n." Show that R is an equivalence relation on $\mathbb{Z}$.

Solution.
$\equiv$ is reflexive: For all $a \in \mathbb{Z}$, $a - a = 0 \cdot n$. That is, $a \equiv a \ (mod\ n)$.
$\equiv$ is symmetric: Let $a, b \in \mathbb{Z}$ such that $a \equiv b \ (mod\ n)$. Then there is an integer k such that $a - b = kn$. Multiply both sides of this equality by (-1) and letting $k' = -k$ we find that $b - a = k'n$. That is $b \equiv a \ (mod\ n)$.
$\equiv$ is transitive: Let $a, b, c \in \mathbb{Z}$ be such that $a \equiv b \ (mod\ n)$ and $b \equiv c \ (mod\ n)$. Then there exist integers k_1 and k_2 such that $a - b = k_1 n$ and $b - c = k_2 n$. Adding these equalities together we find $a - c = kn$ where $k = k_1 + k_2 \in \mathbb{Z}$ which shows that $a \equiv c \ (mod\ n)$ ■

Theorem 16.2
Let R be an equivalence relation on A. For each $a \in A$ let

$$[a] = \{x \in A | xRa\}$$

$$A/R = \{[a] | a \in A\}.$$

Then the union of all the elements of A/R is equal to A and the intersection of any two distinct members of A/R is the empty set. That is, A/R forms a partition of A.

Proof.
By the definition of $[a]$ we have that $[a] \subseteq A$. Hence, $\cup_{a \in A}[a] \subseteq A$. We next show that $A \subseteq \cup_{a \in A}[a]$. Indeed, let $a \in A$. Since A is reflexive, $a \in [a]$ and consequently $a \in \cup_{b \in A}[b]$. Hence, $A \subseteq \cup_{b \in A}[b]$. It follows that $A = \cup_{a \in A}[a]$. This establishes (i).
It remains to show that if $[a] \neq [b]$ then $[a] \cap [b] = \emptyset$ for $a, b \in A$. Suppose the contrary. That is, suppose $[a] \cap [b] \neq \emptyset$. Then there is an element $c \in [a] \cap [b]$. This means that $c \in [a]$ and $c \in [b]$. Hence, $a \ R \ c$ and $b \ R \ c$. Since R is symmetric and transitive, $a \ R \ b$. We will show that the conclusion $a \ R \ b$ leads to $[a] = [b]$. The proof is by double inclusions. Let $x \in [a]$. Then $x \ R \ a$. Since $a \ R \ b$ and R is transitive, $x \ R \ b$ which means that $x \in [b]$. Thus, $[a] \subseteq [b]$. Now interchange the letters a and b to show that $[b] \subseteq [a]$. Hence, $[a] = [b]$

which contradicts our assumption that $[a] \neq [b]$. This establishes (ii). Thus, A/R is a partition of A ■

The sets $[a]$ defined in the previous exercise are called the **equivalence classes** of A given by the relation R. The element a in $[a]$ is called a **representative** of the equivalence class $[a]$.

Example 16.6
Let R be an equivalence relation on A. Show that if aRb then $[a] = [b]$.

Solution.
$[a] \subseteq [b]$: Let $c \in [a]$. Then cRa. But aRb so that cRb since R is transitive. Hence, $c \in [b]$.
$[b] \subseteq [a]$: Let $c \in [b]$. Then cRb. Since R is symmetric, bRa. Hence, cRa since R is transitive. Thus, $c \in [a]$ ■

Example 16.7
Find the equivalence classes of the the equivalence relation on $\mathbb{Z}$ defined by $a \equiv b \bmod 4$.

Solution.
For any integer $a \in \mathbb{Z}$, the congruence class of a is

$$[a] = \{n \in \mathbb{Z} | n - a = 4k \text{ for some } k \in \mathbb{Z}\}.$$

Hence,

$$\begin{aligned}
[0] =& \{0, \pm 4, \pm 8, \pm 12, \cdots\} \\
[1] =& \{\cdots, -11, -7, -3, 1, 5, 9, \cdots\} \\
[2] =& \{\cdots, -10, -6, -2, 2, 6, 10, \cdots\} \\
[3] =& \{\cdots, -9, -5, -1, 3, 7, 11, \cdots\}.
\end{aligned}$$

Note that $\{[0], [1], [2], [3]\}$ is a partition of $\mathbb{Z}$. Also, note that $[0] = [\pm 4] = [\pm 8] = \cdots$; $[1] = [-11] = [-7] = \cdots$, etc ■

Review Problems

Problem 16.1
Consider the binary relation on $\mathbb{R}$ defined as follows:

$$x, y \in R,\ x\ R\ y \Leftrightarrow x \geq y.$$

Is R reflexive? symmetric? transitive?

Problem 16.2
Consider the binary relation on $\mathbb{R}$ defined as follows:

$$x, y \in R,\ x\ R\ y \Leftrightarrow xy \geq 0.$$

Is R reflexive? symmetric? transitive?

Problem 16.3
Let $A \neq \emptyset$ and $\mathcal{P}(A)$ be the power set of A. Consider the binary relation on $\mathcal{P}(A)$ defined as follows:

$$X, Y \in \mathcal{P}(A),\ X\ R\ Y \Leftrightarrow X \subseteq Y.$$

Is R reflexive? symmetric? transitive?

Problem 16.4
Let E be the binary relation on $\mathbb{Z}$ defined as follows:

$$a\ E\ b \Leftrightarrow m \equiv n\ (mod\ 2).$$

Show that E is an equivalence relation on $\mathbb{Z}$ and find the different equivalence classes.

Problem 16.5
Let I be the binary relation on $\mathbb{R}$ defined as follows:

$$a\ I\ b \Leftrightarrow a - b \in \mathbb{Z}.$$

Show that I is an equivalence relation on $\mathbb{R}$ and find the different equivalence classes.

Problem 16.6
Let A be the set all straight lines in the cartesian plane. Let $||$ be the binary relation on A defined as follows:

$$l_1||l_2 \Leftrightarrow l_1 \text{ is parallel to } l_2.$$

Show that $||$ is an equivalence relation on A and find the different equivalence classes.

Problem 16.7
Let $A = \mathbb{N} \times \mathbb{N}$. Define the binary relation R on A as follows:

$$(a, b)\ R\ (c, d) \Leftrightarrow a + d = b + c.$$

(a) Show that R is reflexive.
(b) Show that R is symmetric.
(c) Show that R is transitive.
(d) List five elements in $[(1, 1)]$.
(e) List five elements in $[(3, 1)]$.
(f) List five elements in $[(1, 2)]$.
(g) Describe the distinct equivalence classes of R.

Problem 16.8
Let R be a binary relation on a set A and suppose that R is symmetric and transitive. Prove the following: If for every $x \in A$ there is a $y \in A$ such that $x\ R\ y$ then R is reflexive and hence an equivalence relation on A.

Problem 16.9
Prove Theorem 16.1.

Problem 16.10
Let R and S be two equivalence relations on a non-empty set A. Show that $R \cap S$ is also an equivalence relation on A.

Problem 16.11
Let A be a set of 10 elements and let R be an equivalence relation on A. Suppose that $a, b, c \in A$ with $|[a]| = 3,\ |[b]| = 5$, and $|[c]| = 1$. . How many equivalence classes does A contain?

Problem 16.12
Define the relation R on $\mathbb{Z}$ by $a\ R\ b$ if and only id $2a + 5b \equiv 0 (\text{mod } 7)$. Show that R is an equivalence relation on $\mathbb{Z}$.

Problem 16.13
Consider the following relations on $\mathbb{Z}$. Explain why each is not an equivalence relation.
(a) $a\ R\ b$ if and only if $a^2 - b^2 \leq 7$.
(b) $a\ R\ b$ if and only if $a + b \equiv 0 (\text{mod } 5)$.
(c) $a\ R\ b$ if and only if $a^2 + b^2 = 0$.

Problem 16.14
Let $A = \{1, 2, 3, 4, 5\}$ and R be an equivalence relation on A given by

$$R = \{(1,1), (1,3), (1,4), (2,2), (2,5), (3,1), (3,3), (3,4), (4,1), (4,3), (4,4), (5,2), (5,5)\}.$$

Determine the equivalence classes of R.

Problem 16.15
Let R be the relation on $\mathbb{N} \times \mathbb{N}$ defined by $(a, b)\ R\ (c, d)$ if and only if $ad = bc$. Show that R is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.

Problem 16.16
Let R be the relation on $\mathbb{Z}$ defined by $x\ R\ y$ if and only if $x^2 = y^2$. Show that R is an equivalence relation. Find [4].

Problem 16.17
Let $A = \{a, b, c, d, e\}$. Suppose R is an equivalence relation on A. Suppose also that $a\ R\ d$ and $b\ R\ c, e\ R\ a$ and $c\ R\ e$. How many equivalence classes does R have?

Problem 16.18
Let R be the relation on $R \times \mathbb{R}$ defined by

$$(x_1, y_1)\ R\ (x_2, y_2) \Leftrightarrow x_1^2 + y_1^2 = x_2^2 + y_2^2.$$

Show that R is an equivalence relation and describe geometrically the equivalence classes of R.

Problem 16.19
Define a relation R on $\mathbb{R}$ by

$$a \ R \ b \Leftrightarrow |a| + |b| = |a + b|.$$

Show that R is reflexive, symmetric, but not transitive.

Problem 16.20
Let R be the relation on $\mathbb{R}$ defined by

$$a \ R \ b \Leftrightarrow a - b \in \mathbb{Z}.$$

Show that of $a \ R \ b$ and $c \ R \ d$ then $(a + c) \ R \ (b + d)$.

17 Partial Order Relations

A relation $\leq$ on a set A is called **a partial order** if $\leq$ is reflexive, antisymmetric, and transitive. In this case we call $(A, \leq)$ a **poset.**

Example 17.1
Show that the set $\mathbb{Z}$ of integers together with the relation of inequality $\leq$ is a poset.

Solution.
$\leq$ is reflexive: For all $x \in \mathbb{Z}$ we have $x \leq x$ since $x = x$.
$\leq$ is antisymmetric: By the trichotomy law of real numbers, for a given pair of numbers x and y only one of the following is true: $x < y, x = y$, or $x > y$. So if $x \leq y$ and $y \leq x$ then we must have $x = y$.
$\leq$ is transitive: If $x \leq y$ and $y \leq z$ then $x \leq z$ ■

Example 17.2
Show that the relation $a|b$ in $\mathbb{N} = \{1, 2, 3, \cdots\}$ is a partial order relation.

Solution.
Reflexivity: Since $a = 1 \cdot a$, we have $a|a$.
Antisymmetry: Suppose that $a|b$ and $b|a$. Then there exist positive integers k_1 and k_2 such that $b = k_1 a$ and $a = k_2 b$. Hence, $a = k_1 k_2 a$ which implies that $k_1 k_2 = 1$. Since $k_1, k_2 \in \mathbb{N}$, we must have $k_1 = k_2 = 1$; that is, $a = b$.
Transitivity: Suppose that $a|b$ and $b|c$. Then there exist positive integers k_1 and k_2 such that $b = k_1 a$ and $c = k_2 b$. Thus, $c = k_1 k_2 a$ which means that $a|c$ ■

Example 17.3
Let $\mathcal{P}(X)$ be the power set of X. Let R be the relation on $\mathcal{P}(X)$defined by

$$A \; R \; B \Leftrightarrow A \subseteq B.$$

Show that $\mathcal{P}(X)$ is a poset.

Solution.
$\subseteq$ is reflexive: For any set $A \in \mathcal{P}(X)$, $A \subseteq A$.
$\subseteq$ is antisymmetric: By the definition of $=$ of sets if $A \subseteq B$ and $B \subseteq A$ then $A = B$, where $A, B \in \mathcal{P}(X)$.

$\subseteq$ is transitive: We have seen in Example 13.1, that if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$ ■

Another simple pictorial representation of a partial order is the so called **Hasse diagram.** The Hasse diagram of a partial order on the set A is a drawing of the points of A and some of the arrows of the digraph of the order relation. We assume that the directed edges of the Hasse diagram point upward. There are rules to determine which arrows are drawn and which are omitted, namely,
• omit all arrows that can be inferred from transitivity
• omit all loops
• draw arrows without "heads".

Example 17.4
Let $A = \{1, 2, 3, 9, 18\}$ and the "divides" relation on A. Draw the Hasse diagram of this relation.

Solution.
The directed graph of the given relation and the cooresponding Hasse diagram are shown in Figure 17.1 ■

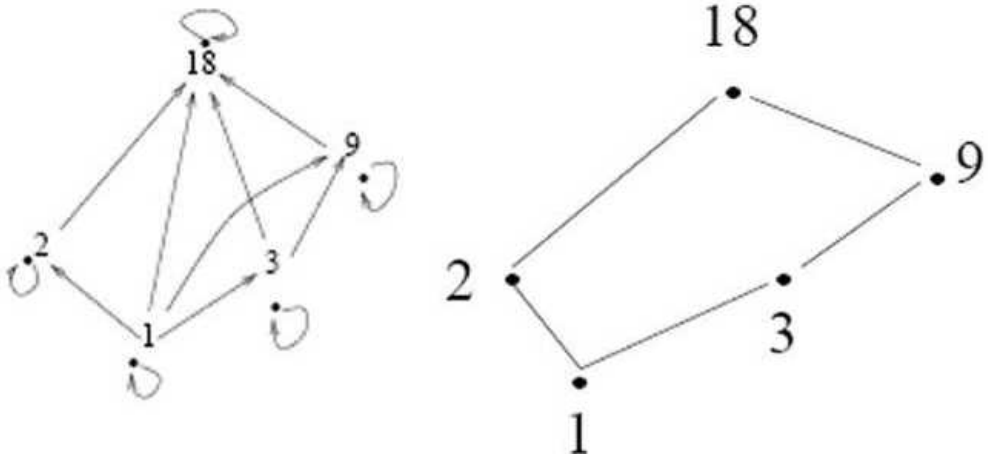


Figure 17.1

Now, given the Hasse diagram of a partial order relation one can find the digraph as follows:
• reinsert the direction markers on the arrows making all arrows point upward
• add loops at each vertex

• for each sequence of arrows from one point to a second point and from that second point to a third point, add an arrow from the first point to the third.

Example 17.5
Let $A = \{1, 2, 3, 4\}$ be a poset. Find the directed graph corresponding to the Hasse diagram on A shown in Figure 17.2.

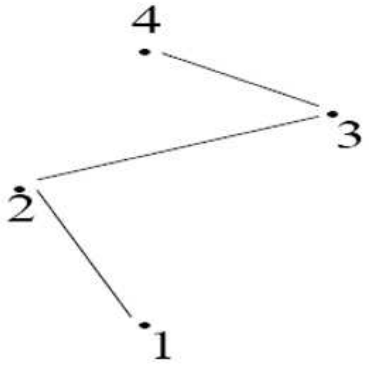


Figure 17.2

Solution.
The directed graph is shown in Figure 17.3 ■

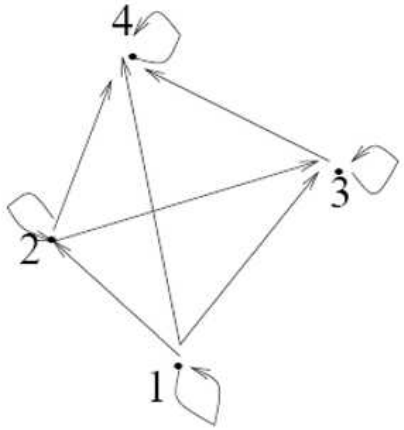


Figure 17.3

Next, if A is a poset then we say that a and b are **comparable** if either $a \leq b$ or $b \leq a$. If every pair of elements of A are comparable then we call $\leq$ a **total order**.

Example 17.6
Consider the "divides" relation defined on the set $A = \{5, 15, 30\}$. Prove that this relation is a total order on A.

Solution.
The fact that the "divides" relation is a partial order is easy to verify. Since $5|15, 5|30$, and $15|30$, any pair of elements in A are comparable. Thus, the "divides" relation is a total order on A ■

Example 17.7
Show that the "divides" relation on $\mathbb{N}$ is not a total order.

Solution.
A counterexample of two noncomparable numbers are 2 and 3, since 2 does not divide 3 and 3 does not divide 2 ■

Let $(A, \leq)$ be a poset. An element $a \in A$ is called a **least element** if and only if $a \leq b$ for all $b \in A$. Likewise, an element $b \in A$ is called a **greatest element** of A if and only if $a \leq b$ for all $a \in A$.

Example 17.8
(a) Find the least element of the poset $(\mathbb{N}, \leq)$.
(b) Find the least element and the greatest element of the poset $(\mathcal{P}(A), \subseteq)$ where $A = \{a, b\}$.

Solution.
(a) 1 is the least element of the poset $(\mathbb{N}, \leq)$.
(b) The empty set is the least element of the given poset whereas A is the greatest element ■

A partial order R on a set A is a **well order** if every non-empty subset of A has a least element.

Example 17.9
Show that $(\mathbb{N}, \leq)$ is well-ordered.

Solution.
This is true because every non-empty subset of natural numbers has a least element (See Theorem 10.1) ■

Review Problems

Problem 17.1
Define a relation R on $\mathbb{Z}$ as follows: for all $m, n \in \mathbb{Z}$

$$m \ R \ n \Leftrightarrow m + n \ is \ even.$$

Is R a partial order? Prove or give a counterexample.

Problem 17.2
Define a relation R on $\mathbb{R}$ as follows: for all $m, n \in \mathbb{R}$

$$m \ R \ n \Leftrightarrow m^2 \leq n^2.$$

Is R a partial order? Prove or give a counterexample.

Problem 17.3
Let $S = \{0, 1\}$ and consider the partial order relation R defined on $S \times S$ as follows: for all ordered pairs (a, b) and (c, d) in $S \times S$

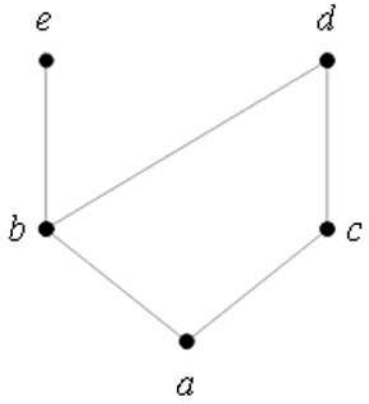
$$(a, b) \ R \ (c, d) \Leftrightarrow a \leq c \ and \ b \leq d.$$

Draw the Hasse diagram for R.

Problem 17.4
Consider the "divides" relation defined on the set $A = \{1, 2, 2^2, \cdots, 2^n\}$, where n is a nonnegative integer.
a. Prove that this relation is a total order on A.
b. Draw the Hasse diagram for this relation when $n = 3$.

Problem 17.5
Let R be a partial order on A. Show that R^{-1} is also a partial order on A.

Problem 17.6
An order relation R is given by the following Hasse diagram. Find the corresponding digraph.



Problem 17.7
Let $\mathcal{F}$ be a collection of finite sets. On this set, we define the relation R by

$$A \ R \ B \Leftrightarrow |A| \leq |B|.$$

Show that R is reflexive, transitive but is neither anti-symmetric nor symmetric.

Problem 17.8
Let $A = \mathbb{N} \times \mathbb{N}$ and define R on A by

$$(a, b)R(c, d) \Leftrightarrow a \leq c \text{ and } b \geq d.$$

Show that (A, R) is a poset.

Problem 17.9
Let $A = \{a, b, c\}$ and consider the poset $(\mathcal{P}(A), \subseteq)$. Let $S = \{\{a\}, \{a, c\}, \{a, b\}\}$. Find the least element and the greatest element of S.

Problem 17.10
Show that the relation $\leq$ on $\mathbb{Z}$ is not well-ordered.

Problem 17.11
Show that if A is well-ordered under $\leq$ then $\leq$ is a total order on A.

Problem 17.12
Suppose that $(A, \leq)$ is a poset and S is a non-empty subset of A. If S has a least element then this element is unique.

Problem 17.13
Let R be thr relation on $\mathbb{Z} \times \mathbb{Z}$ defined by

$$(a, b)R(c, d) \Leftrightarrow \text{either } a < c \text{ or } (a = c \text{ and } b \leq d).$$

This relation is known as the **dictionary order**. Show that R is a total order.

Problem 17.14
Define the relation R on $\mathbb{R}$ by

$$aRb \Leftrightarrow a^3 - 4a \leq b^3 - 4b.$$

Determine whether or not $(\mathbb{R}, R)$ is a poset.

Problem 17.15
Let $A = \{a, b, c, d\}$ and consider the poset $(\mathcal{P}(A), \subseteq)$. Draw the Hasse diagram of this relation.

Problem 17.16
Let A be a non-empty set with $|A| \geq 2$. Show that $\mathcal{P}(A)$ is not a total order under the relation of $\subseteq$.

Problem 17.17
Let R be the relation on $\mathcal{P}(U)$ defined by

$$ARB \Leftrightarrow A \cap B = A.$$

Show that R is reflexive and antisymmetric.

Problem 17.18
Let R be a relation on A. Show that if R is symmetric and transitive then it is an equivalence relation on A.

Problem 17.19
Draw the Hasse diagram for the partial order "divides" on the set A consisting of all the natural numbers less than or equal to 12.

Problem 17.20
Show that the set of positive real numbers is not well-ordered.

18 Bijective and Inverse Functions

Let $f : A \to B$ be a function. We say that f is **injective** or **one-to-one** if and only if for all $x, y \in A$, if $f(x) = f(y)$ then $x = y$. Using the concept of contrapositive, a function f is injective if and only if for all $x, y \in A$, if $x \neq y$ then $f(x) \neq f(y)$. Taking the negation of this last conditional implication we see that f is not injective if and only if there exist two distinct elements a and b of A such that $f(a) = f(b)$ (Example 3.3).

Example 18.1
(a) Show that the identity function I_A on a set A is injective.
(b) Show that the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n^2$ is not injective.

Solution.
(a) Let $x, y \in A$. If $I_A(x) = I_A(y)$ then $x = y$ by the definition of I_A. This shows that I_A is injective.
(b) Since $1^2 = (-1)^2$ and $1 \neq -1$, f is not injective ■

Example 18.2
Show that if $f : \mathbb{R} \to \mathbb{R}$ is increasing then f is one-to-one.

Solution.
Suppose that $x_1 \neq x_2$. Then without loss of generality we can assume that $x_1 < x_2$. Since f is increasing, $f(x_1) < f(x_2)$. That is, $f(x_1) \neq f(x_2)$. Hence, f is one-to-one ■

Example 18.3
Show that the composition of two injective functions is also injective.

Solution.
Let $f : A \to B$ and $g : B \to C$ be two injective functions. We will show that $g \circ f : A \to C$ is also injective. Indeed, suppose that $(g \circ f)(x_1) = (g \circ f)(x_2)$ for $x_1, x_2 \in A$. Then $g(f(x_1)) = g(f(x_2))$. Since g is injective, $f(x_1) = f(x_2)$. Now, since f is injective, $x_1 = x_2$. This completes the proof that $g \circ f$ is injective ■

Now, for any function $f : A \to B$ we have $Range(f) \subseteq B$. If equality holds then we say that f is **surjective** or **onto.** It follows from this definition that a function f is surjective if and only if for each $y \in B$ there is an $x \in A$ such that $f(x) = y$. By taking the negation of this we see that f is not onto if there is a $y \in B$ such that $f(x) \neq y$ for all $x \in A$.

Example 18.4
(a) Show that the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 3x - 5$ is surjective.
(b) Show that the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = 3n - 5$ is not surjective.

Solution.
(a) Let $y \in \mathbb{R}$. Is there an $x \in \mathbb{R}$ such that $f(x) = y$? That is, $3x - 5 = y$. But solving for x we find $x = \frac{y+5}{3} \in \mathbb{R}$ and $f(x) = y$. Thus, f is onto.
(b) Take $m = 3$. If f is onto then there should be an $n \in \mathbb{Z}$ such that $f(n) = 3$. That is, $3n - 5 = 3$. Solving for n we find $n = \frac{8}{3}$ which is not an integer. Hence, f is not onto ■

Example 18.5 *(Projection Functions)*
Let A and B be two nonempty sets. The functions $pr_A : A \times B \to A$ defined by $pr_A(a, b) = a$ and $pr_B : A \times B \to B$ defined by $pr_B(a, b) = b$ are called **projection** functions. Show that pr_A and pr_B are surjective functions.

Solution.
We prove that pr_A is surjective. Indeed, let $a \in A$. Since B is not empty, there is a $b \in B$. But then $(a, b) \in A \times B$ and $pr_A(a, b) = a$. Hence, pr_A is surjective. The proof that pr_B is surjective is similar ■

Example 18.6
Show that the composition of two surjective functions is also surjective.

Solution.
Let $f : A \to B$ and $g : B \to C$, where $Range(f) \subseteq C$, be two surjective functions. We will show that $g \circ f : A \to C$ is also surjective. Indeed, let $z \in C$. Since g is surjective, there is a $y \in B$ such that $g(y) = z$. Since f is surjective, there is an $x \in A$ such that $f(x) = y$. Thus, $g(f(x)) = z$. This shows that $g \circ f$ is surjective ■

Now, we say that a function f is **bijective** or **one-to-one correspondence** if and only if f is both injective and surjective. A bijective function on a set A is called a **permutation.**

Example 18.7
(a) Show that the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 3x - 5$ is a bijective function.
(b) Show that the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is not bijective.

Solution.
(a) First we show that f is injective. Indeed, suppose that $f(x_1) = f(x_2)$. Then $3x_1 - 5 = 3x_2 - 5$ and this implies that $x_1 = x_2$. Hence, f is injective. f is surjective by Example 18.4 (a).
(b) f is not injective since $f(-1) = f(1)$ but $-1 \neq 1$. Hence, f is not bijective ■

Example 18.8
Show that the composition of two bijective functions is also bijective.

Solution.
This follows from Example 18.3 and Example 18.6 ■

Theorem 18.1
Let $f : X \to Y$ be a bijective function. Then there is a function $f^{-1} : Y \to X$ with the following properties:

(a) $f^{-1}(y) = x$ if and only if $f(x) = y$.
(b) $f^{-1} \circ f = I_X$ and $f \circ f^{-1} = I_Y$ where I_X denotes the identity function on X.
(c) f^{-1} is bijective.

Proof.
For each $y \in Y$ there is a unique $x \in X$ such that $f(x) = y$ since f is bijective. Thus, we can define a function $f^{-1} : Y \to X$ by $f^{-1}(y) = x$ where $f(x) = y$.
(a) Follows from the definition of f^{-1}.
(b) Indeed, let $x \in X$ such that $f(x) = y$. Then $f^{-1}(y) = x$ and $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(y) = x = I_X(x)$. Since x was arbitrary, $f^{-1} \circ f = I_X$. The proof that $f \circ f^{-1} = I_Y$ is similar.
(c) We show first that f^{-1} is injective. Indeed, suppose $f^{-1}(y_1) = f^{-1}(y_2)$. Then $f(f^{-1}(y_1)) = f(f^{-1}(y_2))$; that is, $(f \circ f^{-1})(y_1) = (f \circ f^{-1})(y_2)$. By b. we have $I_Y(y_1) = I_Y(y_2)$. From the definition of I_Y we obtain $y_1 = y_2$. Hence, f^{-1} is injective. We next show that f^{-1} is surjective. Indeed, let $y \in Y$. Since f is onto, there is a unique $x \in X$ such that $f(x) = y$. By the definition of f^{-1}, $f^{-1}(y) = x$. Thus, for every element $y \in Y$ there is an element $x \in X$ such that $f^{-1}(y) = x$. This says that f^{-1} is surjective and completes a proof of the theorem ■

Example 18.9
Show that $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 3x - 5$ is bijective and find a formula for its inverse function.

Solution.
We have already proved that f is bijective. We will just find the formula for its inverse function f^{-1}. Indeed, if $y \in Y$ we want to find $x \in X$ such that $f^{-1}(y) = x$, or equivalently, $f(x) = y$. This implies that $3x - 5 = y$ and solving for x we find $x = \frac{y+5}{3}$. Thus, $f^{-1}(y) = \frac{y+5}{3}$ ■

Review Problems

Problem 18.1
(a) Define $g : \mathbb{Z} \to \mathbb{Z}$ by $g(n) = 3n - 2$.
(i) Is g one-to-one? Prove or give a counterexample.
(ii) Is g onto? Prove or give a counterexample.
(b) Define $G : \mathbb{R} \to \mathbb{R}$ by $G(x) = 3x - 2$. Is G onto? Prove or give a counterexample.

Problem 18.2
Determine whether the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \frac{x+1}{x}$ is one-to-one or not.

Problem 18.3
Determine whether the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \frac{x}{x^2+1}$ is one-to-one or not.

Problem 18.4
Let $f : \mathbb{R} \to \mathbb{Z}$ be the floor function $f(x) = \lfloor x \rfloor$.
(a) Is f one-to-one? Prove or give a counterexample.
(b) Is f onto? Prove or give a counterexample.

Problem 18.5
If $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ are one-to-one functions, is $f+g$ also one-to-one? Justify your answer.

Problem 18.6
Define $F : \mathcal{P}\{a, b, c\} \to \mathbb{N}$ to be the number of elements of a subset of $\{a, b, c\}$.
(a) Is F one-to-one? Prove or give a counterexample.
(b) Is F onto? Prove or give a counterexample.

Problem 18.7
If $f : \mathbb{Z} \to \mathbb{Z}$ and $g : \mathbb{Z} \to \mathbb{Z}$ are onto functions, is $f + g$ also onto? Justify your answer.

Problem 18.8
Show that the function $F^{-1} : \mathbb{R} \to \mathbb{R}$ given by $F^{-1}(y) = \frac{y-2}{3}$ is the inverse of the function $F(x) = 3x + 2$.

Problem 18.9
If $f : X \to Y$ and $g : Y \to Z$ are functions and $g \circ f : X \to Z$ is one-to-one, must both f and g be one-to-one? Prove or give a counterexample.

Problem 18.10
If $f : X \to Y$ and $g : Y \to Z$ are functions and $g \circ f : X \to Z$ is onto, must both f and g be onto? Prove or give a counterexample.

Problem 18.11
If $f : X \to Y$ and $g : Y \to Z$ are functions and $g \circ f : X \to Z$ is one-to-one, must f be one-to-one? Prove or give a counterexample.

Problem 18.12
If $f : X \to Y$ and $g : Y \to Z$ are functions and $g \circ f : X \to Z$ is onto, must g be onto? Prove or give a counterexample.

Problem 18.13
Let $f : W \to X, g : X \to Y$ and $h : Y \to Z$ be functions. Must $h \circ (g \circ f) = (h \circ g) \circ f$? Prove or give a counterexample.

Problem 18.14
Let $f : X \to Y$ and $g : Y \to Z$ be two bijective functions. Show that $(g \circ f)^{-1}$ exists and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Problem 18.15
(a) Compare $|A|$ and $|B|$ when $f : A \to B$ is one-to-one.
(b) Compare $|A|$ and $|B|$ when $f : A \to B$ is onto.
(c) Compare $|A|$ and $|B|$ when $f : A \to B$ is one-to-one correspondence.

Problem 18.16
Let $f : A \to B$ be a function. Define the relation R on A by

$$aRB \Leftrightarrow f(a) = f(b).$$

(a) Show that R is an equivalence relation.
(b) Show that the function $F : A/R \to \text{Range}(f)$ defined by $F([a]) = f(a)$ is one-to-one correspondence.

Problem 18.17
Let $A = B = \{1, 2, 3\}$. Consider the function $f = \{(1, 2), (2, 3), (3, 3)\}$. Is f injective? Is f surjective?

Problem 18.18
Show that $f : \mathbb{Z} \to \mathbb{N}$ defined by $f(x) = |x| + 1$ is onto but not one-to-one.

Problem 18.19
Let $f : A \to B$. For any subset C of B we define $f^{-1}(C) = \{a \in A : f(a) \in C\}$. Show that $f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T)$ where $S, T \subseteq B$.

Problem 18.20
Find the inverse of the function $f(x) = \frac{x+1}{3x+2}$.

19 The Pigeonhole Principle

The **Pigeonhole principle** asserts that if n pigeons fly into k holes with $n > k$ then some of the pigeonholes contain at least two pigeons. The reason this statement is true can be seen by arguing by contradiction. If the conclusion is false, each pigeonhole contains at most one pigeon and, in this case, we can account for at most k pigeons. Since there are more pigeons than holes, we have a contradiction.
In problem solving, the "pigeons" are often numbers or objects, and the "pigeonholes" are properties that the numbers/objects might possess.

Example 19.1
Ten persons have first names George, William, and Laura and last names Moe, Carineo, and Barber. Show that at least two persons have the same first and last names.

Solution.
The pigeons are the ten persons and a hole is an ordered pair (First Name, Last Name). Since there are at most nine holes, according to the pigeonhole principle there exist at least two persons with the same first and last name ■

Generalized Pigeonhole Principle: If n pigeons fly into k holes with $n > k$, then there is at least one pigeonhole with at least $\lceil \frac{n}{k} \rceil$ pigeons.

A mathematical way to formulate the Generalized Pigeonhole Principle is given by the following thoerem.

Theorem 19.1
Let S be a finite set and $\{A_1, A_2, \cdots, A_k\}$ be a partition of S with $|S| > k$. There is an index $1 \leq i \leq k$ such that $|A_i| \geq \left\lceil \frac{|S|}{k} \right\rceil$.

Proof.
The proof is by contradiction. Suppose that $|A_i| < \left\lceil \frac{|S|}{k} \right\rceil$ for all $1 \leq i \leq k$. Then $|A_i| \leq \left\lceil \frac{|S|}{k} \right\rceil - 1$ for all $1 \leq i \leq k$. Since $\{A_1, A_2, \cdots, A_k\}$ is a partition

of S, we have

$$\begin{aligned}|S| &= |A_1| + |A_2| + \cdots + |A_k| \\ &\leq \left(\left\lceil \frac{|S|}{k} \right\rceil - 1\right) + \left(\left\lceil \frac{|S|}{k} \right\rceil - 1\right) + \cdots + \left(\left\lceil \frac{|S|}{k} \right\rceil - 1\right) \\ &= k\left(\left\lceil \frac{|S|}{k} \right\rceil - 1\right) < k\left(\frac{|S|}{k} + 1 - 1\right) = |S|\end{aligned}$$

and this is a contradiction ■

Example 19.2
Let S and T be two finite sets such that $|S| > k|T|$ where k is a positive integer. Show that for any function $f : S \to T$ there is a $t \in T$ such that the set $A_t = \{s \in S : f(s) = t\}$ has more than k elements.

Solution.
For each $t \in T$ the set A_t is a subset of S. Moreover, if t_1 and t_2 are two different elements of T and $s \in A_{t_1} \cap A_{t_2}$ then $f(s) = t_1$ and $f(s) = t_2$ and this contradicts the definition of a function. Hence, $A_{t_1} \cap A_{t_2} = \emptyset$. Finally, if $s \in S$ then $f(s) = t \in T$ so that $s \in A_t$. Hence, $S = \cup_{t\in T} A_t$. It follows that $\{A_t\}_{t\in T}$ is a partition of S. By Theorem 19.1, there is a $t \in T$ such that$|A_t| \geq \frac{|S|}{|T|} > k$. That is, A_t has at least k elements ■

As a consequence of the above example, we have

Example 19.3
If S and T are finite sets such that $|S| > |T|$ then any function $f : S \to T$ is not one-to-one.

Solution.
Let $k = 1$ in the previous problem. Then there is a set $\{s \in S : f(s) = t\}$ with more than one element. Say, s_1, s_2 are such that $f(s_1) = f(s_2) = t$ with $s_1 \neq s_2$. But this says that f is not one-to-one ■

Review Problems

Problem 19.1
A family has 10 children. Show that at least two children were born on the same day of the week.

Problem 19.2
Show that if 11 people take an elevator in a 10-story building then at least two people exist the elevator on the same floor.

Problem 19.3
A class of 11 students wrote a short essay. George Perry made 9 errors, each of the other students made less than that number. Prove that at least two students made equal number of errors.

Problem 19.4
Let $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Prove that if five integers are selected from A, then at least one pair of integers have a sum of 9.

Problem 19.5
Prove that, given any 12 natural numbers, we can chose two of them and such that their difference is divisible by 11.

Problem 19.6
In a group of 1500, find the least number of people who share the same birthday.

Problem 19.7
Suppose that every student in aclass 18 flipped a coin four times. Show that at least two students would have the exact same sequence of heads and tails.

Problem 19.8
Show that mong any N positive integers, there exists 2 whose difference is divisible by $N - 1$.

Problem 19.9
Given any six integers between 1 and 10, inclusive, show that 2 of them have an odd sum.

Problem 19.10
Show that among any 13 people, at least two share a birth month.

Problem 19.11
Suppose that more than kn marbles are distributed over n jars. Show that one jar will contain at least $k + 1$ marbles.

Problem 19.12
Use the generalized pigeonhole principle to show that among 85 people, at least 4 must have the same last initial.

Problem 19.13
How many students must be in a class to guarantee that at least two students receive the same score on the final exam, if the exam is graded on a scale from 0 to 100 points.

Problem 19.14
Show that for any given N positive integers, the sum of some of these integers (perhaps one of the numbers itself) is divisible by N.

Problem 19.15
If there are 6 people at a party, then show that either 3 of them knew each other before the party or 3 of them were complete strangers before the party.

Problem 19.16
How many cards must be selected from a standard deck of 52 cards to ensure that we get at least 3 cards of the same suit?

Problem 19.17
Suppose we have 27 different odd positive integers all less than 100. Show that there is a pair of numbers whose sum is 102.

Problem 19.18
Among 100 people, at least how many people were born in the same month?

Problem 19.19
Show that an arbitrary subset A of $n + 1$ integers from the set $\{1, \cdots, 2n\}$ will contain a pair of consecutive integers.

Problem 19.20
Fifteen children together gathered 100 nuts. Prove that some pair of children gathered the same number of nuts. Hint: Use the method of proof by contradiction.

20 Recursion

A **recurrence relation** for a sequence $a_0, a_1, \cdots$ is a relation that defines a_n in terms of $a_0, a_1, \cdots, a_{n-1}$. The formula relating a_n to earlier values in the sequence is called the **generating rule**. The assignment of a value to one of the a's is called an **initial condition**.

Example 20.1
The **Fibonacci** sequence

$$1, 1, 2, 3, 5, \cdots$$

is a sequence in which every number after the first two is the sum of the preceding two numbers. Find the generating rule and the initial conditions.

Solution.
The initial conditions are $a_0 = a_1 = 1$ and the generating rule is $a_n = a_{n-1} + a_{n-2}, n \geq 2$ ■

A **solution** to a recurrence relation is an explicit formula for a_n in terms of n.
The most basic method for finding the solution of a sequence defined recursively is by using **iteration.** The iteration method consists of starting with the initial values of the sequence and then calculate successive terms of the sequence until a pattern is observed. At that point one guesses an explicit formula for the sequence and then uses mathematical induction to prove its validity.

Example 20.2
Consider the **arithmetic sequence**

$$a_n = a_{n-1} + d, \quad n \geq 1$$

where a_0 is the initial value. Find an explicit formula for a_n.

Solution.
Listing the first four terms of the sequence after a_0 we find

$$\begin{aligned} a_1 &= a_0 + d \\ a_2 &= a_0 + 2d \\ a_3 &= a_0 + 3d \\ a_4 &= a_0 + 4d. \end{aligned}$$

Hence, a guess is $a_n = a_0 + nd$. Next, we prove the validity of this formula by induction:
Basis of induction: For $n = 0, a_0 = a_0 + (0)d$.
Induction hypothesis: Suppose that $a_n = a_0 + nd$.
Induction step: We must show that $a_{n+1} = a_0 + (n+1)d$. By the definition of a_{n+1}, we have $a_{n+1} = a_n + d = a_0 + nd + d = a_0 + (n+1)d$ ■

Example 20.3
Consider the **geometric sequence**

$$a_n = ra_{n-1}, \quad n \geq 1$$

where a_0 is the initial value. Find an explicit formula for a_n.

Solution.
Listing the first four terms of the sequence after a_0 we find

$$\begin{aligned} a_1 &= ra_0 \\ a_2 &= r^2 a_0 \\ a_3 &= r^3 a_0 \\ a_4 &= r^4 a_0. \end{aligned}$$

Hence, a guess is $a_n = r^n a_0$. Next, we prove the validity of this formula by induction.
Basis of induction: For $n = 0, a_0 = r^0 a_0$.
Induction hypothesis: Suppose that $a_n = r^n a_0$.
Induction step: We must show that $a_{n+1} = r^{n+1} a_0$. By the definition of a_{n+1} we have $a_{n+1} = ra_n = r(r^n a_0) = r^{n+1} a_0$ ■

When an iteration does not apply, other methods are available for finding explicit formulas for special classes of recursively defined sequences. The method explained below works for sequences of the form

$$a_n = Aa_{n-1} + Ba_{n-2} \tag{20.1}$$

where n is greater than or equal to some fixed nonnegative integer k and A and B are real numbers with $B \neq 0$. Such an equation is called a **second-order linear homogeneous recurrence relation with constant coefficients**.

Example 20.4
Does the Fibonacci sequence satisfy a second-order linear homogeneous relation with constant coefficients?

Solution.
Recall that the Fibonacci sequence is defined recursively by $a_n = a_{n-1} + a_{n-2}$ for $n \geq 2$ and $a_0 = a_1 = 1$. Thus, a_n satisfies a second-order linear homogeneous relation with $A = B = 1$ ■

The following theorem gives a technique for finding solutions to (20.1).

Theorem 20.1
Equation (20.1) is satisfied by the sequence $1, t, t^2, \cdots, t^n, \cdots$ where $t \neq 0$ if and only if t is a solution to the **characteristic equation**

$$t^2 - At - B = 0. \tag{20.2}$$

Proof.
($\Longrightarrow$): Suppose that t is a nonzero real number such that the sequence $1, t, t^2, \cdots$ satisfies (20.1). We will show that t satisfies the equation $t^2 - At - B = 0$. Indeed, for $n \geq k$ we have

$$t^n = At^{n-1} + Bt^{n-2}.$$

Since $t \neq 0$ we can divide through by t^{n-2} and obtain $t^2 - At - B = 0$.
($\Longleftarrow$) : Suppose that t is a nonzero real number such that $t^2 - At - B = 0$. Multiply both sides of this equation by t^{n-2} to obtain

$$t^n = At^{n-1} + Bt^{n-2}.$$

This says that the sequence $1, t, t^2, \cdots$ satisfies (20.1) ■

Example 20.5
Consider the recurrence relation

$$a_n = a_{n-1} + 2a_{n-2}, \quad n \geq 2.$$

Find two sequences that satisfy the given generating rule and have the form $1, t, t^2, \cdots$.

Solution.
According to the previous theorem t must satisfy the characteristic equation

$$t^2 - t - 2 = 0.$$

Solving for t we find $t = 2$ or $t = -1$. So the two solutions to the given recurrence sequence are $\{1, 2, 2^2, \cdots, 2^n, \cdots\}$ and $\{1, -1, \cdots, (-1)^n, \cdots\}$ ■

Are there other solutions than the ones provided by Theorem 20.1? The answer is yes according to the following theorem.

Theorem 20.2
If s_n and t_n are solutions to (20.1) then for any real numbers C and D the sequence

$$a_n = Cs_n + Dt_n, \quad n \geq 0$$

is also a solution.

Proof.
Since s_n and t_n are solutions to (20.1), for $n \geq 2$ we have

$$\begin{aligned} s_n =& As_{n-1} + Bs_{n-2} \\ t_n =& At_{n-1} + Bt_{n-2}. \end{aligned}$$

Therefore,

$$\begin{aligned} Aa_{n-1} + Ba_{n-2} =& A(Cs_{n-1} + Dt_{n-1}) + B(Cs_{n-2} + Dt_{n-2}) \\ =& C(As_{n-1} + Bs_{n-2}) + D(At_{n-1} + Bt_{n-2}) \\ =& Cs_n + Dt_n = a_n \end{aligned}$$

so that a_n satisfies (20.1) ■

Example 20.6
Find a solution to the recurrence relation

$$\begin{aligned} a_0 =& 1, a_1 = 8 \\ a_n =& a_{n-1} + 2a_{n-2}, \quad n \geq 2. \end{aligned}$$

Solution.
By the previous theorem and Example 20.5, $a_n = C2^n + D(-1)^n,\ n \geq 2$ is a solution to the recurrence relation

$$a_n = a_{n-1} + 2a_{n-2}.$$

If a_n satisfies the system then we must have

$$\begin{aligned} a_0 &= C2^0 + D(-1)^0 \\ a_1 &= C2^1 + D(-1)^1. \end{aligned}$$

This yields the system

$$\begin{cases} C + D &= 1 \\ 2C - D &= 8. \end{cases}$$

Solving this system to find $C = 3$ and $D = -2$. Hence, $a_n = 3 \cdot 2^n - 2(-1)^n$ ■

Next, we discuss the case when the characteristic equation has a single root.

Theorem 20.3
Let A and B be real numbers and suppose that the characteristic equation

$$t^2 - At - B = 0$$

has a single root r. Then the sequences $\{1, r, r^2, \cdots\}$ and $\{0, r, 2r^2, 3r^3, \cdots, nr^n, \cdots\}$ both satisfy the recurrence relation

$$a_n = Aa_{n-1} + Ba_{n-2}.$$

Proof.
Since r is a root to the characteristic equation, the sequence $\{1, r, r^2, \cdots\}$ is a solution to the recurrence relation

$$a_n = Aa_{n-1} + Ba_{n-2}.$$

Now, since r is the only solution to the characteristic equation we have

$$(t - r)^2 = t^2 - At - B.$$

This implies that $A = 2r$ and $B = -r^2$. Let $s_n = nr^n,\ \ n \geq 0$. Then

$$\begin{aligned} As_{n-1} + Bs_{n-2} =& A(n-1)r^{n-1} + B(n-2)r^{n-2} \\ =& 2r(n-1)r^{n-1} - r^2(n-2)r^{n-2} \\ =& 2(n-1)r^n - (n-2)r^n \\ =& nr^n = s_n \end{aligned}$$

So s_n is a solution to $a_n = Aa_{n-1} + Ba_{n-2}$. ■

Example 20.7
Find an explicit formula for

$$\begin{aligned} a_0 =& 1, a_1 = 3 \\ a_n =& 4a_{n-1} - 4a_{n-2}, \quad n \geq 2 \end{aligned}$$

Solution.
Solving the characteristic equation

$$t^2 - 4t + 4 = 0$$

we find the single root $r = 2$. Thus,

$$a_n = C2^n + Dn2^n$$

is a solution to the equation $a_n = 4a_{n-1} - 4a_{n-2}$. Since $a_0 = 1$ and $a_1 = 3$, we obtain the following system of equations:

$$\begin{aligned} C =& 1 \\ 2C + 2D =& 3 \end{aligned}$$

Solving this system to obtain $C = 1$ and $D = \frac{1}{2}$. Hence, $a_n = 2^n + \frac{n}{2}2^n$ ■

Example 20.8
A function is said to be defined **recursively** or to be a **recursive function** if its rule of definition refers to itself. Define the factorial function recursively.

Solution.
We have

$$\begin{aligned} f(0) =& 1 \\ f(n) =& nf(n-1), \quad n \geq 1 \end{aligned}$$ ■

Example 20.9
Let $G : \mathbb{N} \to \mathbb{Z}$ be the relation given by

$$G(n) = \begin{cases} 1, & \text{if } n = 1 \\ 1 + G(\frac{n}{2}), & \text{if n is even} \\ G(3n-1), & \text{if } n > 1 \text{ is odd.} \end{cases}$$

Show that G is not a function.

Solution.
Assume that G is a function so that $G(5)$ exists. Listing the first five values of G we find

$$\begin{aligned}
G(1) =& 1\\
G(2) =& 2\\
G(3) =& G(8) = 1 + G(4) = 2 + G(2) = 4\\
G(4) =& 1 + G(2) = 3\\
G(5) =& G(14) = 1 + G(7)\\
=& 1 + G(20)\\
=& 2 + G(10)\\
=& 3 + G(5)
\end{aligned}$$

But the last equality implies that $0 = 3$ which is impossible. Hence, G does not define a function. ■

Review Problems

Problem 20.1
Find the first four terms of the following recursively defined sequence:

$$\begin{aligned} v_1 =& 1, v_2 = 2 \\ v_n =& v_{n-1} + v_{n-2} + 1, \quad n \geq 3. \end{aligned}$$

Problem 20.2
Prove each of the following for the Fibonacci sequence:
(a) $F_k^2 - F_{k-1}^2 = F_k F_{k+1} - F_{k+1} F_{k-1}, \quad k \geq 1.$
(b) $F_{k+1}^2 - F_k^2 - F_{k-1}^2 = 2F_k F_{k-1}, \quad k \geq 1.$
(c) $F_{k+1}^2 - F_k^2 = F_{k-1} F_{k+2}, \quad k \leq 1.$
(d) $F_{n+2} F_n - F_{n+1}^2 = (-1)^n$ for all $n \geq 0.$

Problem 20.3
Find $\lim_{n\to\infty} \frac{F_{n+1}}{F_n}$ where $F_0, F_1, F_2, \cdots$ is the Fibonacci sequence. (Assume that the limit exists.)

Problem 20.4
Define $x_0, x_1, x_2, \cdots$ as follows:

$$x_n = \sqrt{2 + x_{n-1}}, \quad x_0 = 0.$$

Find $\lim_{n\to\infty} x_n$.

Problem 20.5
Find a formula for each of the following sums:
(a) $1 + 2 + \cdots + (n-1), \quad n \geq 2.$
(b) $3 + 2 + 4 + 6 + 8 + \cdots + 2n, \quad n \geq 1.$
(c) $3 \cdot 1 + 3 \cdot 2 + 3 \cdot 3 + \cdots 3 \cdot n, \quad n \geq 1.$

Problem 20.6
Find a formula for each of the following sums:
(a) $1 + 2 + 2^2 + \cdots + 2^{n-1}, \quad n \geq 1.$
(b) $3^{n-1} + 3^{n-2} + \cdots + 3^2 + 3 + 1, \quad n \geq 1.$
(c) $2^n + 3 \cdot 2^{n-2} + 3 \cdot 2^{n-3} + \cdots + 3 \cdot 2^2 + 3 \cdot 2 + 3, \quad n \geq 1.$
(d) $2^n - 2^{n-1} + 2^{n-2} - 2^{n-3} + \cdots + (-1)^{n-1} \cdot 2 + (-1)^n, \quad n \geq 1.$

Problem 20.7
Use iteration to guess a formula for the following recursively defined sequence and then use mathematical induction to prove the validity of your formula: $c_1 = 1, c_n = 3c_{n-1} + 1$, for all $n \geq 2$.

Problem 20.8
Use iteration to guess a formula for the following recursively defined sequence and then use mathematical induction to prove the validity of your formula: $w_0 = 1, w_n = 2^n - w_{n-1}$, for all $n \geq 2$.

Problem 20.9
Determine whether the recursively defined sequence: $a_1 = 0$ and $a_n = 2a_{n-1} + n - 1$ satisfies the recursive formula $a_n = (n-1)^2,\ n \geq 1$.

Problem 20.10
Which of the following are second-order homogeneous recurrence relations with constant coefficients?
(a) $a_n = 2a_{n-1} - 5a_{n-2}$.
(b) $b_n = nb_{n-1} + b_{n-2}$.
(c) $c_n = 3c_{n-1} \cdot c_{n-2}^2$.
(d) $d_n = 3d_{n-1} + d_{n-2}$.
(e) $r_n = r_{n-1} - r_{n-2} - 2$.
(f) $s_n = 10s_{n-2}$.

Problem 20.11
Let $a_0, a_1, a_2, \cdots$ be the sequence defined by the recursive formula

$$a_n = C \cdot 2^n + D, \quad n \geq 0$$

where C and D are real numbers.
(a) Find C and D so that $a_0 = 1$ and $a_1 = 3$. What is a_2 in this case?
(b) Find C and D so that $a_0 = 0$ and $a_1 = 2$. What is a_2 in this case?

Problem 20.12

Let $a_0, a_1, a_2, \cdots$ be the sequence defined by the recursive formula

$$a_n = C \cdot 2^n + D, \quad n \geq 0$$

where C and D are real numbers. Show that for any choice of C and D,

$$a_n = 3a_{n-1} - 2a_{n-2}, \quad n \geq 2.$$

Problem 20.13
Let $a_0, a_1, a_2, \cdots$ be the sequence defined by the recursive formula

$$\begin{aligned} a_0 =& 1, a_1 = 2 \\ a_n =& 2a_{n-1} + 3a_{n-2}, \quad n \geq 2. \end{aligned}$$

Find an explicit formula for the sequence.

Problem 20.14
Let $a_0, a_1, a_2, \cdots$ be the sequence defined by the recursive formula

$$\begin{aligned} a_0 =& 1, a_1 = 4 \\ a_n =& 2a_{n-1} - a_{n-2}, \quad n \geq 2. \end{aligned}$$

Find an explicit formula for the sequence.

Problem 20.15
Show that the relation $F : \mathbb{N} \to \mathbb{Z}$ given by the rule

$$F(n) = \begin{cases} 1 & \text{if } n = 1. \\ F(\frac{n}{2}) & \text{if n is even} \\ 1 - F(5n-9) & \text{if } n \text{ is odd and } n > 1 \end{cases}$$

does not define a function.

Problem 20.16
Find a solution for the recurrence relation

$$\begin{aligned} a_0 =& 1 \\ a_n =& a_{n-1} + 2, \quad n \geq 1. \end{aligned}$$

Problem 20.17
Find a solution to the recurrence relation

$$\begin{aligned} a_0 =& 0 \\ a_n =& a_{n-1} + (n-1), \quad n \geq 1. \end{aligned}$$

Problem 20.18
Find an explicit formula for the Fibonacci sequence

$$\begin{aligned} a_0 =& a_1 = 1 \\ a_n =& a_{n-1} + a_{n-2}. \end{aligned}$$

Fundamentals of Counting

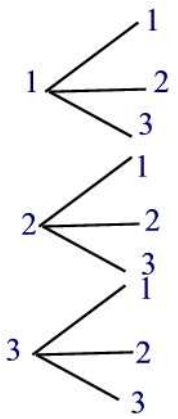
The major goal of this chapter is to establish several (combinatorial) techniques for counting large finite sets without actually listing their elements. These techniques provide effective methods for counting the size of events, an important concept in probability theory.

21 The Fundamental Principle of Counting

Sometimes one encounters the question of listing all the outcomes of a certain experiment. One way for doing that is by constructing a so-called **tree diagram.**

Example 21.1
List all two-digit numbers that can be constructed from the digits 1,2, and 3.

Solution.



The different numbers are $\{11, 12, 13, 21, 22, 23, 31, 32, 33\}$ ■

Of course, trees are manageable as long as the number of outcomes is not large. If there are many stages to an experiment and several possibilities at each stage, the tree diagram associated with the experiment would become too large to be manageable. For such problems the counting of the outcomes is simplified by means of algebraic formulas. The commonly used formula is the **Fundamental Principle of Counting**, also known as the **multiplication rule of counting**, which states:

Theorem 21.1
If a choice consists of k steps, of which the first can be made in n_1 ways, for each of these the second can be made in n_2 ways,$\cdots$, and for each of these the k^{th} can be made in n_k ways, then the whole choice can be made in $n_1 \cdot n_2 \cdot \cdots n_k$ ways.

Proof.
In set-theoretic term, we let S_i denote the set of outcomes for the i^{th} task, $i = 1, 2, \cdots, k$. Note that $n(S_i) = n_i$. Then the set of outcomes for the entire job is the Cartesian product $S_1 \times S_2 \times \cdots \times S_k = \{(s_1, s_2, \cdots, s_k) : s_i \in S_i, 1 \leq i \leq k\}$. Thus, we just need to show that

$$n(S_1 \times S_2 \times \cdots \times S_k) = n(S_1) \cdot n(S_2) \cdots n(S_k).$$

The proof is by induction on $k \geq 2$.

Basis of Induction
This is just Example 15.3(a).
Induction Hypothesis
Suppose

$$n(S_1 \times S_2 \times \cdots \times S_k) = n(S_1) \cdot n(S_2) \cdots n(S_k).$$

Induction Conclusion
We must show

$$n(S_1 \times S_2 \times \cdots \times S_{k+1}) = n(S_1) \cdot n(S_2) \cdots n(S_{k+1}).$$

To see this, note that there is a one-to-one and onto correspondence between the sets $S_1 \times S_2 \times \cdots \times S_{k+1}$ and $(S_1 \times S_2 \times \cdots S_k) \times S_{k+1}$ given by $f(s_1, s_2, \cdots, s_k, s_{k+1}) = ((s_1, s_2, \cdots, s_k), s_{k+1})$. Thus, $n(S_1 \times S_2 \times \cdots \times S_{k+1}) = n((S_1 \times S_2 \times \cdots S_k) \times S_{k+1}) = n(S_1 \times S_2 \times \cdots S_k) n(S_{k+1})$ (by Example 15.3(a)). Now, applying the induction hypothesis gives

$$n(S_1 \times S_2 \times \cdots S_k \times S_{k+1}) = n(S_1) \cdot n(S_2) \cdots n(S_{k+1}) \blacksquare$$

Example 21.2
The following three factors were considered in the study of the effectivenenss of a certain cancer treatment:

(i) Medicine $(A_1, A_2, A_3, A_4, A_5)$
(ii) Dosage Level (Low, Medium, High)
(iii) Dosage Frequency (1,2,3,4 times/day)

Find the number of ways that a cancer patient can be given the medecine?

Solution.
The choice here consists of three stages, that is, $k = 3$. The first stage, can be made in $n_1 = 5$ different ways, the second in $n_2 = 3$ different ways, and the third in $n_3 = 4$ ways. Hence, the number of possible ways a cancer patient can be given medecine is $n_1 \cdot n_2 \cdot n_3 = 5 \cdot 3 \cdot 4 = 60$ different ways ■

Example 21.3
How many license-plates with 3 letters followed by 3 digits exist?

Solution.
A 6-step process: (1) Choose the first letter, (2) choose the second letter, (3) choose the third letter, (4) choose the first digit, (5) choose the second digit, and (6) choose the third digit. Every step can be done in a number of ways that does not depend on previous choices, and each license plate can be specified in this manner. So there are $26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 = 17,576,000$ ways ■

Example 21.4
How many numbers in the range 1000 - 9999 have no repeated digits?

Solution.
A 4-step process: (1) Choose first digit, (2) choose second digit, (3) choose third digit, (4) choose fourth digit. Every step can be done in a number of ways that does not depend on previous choices, and each number can be specified in this manner. So there are $9 \cdot 9 \cdot 8 \cdot 7 = 4,536$ ways ■

Example 21.5
How many license-plates with 3 letters followed by 3 digits exist if exactly one of the digits is 1?

Solution.
In this case, we must pick a place for the 1 digit, and then the remaining digit places must be populated from the digits $\{0, 2, \cdots 9\}$. A 6-step process: (1) Choose the first letter, (2) choose the second letter, (3) choose the third letter, (4) choose which of three positions the 1 goes, (5) choose the first of the other digits, and (6) choose the second of the other digits. Every step can be done in a number of ways that does not depend on previous choices, and each license plate can be specified in this manner. So there are $26 \cdot 26 \cdot 26 \cdot 3 \cdot 9 \cdot 9 = 4,270,968$ ways ■

Review Problems

Problem 21.1
If each of the 10 digits 0-9 is chosen at random, how many ways can you choose the following numbers?
(a) A two-digit code number, repeated digits permitted.
(b) A three-digit identification card number, for which the first digit cannot be a 0. Repeated digits permitted.
(c) A four-digit bicycle lock number, where no digit can be used twice.
(d) A five-digit zip code number, with the first digit not zero. Repeated digits permitted.

Problem 21.2
(a) If eight cars are entered in a race and three finishing places are considered, how many finishing orders can they finish? Assume no ties.
(b) If the top three cars are Buick, Honda, and BMW, in how many possible orders can they finish?

Problem 21.3
You are taking 2 shirts(white and red) and 3 pairs of pants (black, blue, and gray) on a trip. How many different choices of outfits do you have?

Problem 21.4
A Poker club has 10 members. A president and a vice-president are to be selected. In how many ways can this be done if everyone is eligible?

Problem 21.5
In a medical study, patients are classified according to whether they have regular (RHB) or irregular heartbeat (IHB) and also according to whether their blood pressure is low (L), normal (N), or high (H). Use a tree diagram to represent the various outcomes that can occur.

Problem 21.6
If a travel agency offers special weekend trips to 12 different cities, by air, rail, bus, or sea; in how many different ways can such a trip be arranged?

Problem 21.7
If twenty different types of wine are entered in wine-tasting competition, in how many different ways can the judges award a first prize and a second prize?

Problem 21.8
In how many ways can the 24 members of a faculty senate of a college choose a president, a vice-president, a secretary, and a treasurer?

Problem 21.9
Find the number of ways in which four of ten new novels can be ranked first, second, third, and fourth according to their figure sales for the first three months.

Problem 21.10
How many ways are there to seat 8 people, consisting of 4 couples, in a row of seats (8 seats wide) if all couples are to get adjacent seats?

Problem 21.11
On an English test, a student must write two essays. For the first essay, the student must select from topics A, B, and C. For the second essay, the student must select from topics 1, 2, 3, and 4. How many different ways can the student select the two essay topics?

Problem 21.12
A civics club consists of 9 female Democrats, 5 male Democrats, 6 female Republicans, and 7 male Republicans. How many ways can the club choose
(a) a female Democrat and a male Republican to serve on the budget committee?
(b) a female Democrat or a male Republican to serve as chairperson?
(c) a female or a Republican to serve as chairperson?

Problem 21.13
To open your locker at the fitness center, you must enter five digits in order from the set $0, 1, 2, \cdots, 9$. How many different keypad patterns are possible if
(a) any digits can be used in any position and repetition of digits is allowed?
(b) the digit 0 cannot be used as the first digit, but otherwise any digit can be used in any position and repetition is allowed?
(c) any digits can be used in any position, but repetition is not allowed?

Problem 21.14
Professor Watson teaches an advanced cognitive sociology class of 10 students. She has a visually challenged student, Marie, who must sit in the

front row next to her tutor, who is also a member of the class. If there are six chairs in the first row of her classroom, how many different ways can Professor Watson assign students to sit in the first row?

Problem 21.15
Mias Pizza advertises a special in which you can choose a thin crust, thick crust, or cheese crust pizza with any combination of different toppings. The ad says that there are almost 200 different ways that you can order the pizza. What is the smallest number of toppings available?

Problem 21.16
Telephone numbers in the United States have 10 digits. The first three are the area code and the next seven are the local telephone number. How many different telephone numbers are possible within each area code? (A telephone number cannot have 0 or 1 as its first or second digit.)

Problem 21.17
How many non-repeating odd three-digit counting numbers are there?

Problem 21.18
A teacher is taking 13 pre-schoolers to the park. How many ways can the children line up, in a single line, to board the bus?

Problem 21.19
A travel agent plans trips for tourists from Chicago to Miami. He gives them three ways to get from town to town: airplane, bus, train. Once the tourists arrive, there are two ways to get to the hotel: hotel van or taxi. The cost of each type of transportation is given in the table below.

Transportation Type	Cost ($)
Airplane	350
Bus	150
Train	225
Hotel Van	60
Taxi	40

Draw a tree diagram to illustrate the possible choices for the tourists. Determine the cost for each outcome.

Problem 21.20
Suppose that we are carrting out a quality control check in a particleboard mill and we have to select 3 sheets from the production line, 1 piece at a time. The mill produces either defective (D) or non-defective (N) boards. Draw a tree diagram showing all the outcomes.

22 Permutations

Consider the following problem: In how many ways can 8 horses finish in a race (assuming there are no ties)? We can look at this problem as a decision consisting of 8 steps. The first step is the possibility of a horse to finish first in the race, the second step is the possibility of a horse to finish second, $\cdots$, the 8^{th} step is the possibility of a horse to finish 8^{th} in the race. Thus, by the Fundamental Principle of Counting there are

$$8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 40,320 \text{ ways.}$$

This problem exhibits an example of an ordered arrangement, that is, the order the objects are arranged is important. Such an ordered arrangement is called a **permutation**. Products such as $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ can be written in a shorthand notation called factorial. That is, $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 8!$ (read "8 factorial"). In general, we define **n factorial** by

$$n! = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1, \ n \geq 1$$

where n is a whole number. By convention we define

$$0! = 1$$

Example 22.1
Evaluate the following expressions: (a) 6! (b) $\frac{10!}{7!}$.

Solution.
(a) $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$
(b) $\frac{10!}{7!} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 10 \cdot 9 \cdot 8 = 720$ ■

Using factorials and the Fundamental Principle of Counting, we see that the number of permutations of n objects is $n!$.

Example 22.2
There are 5! permutations of the 5 letters of the word "rehab." In how many of them is h the second letter?

Solution.
Then there are 4 ways to fill the first spot. The second spot is filled by the letter h. There are 3 ways to fill the third, 2 to fill the fourth, and one way to fill the fifth. There are 4! such permutations ■

Example 22.3
Five different books are on a shelf. In how many different ways could you arrange them?

Solution.
The five books can be arranged in $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5! = 120$ ways ■

Counting Permutations
We next consider the permutations of a set of objects taken from a larger set. Suppose we have n items. How many ordered arrangements of k items can we form from these n items? The number of permutations is denoted by ${}_nP_k$. The n refers to the number of different items and the k refers to the number of them appearing in each arrangement. A formula for ${}_nP_k$ is given next.

Theorem 22.1
For any non-negative integer n and $0 \leq k \leq n$ we have

$$ {}_nP_k = \frac{n!}{(n-k)!}. $$

Proof.
We can treat a permutation as a decision with k steps. The first step can be made in n different ways, the second in $n-1$ different ways, ..., the k^{th} in $n-k+1$ different ways. Thus, by the Fundamental Principle of Counting there are $n(n-1)\cdots(n-k+1)$ $k-$permutations of n objects. That is, ${}_nP_k = n(n-1)\cdots(n-k+1) = \frac{n(n-1)\cdots(n-k+1)(n-k)!}{(n-k)!} = \frac{n!}{(n-k)!}$ ■

Example 22.4
How many license plates are there that start with three letters followed by 4 digits (no repetitions)?

Solution.
The decision consists of two steps. The first is to select the letters and this can be done in ${}_{26}P_3$ ways. The second step is to select the digits and this can be done in ${}_{10}P_4$ ways. Thus, by the Fundamental Principle of Counting there are ${}_{26}P_3 \cdot {}_{10}P_4 = 78,624,000$ license plates ■

Example 22.5
How many five-digit zip codes can be made where all digits are different? The possible digits are the numbers 0 through 9.

Solution.
The answer is ${}_{10}P_5 = \frac{10!}{(10-5)!} = 30,240$ zip codes ■

Review Problems

Problem 22.1
Find m and n so that ${}_mP_n = \frac{9!}{6!}$

Problem 22.2
How many four-letter code words can be formed using a standard 26-letter alphabet
(a) if repetition is allowed?
(b) if repetition is not allowed?

Problem 22.3
Certain automobile license plates consist of a sequence of three letters followed by three digits.
(a) If letters can not be repeated but digits can, how many possible license plates are there?
(b) If no letters and no digits are repeated, how many license plates are possible?

Problem 22.4
A permutation lock has 40 numbers on it.
(a) How many different three-number permutation lock can be made if the numbers can be repeated?
(b) How many different permutation locks are there if the three numbers are different?

Problem 22.5
(a) 12 cabinet officials are to be seated in a row for a picture. How many different seating arrangements are there?
(b) Seven of the cabinet members are women and 5 are men. In how many different ways can the 7 women be seated together on the left, and then the 5 men together on the right?

Problem 22.6
Using the digits 1, 3, 5, 7, and 9, with no repetitions of the digits, how many
(a) one-digit numbers can be made?
(b) two-digit numbers can be made?
(c) three-digit numbers can be made?
(d) four-digit numbers can be made?

Problem 22.7
There are five members of the Math Club. In how many ways can the positions of a president, a secretary, and a treasurer, be chosen?

Problem 22.8
Find the number of ways of choosing three initials from the alphabet if none of the letters can be repeated. Name initials such as MBF and BMF are considered different.

Problem 22.9
(a) How many four-letter words can be made using the standard alphabet?
(b) How many four-letter words can be made using the standard alphabet, where the letters are all different?
(c) How many four-letter words have at least two letters the same?

Problem 22.10
Twelve people need to be photographed, but there are only five chairs. (The rest of the people will be standing behind and their order does not matter.) How many ways can you sit the twelve people on the five chairs?

Problem 22.11
An investor is going to invest $16,000 in 4 stocks chosen from a list of 12 prepared by his broker. How many different investments are possible if $6,000 is invested in one stock, $5,000 in another, $3,000 in the third, and $2,000 in the fourth?

Problem 22.12
Suppose certain account numbers are to consist of two letters followed by four digits and then three more letters, where repetitions of letters or digits are not allowed within any of the three groups, but the last group of letters may contain one or both of those used in the first group. How many such accounts are possible?

Problem 22.13
A suitcase contains 6 distinct pairs of socks and 4 distinct pairs of pants. If a traveler randomly picks 2 pairs of socks and then 3 pairs of pants, how many ways can this be done?

Problem 22.14
The number of permutations of n items, where n_1 items are identical, n_2 items are identical, n_3 items are identical, and so on, is given by:

$$\frac{n!}{n_1!n_2!\ldots}.$$

In how many distinct ways can the letters of the word MISSISSIPPI be arranged?

Problem 22.15
How many different seven-digit phone numbers can be made from the digits 1,1,1,3,3,5,5?

23 Combinations

In a permutation the order of the set of objects or people is taken into account. However, there are many problems in which we want to know the number of ways in which k objects can be selected from n distinct objects in arbitrary order. For example, when selecting a two-person committee from a club of 10 members the order in the committee is irrelevant. That is choosing Mr. A and Ms. B in a committee is the same as choosing Ms. B and Mr. A. A combination is defined as a possible selection of a certain number of objects taken from a group without regard to order. More precisely, the number of $k-$element subsets of an $n-$element set is called the number of **combinations of n objects taken k at a time**. It is denoted by ${}_nC_k$ and is read "n choose k". The formula for ${}_nC_k$ is given next.

Theorem 23.1
If ${}_nC_k$ denotes the number of ways in which k objects can be selected from a set of n distinct objects then

$$ {}_nC_k = \frac{{}_nP_k}{k!} = \frac{n!}{k!(n-k)!}. $$

Proof.
Since the number of groups of k elements out of n elements is ${}_nC_k$ and each group can be arranged in $k!$ ways, we have ${}_nP_k = k!{}_nC_k$. It follows that

$$ {}_nC_k = \frac{{}_nP_k}{k!} = \frac{n!}{k!(n-k)!} \blacksquare $$

An alternative notation for ${}_nC_k$ is $\begin{pmatrix} n \\ k \end{pmatrix}$. We define ${}_nC_k = 0$ if $k < 0$ or $k > n$.

Example 23.1
A jury consisting of 2 women and 3 men is to be selected from a group of 5 women and 7 men. In how many different ways can this be done? Suppose that either Steve or Harry must be selected but not both, then in how many ways this jury can be formed?

Solution.
There are ${}_5C_2 \cdot {}_7C_3 = 350$ possible jury combinations consisting of 2 women

and 3 men. Now, if we suppose that Steve and Harry can not serve together then the number of jury groups that do not include the two men at the same time is $({}_5C_2)({}_5C_2)({}_2C_1) = 200$ ■

The next theorem discusses some of the properties of combinations.

Theorem 23.2
Suppose that n and k are whole numbers with $0 \leq k \leq n$. Then
(a) ${}_nC_0 =_n C_n = 1$ and ${}_nC_1 =_n C_{n-1} = n$.
(b) Symmetry property: ${}_nC_k =_n C_{n-k}$.
(c) Pascal's identity: ${}_{n+1}C_k =_n C_{k-1} +_n C_k$.

Proof.
(a) From the formula of ${}_nC_k$ we have ${}_nC_0 = \frac{n!}{0!(n-0)!} = 1$ and ${}_nC_n = \frac{n!}{n!(n-n)!} = 1$. Similarly, ${}_nC_1 = \frac{n!}{1!(n-1)!} = n$ and ${}_nC_{n-1} = \frac{n!}{(n-1)!} = n$.
(b) Indeed, we have ${}_nC_{n-k} = \frac{n!}{(n-k)!(n-n+k)!} = \frac{n!}{k!(n-k)!} =_n C_k$.
(c) We have

$$\begin{aligned}
{}_nC_{k-1} +_n C_k =& \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!} \\
=& \frac{n!k}{k!(n-k+1)!} + \frac{n!(n-k+1)}{k!(n-k+1)!} \\
=& \frac{n!}{k!(n-k+1)!}(k+n-k+1) \\
=& \frac{(n+1)!}{k!(n+1-k)!} =_{n+1} C_k \blacksquare
\end{aligned}$$

Example 23.2
The Russellville School District has six members. In how many ways
(a) can all six members line up for a picture?
(b) can they choose a president and a secretary?
(c) can they choose three members to attend a state conference with no regard to order?

Solution.
(a) ${}_6P_6 = 6! = 720$ different ways
(b) ${}_6P_2 = 30$ ways
(c) ${}_6C_3 = 20$ different ways ■

Pascal's identity allows one to construct the so-called Pascal's triangle (for $n = 10$) as shown in Figure 16.1.

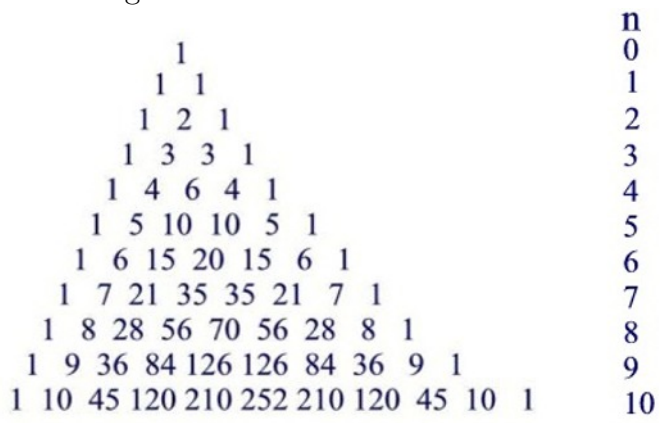


Figure 16.1

As an application of combination we have the following theorem which provides an expansion of $(x + y)^n$, where n is a non-negative integer.

Theorem 23.3 *(Binomial Theorem)*
Let x and y be variables, and let n be a non-negative integer. Then

$$(x + y)^n = \sum_{k=0}^{n} {}_nC_k x^{n-k} y^k$$

where ${}_nC_k$ will be called the **binomial coefficient**.

Proof.
The proof is by induction on n.

Basis of induction: For $n = 0$ we have

$$(x + y)^0 = \sum_{k=0}^{0} {}_0C_k x^{0-k} y^k = 1.$$

Induction hypothesis: Suppose that the theorem is true up to n. That is,

$$(x + y)^n = \sum_{k=0}^{n} {}_nC_k x^{n-k} y^k$$

Induction step: Let us show that it is still true for $n+1$. That is

$$(x+y)^{n+1} = \sum_{k=0}^{n+1} {}_{n+1}C_k x^{n-k+1} y^k.$$

Indeed, we have

$$\begin{aligned}
(x+y)^{n+1} =& (x+y)(x+y)^n = x(x+y)^n + y(x+y)^n \\
=& x \sum_{k=0}^{n} {}_nC_k x^{n-k} y^k + y \sum_{k=0}^{n} {}_nC_k x^{n-k} y^k \\
=& \sum_{k=0}^{n} {}_nC_k x^{n-k+1} y^k + \sum_{k=0}^{n} {}_nC_k x^{n-k} y^{k+1} \\
=& [{}_nC_0 x^{n+1} + {}_nC_1 x^n y + {}_nC_2 x^{n-1} y^2 + \cdots + {}_nC_n x y^n] \\
+& [{}_nC_0 x^n y + {}_nC_1 x^{n-1} y^2 + \cdots + {}_nC_{n-1} x y^n + {}_nC_n y^{n+1}] \\
=& {}_{n+1}C_0 x^{n+1} + [{}_nC_1 + {}_nC_0] x^n y + \cdots + \\
& [{}_nC_n + {}_nC_{n-1}] x y^n + {}_{n+1}C_{n+1} y^{n+1} \\
=& {}_{n+1}C_0 x^{n+1} + {}_{n+1}C_1 x^n y + {}_{n+1}C_2 x^{n-1} y^2 + \cdots \\
+& {}_{n+1}C_n x y^n + {}_{n+1}C_{n+1} y^{n+1} \\
=& \sum_{k=0}^{n+1} {}_{n+1}C_k x^{n-k+1} y^k. \blacksquare
\end{aligned}$$

Note that the coefficients in the expansion of $(x+y)^n$ are the entries of the $(n+1)^{\text{st}}$ row of Pascal's triangle.

Example 23.3
Expand $(x+y)^6$ using the Binomial Theorem.

Solution.
By the Binomial Theorem and Pascal's triangle we have

$$(x+y)^6 = x^6 + 6x^5 y + 15x^4 y^2 + 20x^3 y^3 + 15x^2 y^4 + 6xy^5 + y^6 \blacksquare$$

Example 23.4
How many subsets are there of a set with n elements?

Solution.
Since there are ${}_nC_k$ subsets of k elements with $0 \leq k \leq n$, the total number of subsets of a set of n elements is

$$\sum_{k=0}^{n} {}_nC_k = (1+1)^n = 2^n \blacksquare$$

Review Problems

Problem 23.1
Find m and n so that ${}_mC_n = 13$

Problem 23.2
A club with 42 members has to select three representatives for a regional meeting. How many possible choices are there?

Problem 23.3
In a UN ceremony, 25 diplomats were introduced to each other. Suppose that the diplomats shook hands with each other exactly once. How many handshakes took place?

Problem 23.4
There are five members of the math club. In how many ways can the two-person Social Committee be chosen?

Problem 23.5
A medical research group plans to select 2 volunteers out of 8 for a drug experiment. In how many ways can they choose the 2 volunteers?

Problem 23.6
A consumer group has 30 members. In how many ways can the group choose 3 members to attend a national meeting?

Problem 23.7
Which is usually greater the number of combinations of a set of objects or the number of permutations?

Problem 23.8
Determine whether each problem requires a combination or a permutation:
(a) There are 10 toppings available for your ice cream and you are allowed to choose only three. How many possible 3-topping combinations can yo have?
(b) Fifteen students participated in a spelling bee competition. The first place winner will receive \$1,000, the second place \$500, and the third place \$250. In how many ways can the 3 winners be drawn?

Problem 23.9
Use the binomial theorem and Pascal's triangle to find the expansion of $(a + b)^7$.

Problem 23.10
Find the 5^{th} term in the expansion of $(2a - 3b)^7$.

Problem 23.11
Does order matters for the following situations:
(a) 7 digits selected for a phone number.
(b) 3 member of the Math Faculty are selected to form a selection committee for a Discrete Mathematics textbook.
(c) Among all ATU Math Majors, 4 officers must be elected to be the President, Vice-President, Treasurer, and Secretary of the Math Club.

Problem 23.12
(a) Out of a class of 15 students 1 must be chosen to do office duty, 1 to be register monitor and one to be a captain, how many ways can these roles be handed out?
(b) Out of a class of 15 students 3 are needed to do a display, how many ways can they be chosen?

Problem 23.13
Find the constant term in the expansion $\left(2x^2 - \frac{1}{x}\right)^6$.

Problem 23.14
A term in the expansion of $(ma - 4)^5$ is $-5760a^2$. What is the value of m?

Problem 23.15
Find the value of k if the expansion $(a - 2)^{3k-5}$ consists of 23 terms.

Problem 23.16
In the expansion of $(5a - 2b)^9$, find the coefficient of the term containing a^5.

Problem 23.17
What is the third term in row 22 of Pascal's triangle?

Problem 23.18
In how many ways can a President, a Vice-President and a committee of 3 can be selected from a group of 7 individuals?

Problem 23.19
When playing the lottery there are 6 different balls ranging between 0 and 60 that can be chosen from. How many different possibilities are there when picking lottery numbers?

Problem 23.20
Suppose you have a group of 10 children consisting of 4 girls and 6 boys.
(a) How many four-person teams can be chosen that consist of two girls and two boys?
(b) How many four-person teams contain at least one girl?

Basics of Graph Theory

In this chapter we present the basic concepts related to graphs and trees such as the degree of a vertex, connectedness, Euler and Hamiltonian circuits, isomorphisms of graphs, rooted and spanning trees.

24 Graphs and the Degree of a Vertex

An **undirected graph** G consists of a set V_G of **vertices** and a set E_G of **edges** such that each edge $e \in E_G$ is associated with an unordered pair of vertices, called its **endpoints**.
A **directed graph** or **digraph** G consists of a set V_G of vertices and a set E_G of edges such that each edge $e \in E_G$ is associated with an ordered pair of vertices.
We denote a graph by $G = (V_G, E_G)$.

Example 24.1
Find the vertices and edges of the directed graph shown in Figure 24.1.

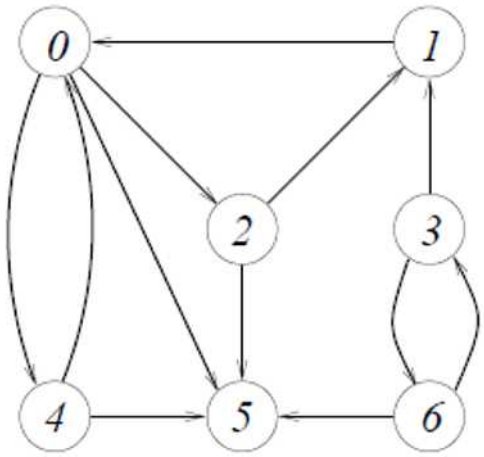


Figure 24.1

Solution.
The vertices are

$$V_G = \{0, 1, 2, 3, 4, 5, 6\}$$

and the edges are

$$E_G = \{(0,2), (0,4), (0,5), (1,0), (2,1), (2,5), (3,1), (3,6), (4,0), (4,5), (6,3), (6,5)\} \blacksquare$$

Two vertices are said to be **adjacent** if there is an edge connecting the two vertices. Two edges associated to the same vertices are called **parallel**. An

edge incident to a single vertex is called a **loop**. A vertex that is not incident on any edge is called an **isolated vertex**. A graph with neither loops nor parallel edges is called a **simple graph**.

Example 24.2
Consider the following graph $G = (V_G, E_G)$.

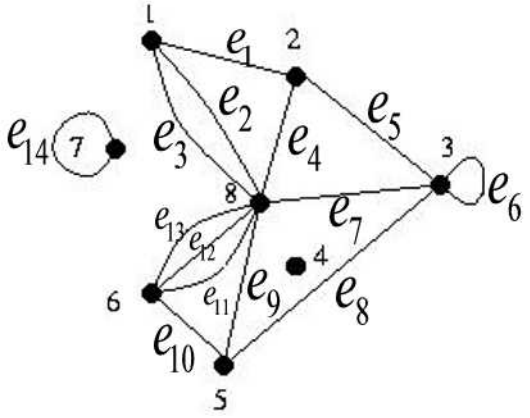


Figure 24.2

(a) Find E_G and V_G.
(b) List the isolated vertices.
(c) List the loops.
(d) List the parallel edges.
(e) List the vertices adjacent to $\{3\}$.
(f) Find all edges incident on $\{8\}$.

Solution.
(a) We have

$$V_G = \{1, 2, 3, 4, 5, 6, 7, 8\}$$

and

$$E_G = \{e_1, e_2, \cdots, e_{14}\}.$$

(b) There is only one isolated vertex, $\{4\}$.
(c) There are two loops $\{e_6, e_{14}\}$.
(d) $\{e_2, e_3, e_{11}, e_{12}, e_{13}\}$.
(e) $\{2, 3, 5, 8\}$.
(f) $\{e_2, e_3, e_4, e_7, e_9, e_{11}, e_{12}, e_{13}\}$ ■

Example 24.3
Which one of the following graphs is simple?

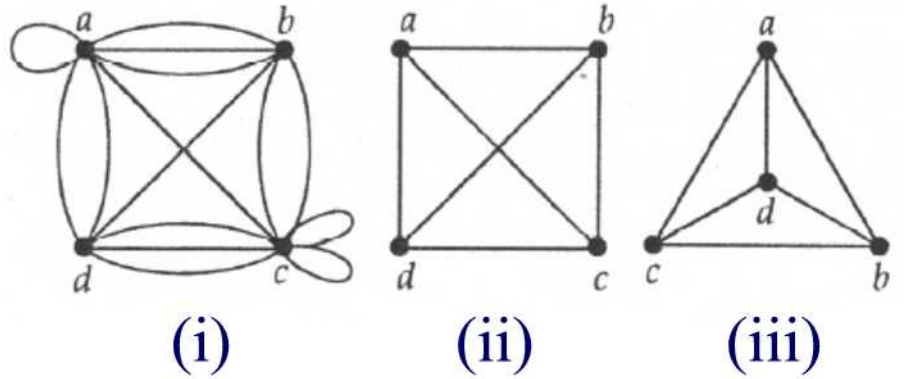


Figure 24.3

Solution.
(i) G is not simple since it has a loop and parallel edges.
(ii) and (iii) are simple graphs ■

A **complete graph** on n vertices, denoted by K_n, is the simple graph that contains exactly one edge between each pair of distinct vertices.

Example 24.4
Draw K_2, K_3, and K_4.

Solution.
K_2, K_4 and K_5 are shown in Figure 24.4 ■

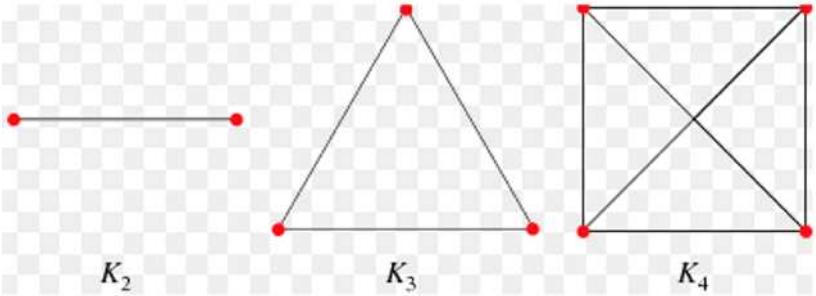


Figure 24.4

A graph in which the vertices can be partitioned into two disjoint sets V_1 and V_2 such that each edge connects a vertex of V_1 to a vertex in V_2 is called **bipartite graph**.

Example 24.5
(a) Show that the graph G is bipartite.

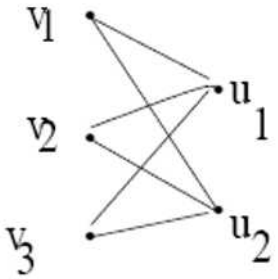


Figure 24.5

(b) Show that K_3 is not bipartite.

Solution.
(a) Clear from the definition and the graph.
(b) Any two sets of vertices of K_3 will have one set with at least two vertices. Thus, according to the definition of bipartite graph, K_3 is not bipartite ■

A **complete bipartite graph** is a bipartite graph in which each vertex in the first set is joined to each vertex in the second set by exactly one edge. If the first set has m elements and the second set has n elements then we denote the bipartite graph by $K_{m,n}$.

Example 24.6
Draw $K_{2,3}$ and $K_{3,3}$.

Solution.
$K_{2,3}$ and $K_{3,3}$ are given in Figure 24.6 ■

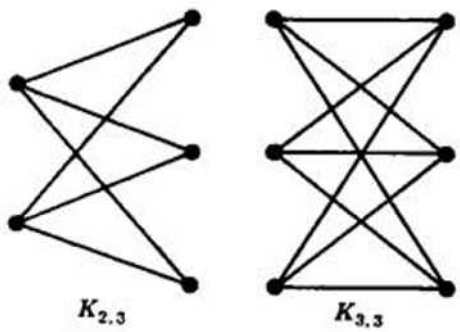


Figure 24.6

The **degree** of a vertex v in an undirected graph, in symbol $deg(v)$, is the number of edges incident on it. By definition, a loop at a vertex contributes twice to the degree of that vertex. The **total degree of G** is the sum of the degrees of all the vertices of G.

Example 24.7
What are the degrees of the vertices in Figure 24.7.

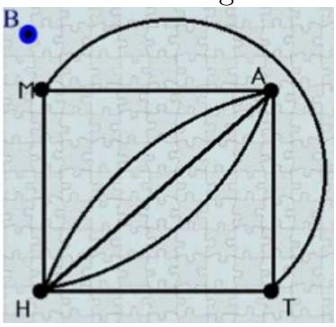


Figure 24.7

Solution.
$deg(B) = 0, deg(A) = 5, deg(T) = 3, deg(M) = 3$, and $deg(H) = 5$ ■

Theorem 24.1 *(The Handshaking Theorem)*
For any graph $G = (V_G, E_G)$ we have

$$2|E_G| = \sum_{v \in V_G} deg(v).$$

Proof.
Suppose that $V_G = \{v_1, v_2, \cdots, v_n\}$. Let $e \in E_G$. If e is a loop then it contributes 2 to the total degree of G. If e is not a loop then let v_i and v_j denote the endpoints of e. Then e contributes 1 to $deg(v_i)$ and contributes 1 to the $deg(v_j)$. Therefore, e contributes 2 to the total degree of G. Since e was chosen arbitrarily, this shows that each edge of G contributes 2 to the total degree of G. Thus,

$$2|E_G| = \sum_{v \in V(G)} deg(v) \blacksquare$$

The following is easily deduced from the previous theorem.

Theorem 24.2
In any graph there are an even number of vertices of odd degree.

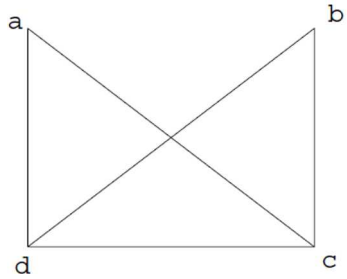
Proof.
Let $G = (V_G, E_G)$ be a graph. By the previous theorem, the sum of all the degrees of the vertices is $T = 2|E_G|$, an even number. Let E be the sum of the numbers $deg(v)$, each which is even and O the sum of numbers $deg(v)$ each which is odd. Then $T = E + O$. That is, $O = T - E$. Since both T and E are even, O is also even. This implies that there must be an even number of the odd degrees. Hence, there must be an even number of vertices with odd degree. ■

Example 24.8
Find a formula for the number of edges in K_n.

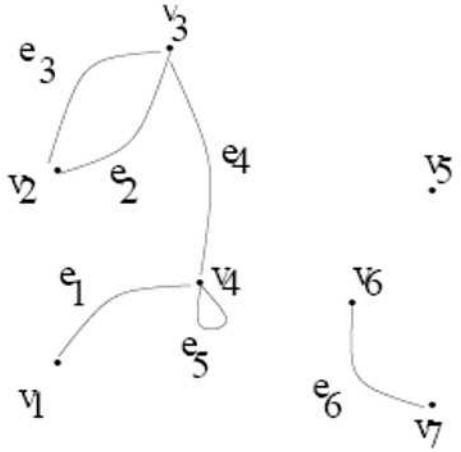
Solution.
Since G is complete, each vertex is adjacent to the remaining vertices. Thus, the degree of each of the n vertices is $n-1$, and we have the sum of the degrees of all of the vertices being $n(n-1)$. By Theorem 24.1, $n(n-1) = 2|E_G|$ ■

Review Problems

Problem 24.1
Find the vertices and edges of the following directed graph.

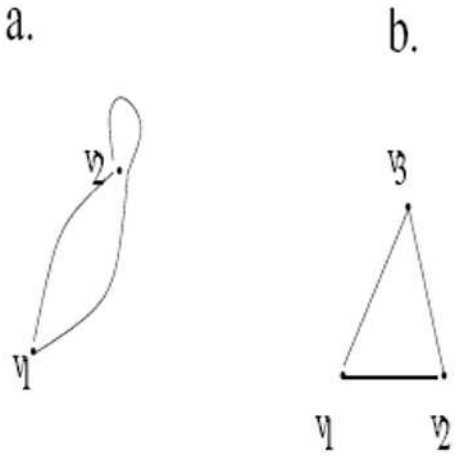


Problem 24.2
Consider the following graph G



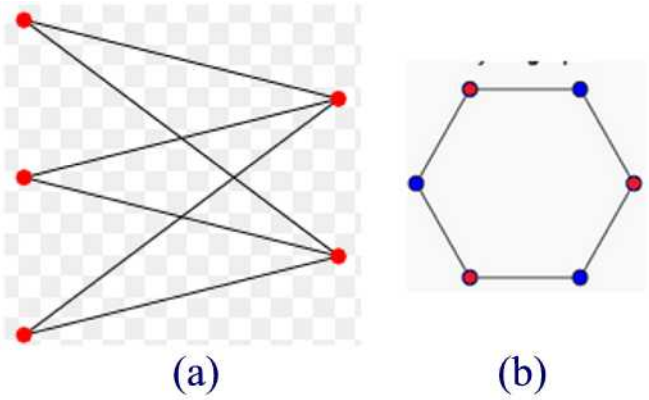
(a) Find E_G and V_G.
(b) List the isolated vertices.
(c) List the loops.
(d) List the parallel edges.
(e) List the vertices adjacent to v_3.
(f) Find all edges incident on v_4.

Problem 24.3
Which one of the following graphs is simple?



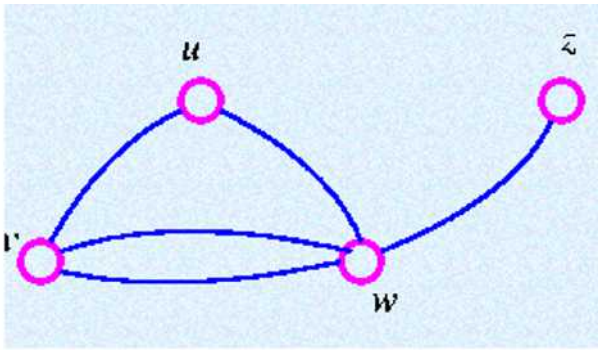
Problem 24.4
Draw K_5.

Problem 24.5
Which of the following graph is bipartite?

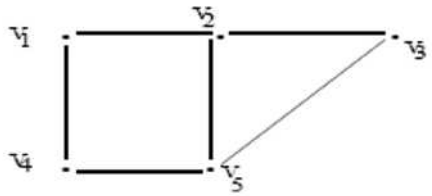


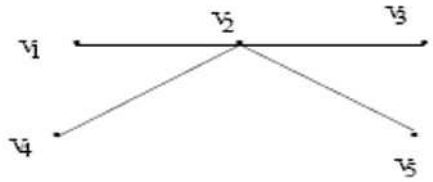
Problem 24.6
Draw the complete bipartite graph $K_{2,4}$.

Problem 24.7
What are the degrees of the vertices in the following graph



Problem 24.8
The **union** of two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ is the graph $G_1 \cup G_2 = (V_1 \cup V_2, E_1 \cup E_2)$. The **intersection** of two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ is the graph $G_1 \cap G_2 = (V_1 \cap V_2, E_1 \cap E_2)$.
Find the union and the intersection of the graphs

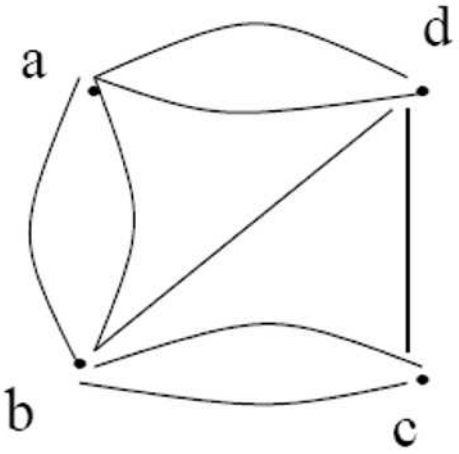




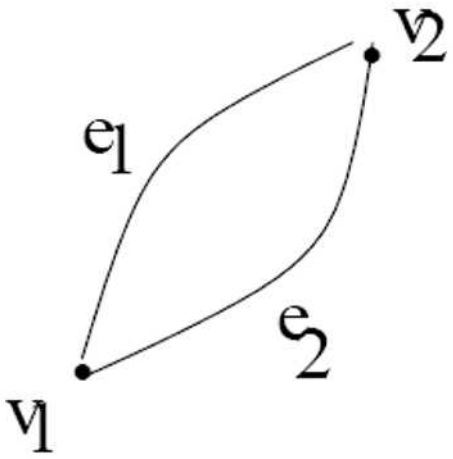
Problem 24.9
Graphs can be represented using matrices. The **adjacency** matrix of a graph G with n vertices is an $n \times n$ matrix A_G such that each entry a_{ij} is the number of edges connecting v_i and v_j. Thus, $a_{ij} = 0$ if there is no edge from v_i to v_j.
(a) Draw a graph with the adjacency matrix

$$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

(b) Use an adjacency matrix to represent the graph

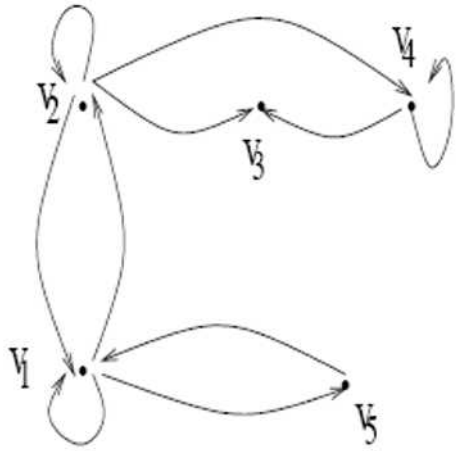


Problem 24.10
A graph $H = (V_H, E_H)$ is a **subgraph** of $G = (V_G, E_G)$ if and only if $V_H \subseteq V_G$ and $E_H \subseteq E_G$.
Find all nonempty subgraphs of the graph



Problem 24.11
When (u, v) is an edge in a directed graph G then u is called the **initial vertex** and v is called the **terminal vertex.** In a directed graph, the **in-degree** of a vertex v, denoted by $deg^-(v)$, is the number of edges with v as their terminal vertex. Similarly, the **out-degree** of v, denoted by $deg^+(v)$, is the number of edges with v as an initial vertex. Note that $deg(v) =$

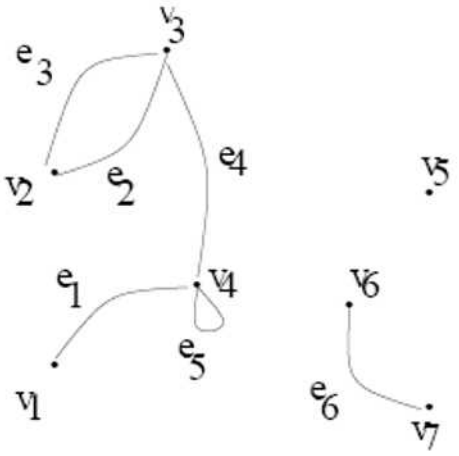
$deg^+(v) + deg^-(v)$.
Find the in-degree and out-degree of each of the vertices in the graph G with directed edges.



Problem 24.12
Show that for a digraph $G = (V_G, E_G)$ we have

$$|E_G| = \sum_{v \in V(G)} deg^-(v) = \sum_{v \in V(G)} deg^+(v).$$

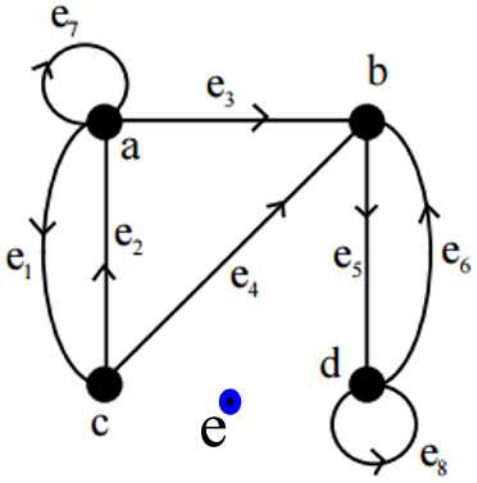
Problem 24.13
Another useful matrix representation of a graph is known as the **incidence matrix.** It is constructed as follows. We label the rows with the vertices and the columns with the edges. The entry for row v and column e is 1 if e is incident on v and 0 otherwise. If e is a loop at v we assign the value 2. It is easy to see that the sum of entries of each column is 2 and that the sum of entries of a row gives the degree of the vertex corresponding to that row. Find the incidence matrix corresponding to the graph



Problem 24.14
If each vertex of an undirected graph has degree k then the graph is called a **regular** graph of degree k.
How many edges are there in a graph with 10 vertices each of degree 6?

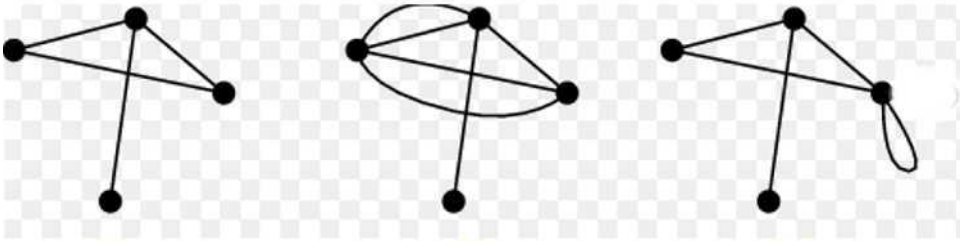
Problem 24.15
Find the vertices and edges of the directed graph shown below.

Problem 24.16
Consider the following graph $G = (V_G, E_G)$.



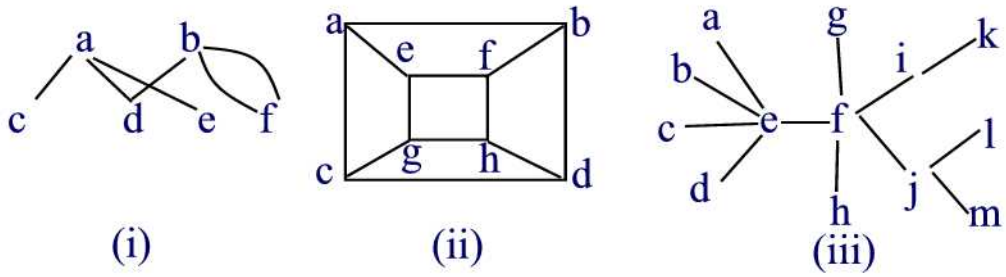
(a) List the isolated vertices.
(b) List the loops.
(c) List the parallel edges.
(d) List the vertices adjacent to $\{b\}$.
(e) Find all edges incident on $\{b\}$.

Problem 24.17
Which one of the following graphs is simple?



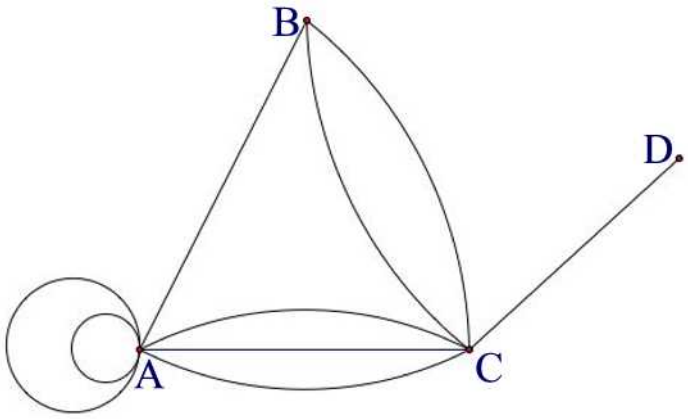
Problem 24.18
Draw the complete graph K_6.

Problem 24.19
Show that each of the following graphs is bipartite.



Problem 24.20
Graph the complete bipartite graphs $K_{3,2}$ and $K_{2,5}$.

Problem 24.21
Find the dgree of each vertex of the graph below.


B
D
A
C

25 Paths and Circuits

In an undirected graph G, a sequence of n non-repeated edges connecting two vertices is called a **path of length** n. A **circuit**, a **cycle**, or a **closed path** is a path which the first and last vertices are the same. A path or circuit is **simple** if no vertex is repeated. A graph that does not contain any circuit is called **acyclic**.

Example 25.1
In the graph below, determine whether the following sequences are paths, simple paths, circuits, or simple circuits.

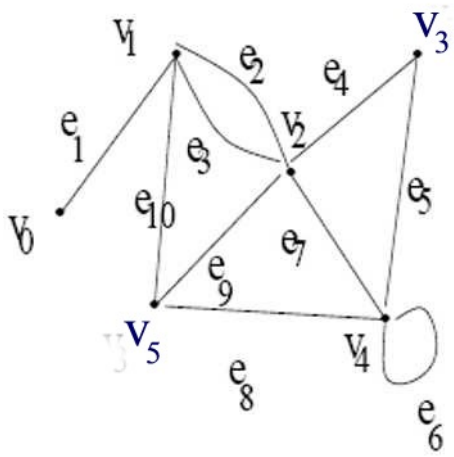


Figure 25.1

(a) $v_0e_1v_1e_{10}v_5e_9v_2e_2v_1$.
(b) $v_3e_5v_4e_8v_5e_{10}v_1e_3v_2$.
(c) $v_1e_2v_2e_3v_1$.
(d) $v_5e_9v_2e_4v_3e_5v_4e_6v_4e_8v_5$.

Solution.
(a) a path (no repeated edge), not a simple path (repeated vertex v_1), not a circuit
(b) a simple path
(c) a simple circuit
(d) a circuit, not a simple circuit (vertex v_4 is repeated) ■

Example 25.2
Give an example of an acyclic graph with three vertices.

Solution.
One such an example is shown in Figure 25.2 ■

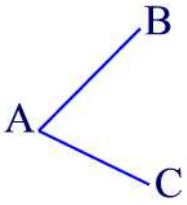


Figure 25.2

An undirected graph is called **connected** if there is a path between every pair of distinct vertices of the graph. A graph that is not connected is said to be **disconnected**. Basically, a graph that is in one piece is said to be connected, whereas one which splits into several pieces is disconnected. Each piece in a disconnected graph is called a **component.**

Example 25.3
Determine which graph is connected and which one is disconnected.

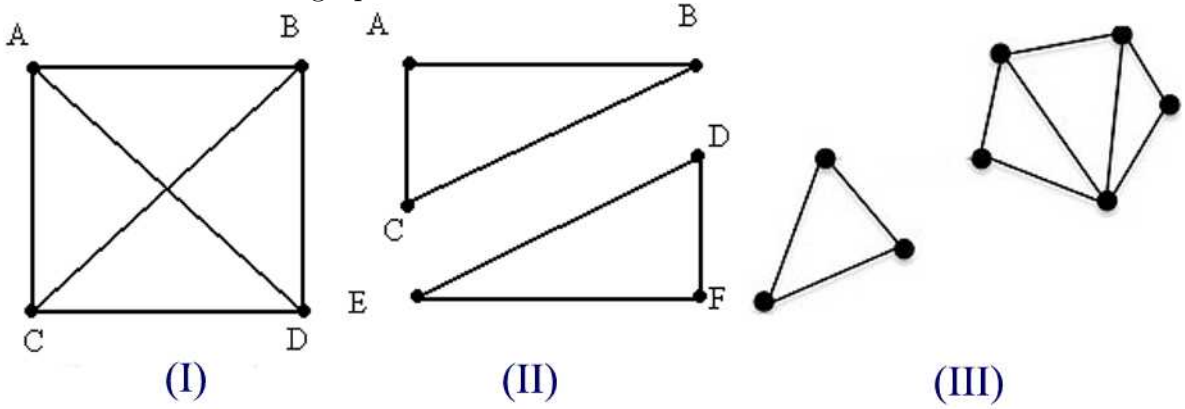


Figure 25.3

Solution.
(I) is connected whereas (II) and (III) are disconnected ■

A path that contains all edges of a graph G is called an **Euler path**. If this path is also a circuit, it is called an **Euler circuit**. Note that an Euler path starts and ends at different vertices whereas an Euler circuit starts and ends at the same vertex.

Example 25.4
Consider the graph in Figure 25.4.

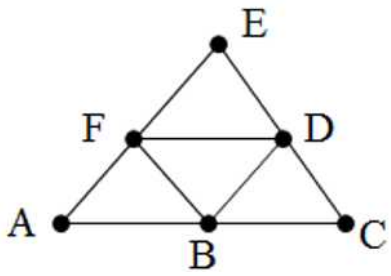


Figure 25.4

(a) Is the circuit $ABCDEFA$ an Euler circuit? Explain.
(b) Is the circuit $ABCDEFBDFA$ an Euler circuit? Explain.

Solution.
(a) The circuit $ABCDEFA$ is not an Euler circuit since it does not uses the edges BD, DF, FB.
(b) The circuit $ABCDEFBDFA$ is an Euler circuit since it uses all the edges of the graph ■

How can we tell if a graph has an Euler circuit or an Euler path? The following theorem whose proof is omitted provides criteria for the existence of either Euler path or Euler circuit.

Theorem 25.1 *(Euler's Theorem)*
Let G be a connected graph.
(a) If a vertex has odd degree, then G has no Euler circuit.
(b) If every vertex has even degree, then G has an Euler circuit.
(c) If there are exactly two vertices of odd degree, then G has an Euler path that starts at one of these vertices and ends at the other.
(d) If there are more than two vertices of odd degree, then G has no Euler path.

Example 25.5
Show that the following graph has no Euler circuit.

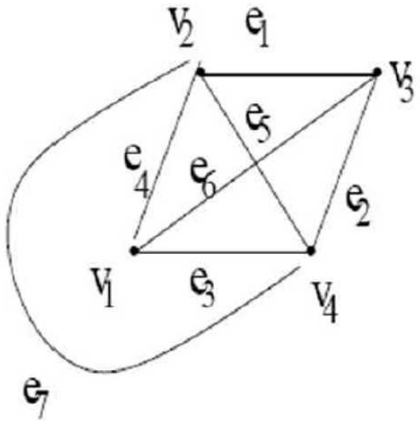


Figure 25.5

Solution.
Vertices v_1 and v_3 both have degree 3, which is odd. Hence, by Theorem 25.1, this graph does not have an Euler circuit ■

Example 25.6
Show that the following graph has an Euler path.

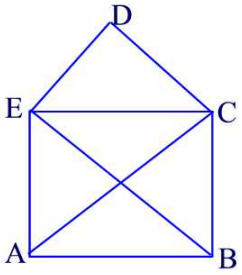
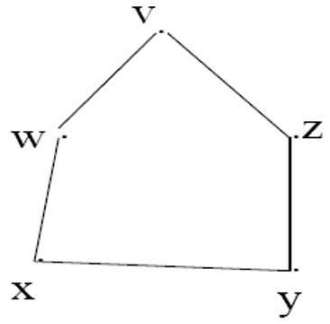


Figure 25.6

Solution.
We have $deg(A) = deg(B) = 3$ and $deg(C) = deg(D) = deg(E) = 4$. Hence, by Theorem 25.1, the graph has an Euler path ■

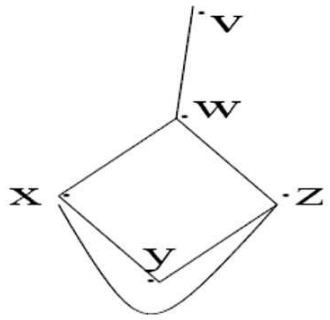
A path is called a **Hamiltonian path** if it visits every vertex of the graph exactly once. A circuit that visits every vertex exactly once except for the last vertex which duplicates the first one is called a **Hamiltonian circuit.**

Example 25.7
Find a Hamiltonian circuit in the graph



Solution.
vwxyzv ■

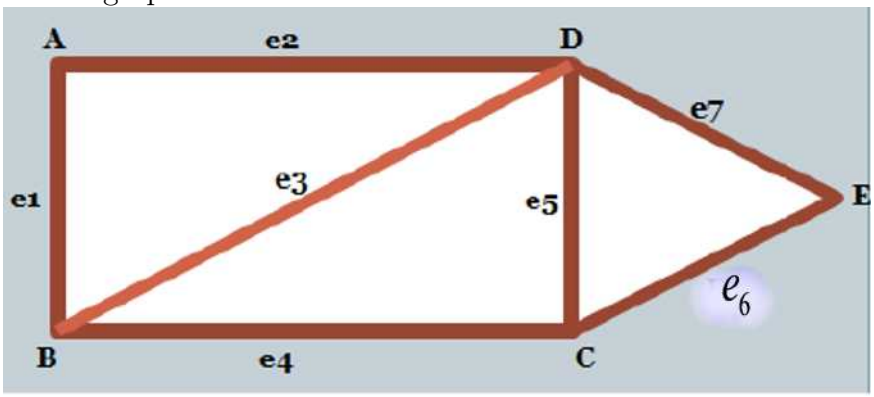
Example 25.8
Show that the following graph has a Hamiltonian path but no Hamiltonian circuit.



Solution.
vwxyz is a Hamiltonian path. There is no Hamiltonian circuit since no cycle goes through v ■

Review Problems

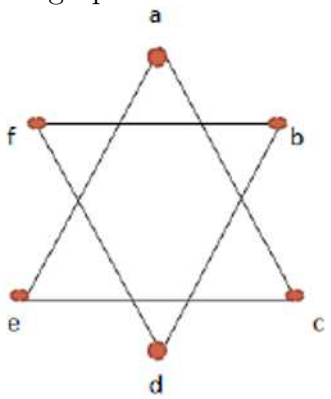
Problem 25.1
Consider the graph shown below.



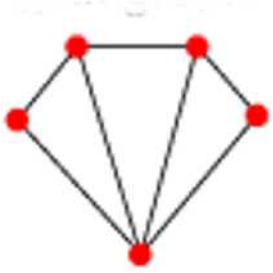
(a) Give an example of a path of length 4 connecting the vertices A and C.
(b) Give an example of a simple path of length 4 connecting the vertices A and B.
(c) Give an example of a simple circuit of length 5 starting and ending at A.

Problem 25.2
Give an example of an acyclic graph with four vertices.

Problem 25.3
Determine which graph is connected and which one is disconnected.

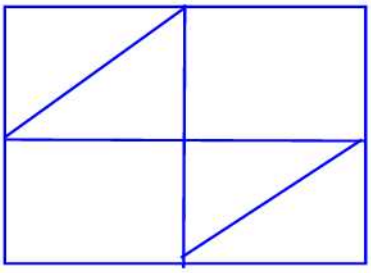


(I)

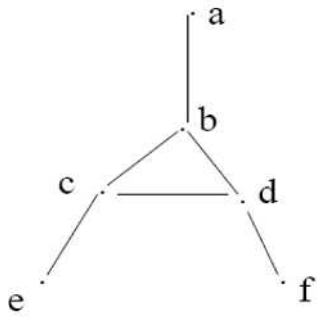


(II)

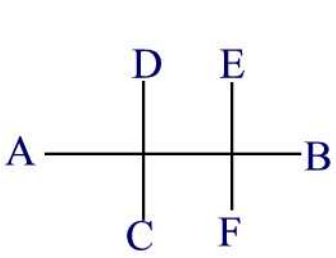
Problem 25.4
Show that the following graph has an Euler circuit.



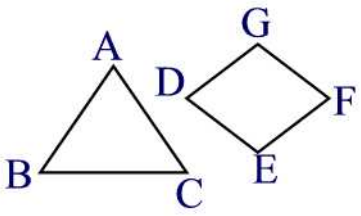
Problem 25.5
Show that the following graph has no Hamiltonian path.



Problem 25.6
Which of the graphs shown below are connected?



(I)

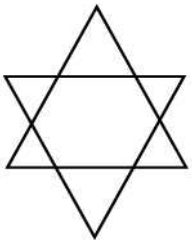


(II)

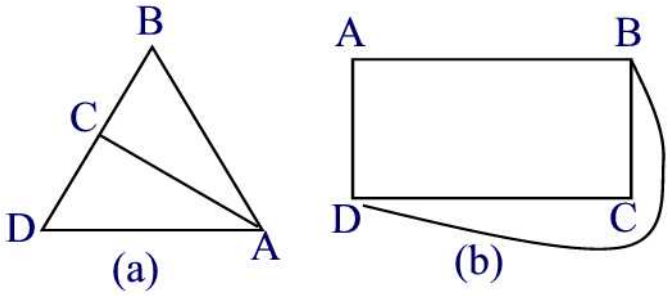
Problem 25.7
If a graph is disconnected then the various connected pieces of the grapg are called the **connected components**. Find the number of connected

components of each of the given graphs.

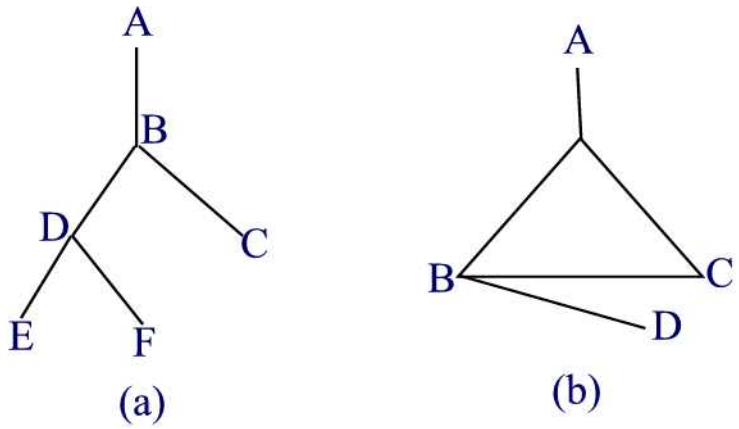
Problem 25.8
Find the connected components of the graph shown below.



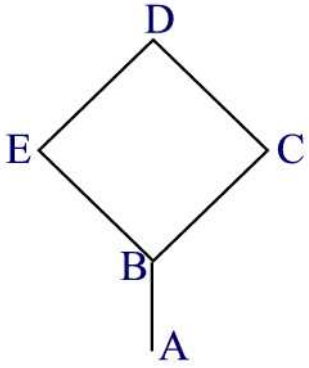
Problem 25.9
Show that the graphs given below do not have an Euler circuit.



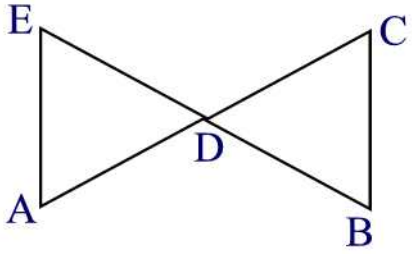
Problem 25.10
Show that the graphs given below do not have an Euler path.



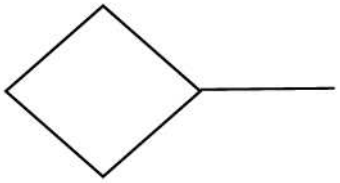
Problem 25.11
Show that the graph given below has an Euler path.



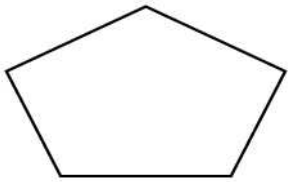
Problem 25.12
Does the graph shown below have a Hamiltonian circuit?



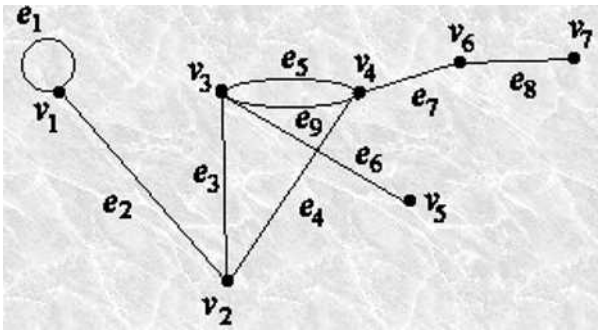
Problem 25.13
Does the graph shown below have a Hamiltonian circuit?



Problem 25.14
Does the graph shown below have a Hamiltonian circuit?



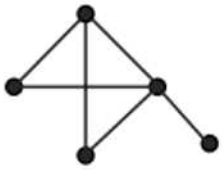
Problem 25.15
Given the graph below.



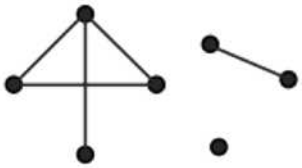
Determine which of the following sequences are paths, simple paths, circuits, or simple circuits:
(a) (i) $v_2e_3v_3e_5v_4e_7v_6$
(ii) $e_2e_3e_9e_7e_7e_5e_6$
(iii) $v_3v_4v_2v_3$
(iv) $v_5v_3v_4v_2v_3v_5$.
(b) Give an example of a path of length 4.

Problem 25.16
Draw an acyclic graph with five vertices.

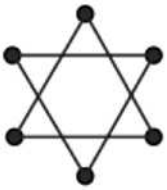
Problem 25.17
Determine which of the following graphs are connected?



G_1

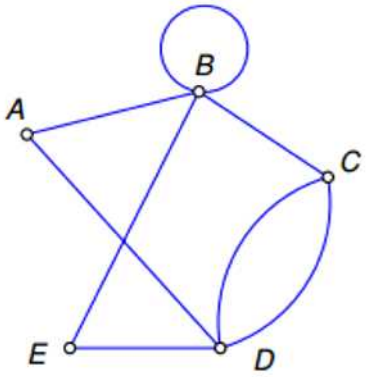


G_2



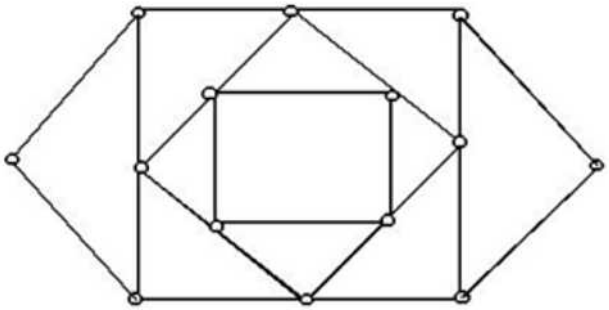
G_3

Problem 25.18
Consider the graph shown below.

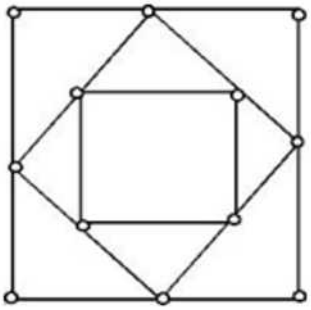


(a) Is the path $BBADCDEBC$ an Euler path?
(b) Is the path $CDCBBADEB$ an Euler path?
(c) Is the path $CDCBBADEBC$ an Euler circuit?
(d) Is the path $CDEBBADC$ an Euler circuit?

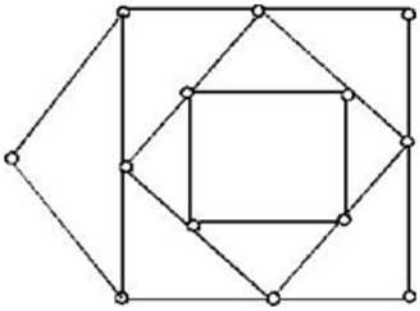
Problem 25.19
Show that the following graph has no Euler circuit and no Euler path.



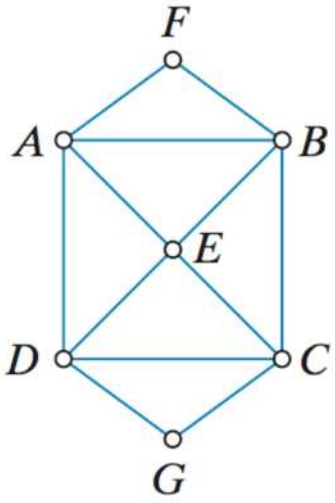
Problem 25.20
Show that the following graph has an Euler circuit.



Problem 25.21
Show that the following graph has an Euler path.



Problem 25.22
Find a Hamiltonian circuit and a Hamiltonian path in the graph


F
A
B
E
D
C
G

26 Trees

An undirected graph is called a **tree** if each pair of distinct vertices has exactly one path between them. Thus, a tree has no parallel edges or loops. Trees are examples of connected acyclic graphs.

Example 26.1
Which of the following graphs are trees?

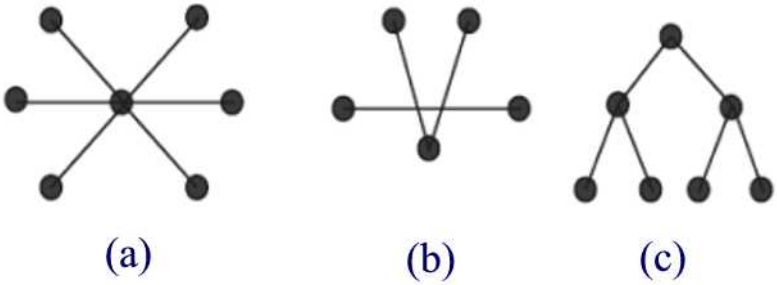


Figure 26.1

Solution.
(a) and (c) satisfy the definition of a tree whereas (b) does not ■

A vertex of degree 1 in a tree is called a **leaf**. A vertex of degree 2 or more in a tree is called a **branch**.
Next, we want to show that the number of edges in a tree is one fewer than the number of vertices. In order to prove this result, we establish first the following lemma.

Lemma 26.1
Let T be a graph with more than one vertex. If T is a tree then one vertex must be of degree 1.

Proof.
We use contrapositive to prove the lemma. Suppose that graph T has no vertex of degree 1. Starting at any vertex v, follow a sequence of distinct edges until a vertex repeats; this is possible because the degree of every vertex is at least two, so upon arriving at a vertex for the first time it is always possible to leave the vertex on another edge. When a vertex repeats for the first time, we have discovered a cycle. Hence, T is not a tree ■

The following result shows that trees have one fewer edge than they have vertices. Thus, it can be used as a criterion for showing that a graph is not a tree.

Theorem 26.1
A tree with n vertices has exactly $n-1$ edges. That is, if $G=(V_G, E_G)$ is a tree then $|E_G| = |V_G| - 1$.

Proof.
The proof is by induction on $n \geq 1$. Let $P(n)$ be the property: Any tree with n vertices has $n-1$ edges.
Basis of induction: $P(1)$ is valid since a tree with one vertex has zero edges.
Induction hypothesis: Suppose that $P(n)$ holds up to $n \geq 1$.
Induction Step: We must show that any tree with $n+1$ vertices has n edges. Indeed, let T be any tree with $n+1$ vertices. Since $n+1 \geq 2$, by the previous lemma, T has a vertex v of degree 1. Let T_0 be the graph obtained by removing v and the edge attached to v. Then T_0 is a tree with n vertices. By the induction hypothesis, T_0 has $n-1$ edges and so T has n edges ■

Example 26.2
Which of the following graphs are trees?

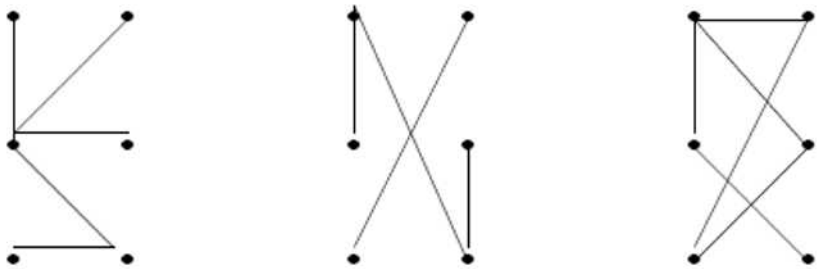


Figure 26.2

Solution.
The first graph satisfies the definition of a tree. The second and third graphs do not satisfy the conclusion of Theorem 26.1 and therefore they are not trees ■

The following is the converse to Theorem 26.1.

Theorem 26.2
Any connected graph with n vertices and $n-1$ edges is a tree.

Proof.
We prove the result by contradiction. Let G be a connected graph with n vertices and $n-1$ edges. Suppose that G is not a tree. Then G has a circuit or a cycle. Let G_1 be the connected graph obtained by removing an edge of the cycle. We continue this process until we reach a connected graph G_k with no cycles, where k is the number of edges removed. Thus, G_k is a tree with n vertices and $n-1-k$ edges. This contradicts Theorem 26.1 ■

Rooted Trees
A **rooted tree** is a tree in which a particular vertex is designated as the **root.** The **level of a vertex** v is the length of the simple path from the root to v. The **height** of a rooted tree is the largest level number that occurs.

Example 26.3
Find the level of each vertex and the height of the following rooted tree.

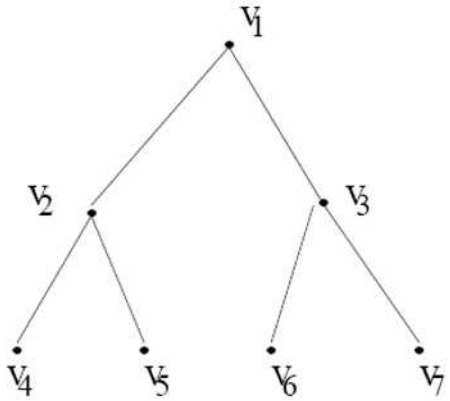


Figure 26.3

Solution.
v_1 is the root of the given tree.

vertex	v_2	v_3	v_4	v_5	v_6	v_7
level	1	1	2	2	2	2

The height of the tree is 2 ■

Let T be a rooted tree with root v_0. Suppose $(v_0, v_1, \cdots, v_n)$ is a simple path in T and x, y, z are three vertices of a tree. Then
(a) v_{n-1} is the **parent** of v_n.
(b) $v_0, v_1, \cdots, v_{n-1}$ are the **ancestors** of v_n.
(c) v_n is the **child** of v_{n-1}.
(d) If x is an ancestor of y then y is a **descendant** of x.
(e) If x and y are children of z then x and y are **siblings**.
(f) If x has no children, then x is a **leaf**.
(g) The **subtree** of T rooted at x is the graph with vertex set V and edge set E, where V is x together with the descendants of x and

$$E = \{e | e \text{ is an edge on a simple path from } x \text{ to some vertex in } V\}.$$

Example 26.4
Consider the rooted tree of Figure 26.4.

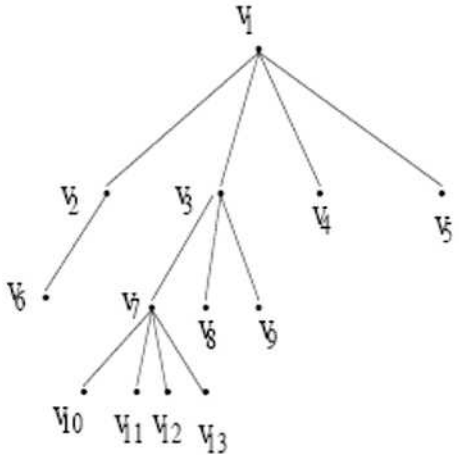


Figure 26.4

(a) Find the parent of v_6.
(b) Find the ancestors of v_{13}.
(c) Find the children of v_3.
(d) Find the descendants of v_{11}.
(e) Find an example of a siblings.
(f) Find the leaves.
(g) Construct the subtree rooted at v_7.

Solution.
(a) v_2.
(b) v_1, v_3, v_7.
(c) v_7, v_8, v_9.
(d) None.
(e) $\{v_2, v_3, v_4, v_5\}$.
(f) $\{v_4, v_5, v_6, v_8, v_9, v_{10}, v_{11}, v_{12}, v_{13}\}$.
(g)

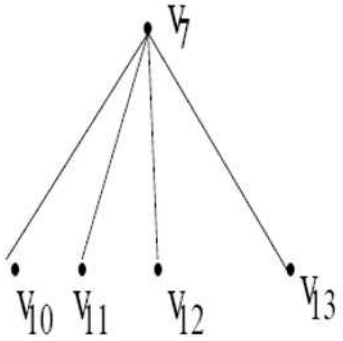


Figure 26.5

Binary Trees

A **binary tree** is a rooted tree such that each vertex has at most two children. Moreover, each child is designated as either a **left child** or a **right child**. A **full binary tree** is a binary tree in which each vertex has either two children or zero children.

Example 26.5
Consider the binary tree shown in Figure 26.6.

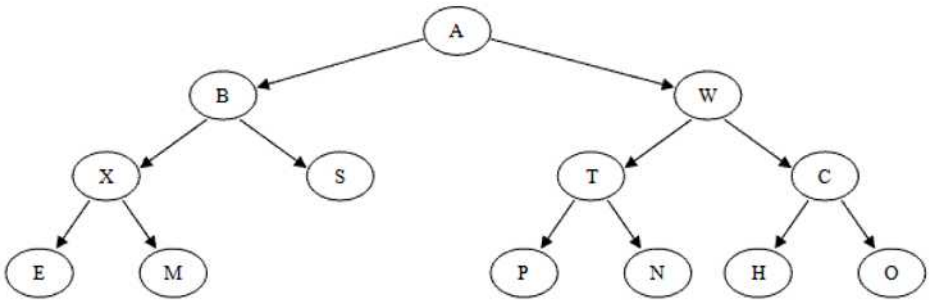


Figure 26.6

(a) Find the left child and the right child of vertex T.
(b) Construct a full binary tree with root at W.

Solution.
(a) The left child is P and the right child is N.
(b) The full binary tree with root at W is shown in Figure 26.7.

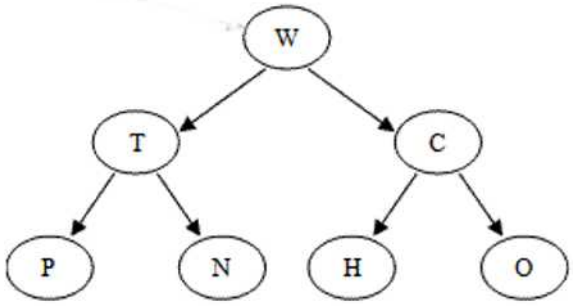


Figure 26.7

Spanning Tree
Let T be a subgraph of a graph G such that T is a tree containing all of the vertices of G. Such a tree is called a **spanning tree**.

Example 26.6
Find a spanning tree of the following graph.

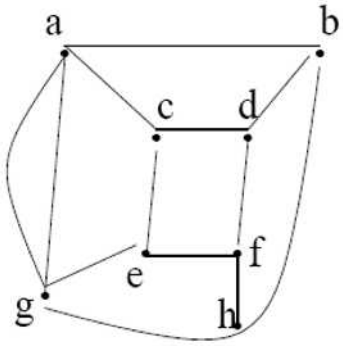


Figure 26.8

Solution.

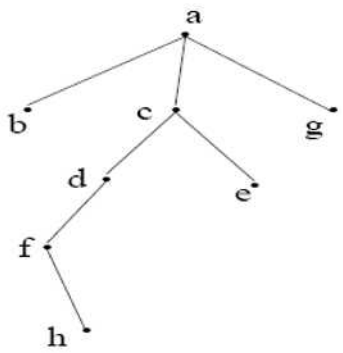


Figure 26.9

The following theorem provides an algorithm for creating a spanning tree of any connected graph.

Theorem 26.3
(a) Every connected graph G has a spanning tree.
(b) Any two spanning trees of G have the same number of edges.

Proof.
(a) If G is circuit-free it is a tree and hence its own spanning tree. If G has a circuit. Remove an edge of this circuit to get a new graph G_1. If G_1 has a circuit remove an edge from the circuit to obtain a new graph G_2. Continue until we reach a circuit-free graph, G_k for some k. G_k is a spanning tree for G.
(b) Any spanning tree of G has $|V| - 1$ edges, where $|V|$ is the number of vertices of G ■

Example 26.7
Find four spanning trees of the graph shown in Figure 26.10.

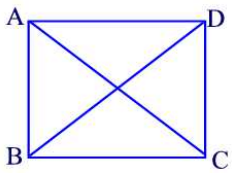


Figure 26.10

Solution.
The four spanning trees are shown in Figure 26.11 ■

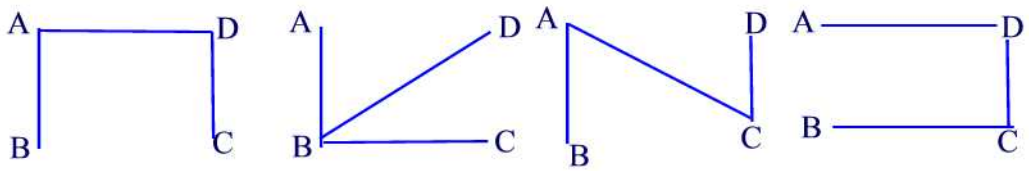
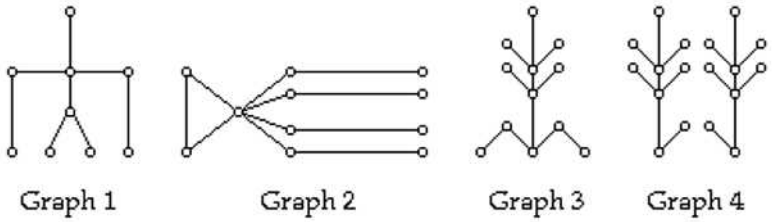


Figure 26.11

Review Problems

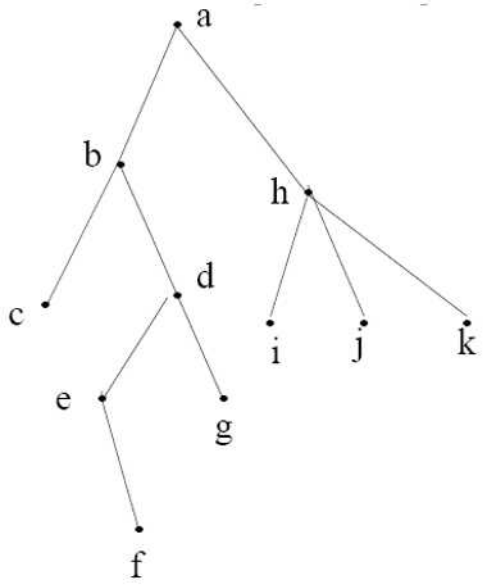
Problem 26.1
Which of the following four graphs is a tree?



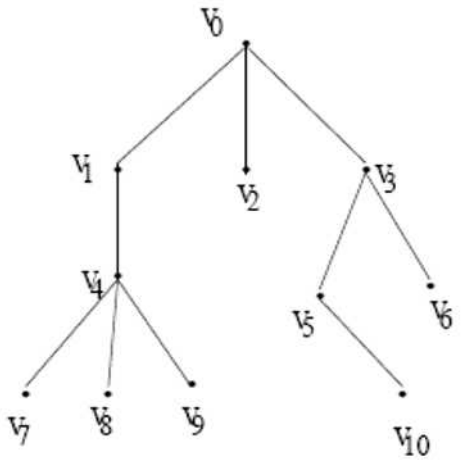
Problem 26.2
Find the number of edges in a tree with 58 vertices.

Problem 26.3
Can a graph with 41 vertices and 40 edges be a tree?

Problem 26.4
Find the level of each vertex and the height of the following rooted tree.



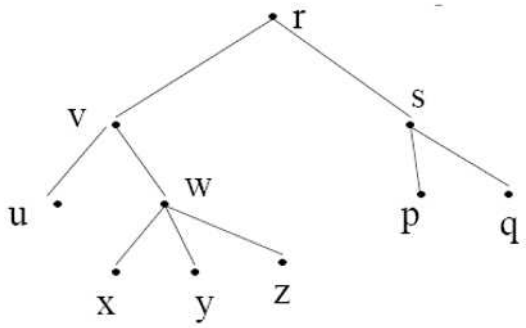
Problem 26.5
Consider the rooted tree



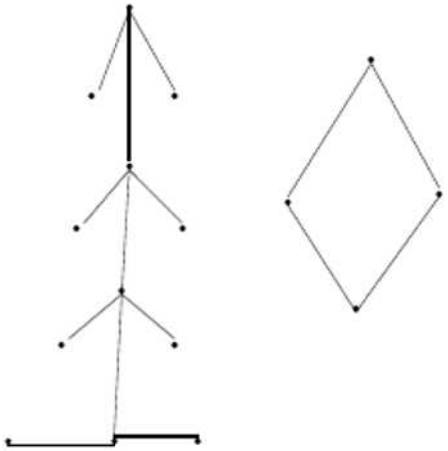
(a) Find the parent of v_6.
(b) Find the ancestors of v_{10}.
(c) Find the children of v_4.
(d) Find the descendants of v_1.
(e) Find all the siblings.
(f) Find the leaves.
(g) Construct the subtree rooted at v_1.

Problem 26.6
A **binary search tree** is a binary tree T in which data are associated with the vertices. The data are arranged so that, for each vertex v in T, each data item in the left subtree of v is less than the data item in v and each data item in the right subtree of v is greater than the data item in v. Using numerical order, form a binary search tree for a number in the set $\{1, 2, \cdots, 15\}$.

Problem 26.7
Procedures for systematically visiting every vertex of a tree are called **traversal algorithms**. In the **preorder traversal**, the root r is listed first and then the subtrees $T_1, T_2, \cdots, T_n$ are listed, from left to right, in order of their roots. The preorder traversal begins by visiting r. It continues by traversing T_1 in preorder, thenT_2 in preorder, and so on, until T_n is traversed in preorder. In which order does a preorder traversal visit the vertices in the following rooted tree?

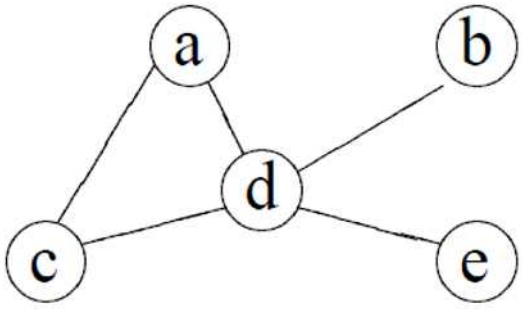


Problem 26.8
A **forest** is a simple graph with no circuits. Which of the following graphs is a forest?

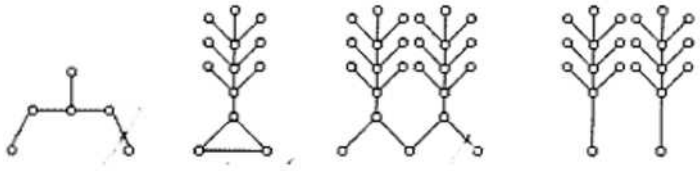


Problem 26.9
What do spanning trees of a connected graph have in common?

Problem 26.10
Find three spanning trees of the graph below.



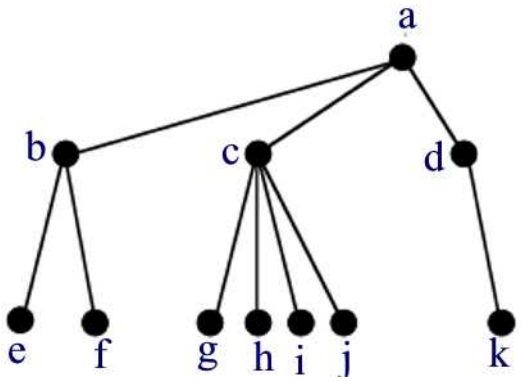
Problem 26.11
Which of the following four graphs is a tree?



Problem 26.12
What is the number of edges in a tree with 49 vertices?

Problem 26.13
Prove that a tree with n vertices has at least two leaves.

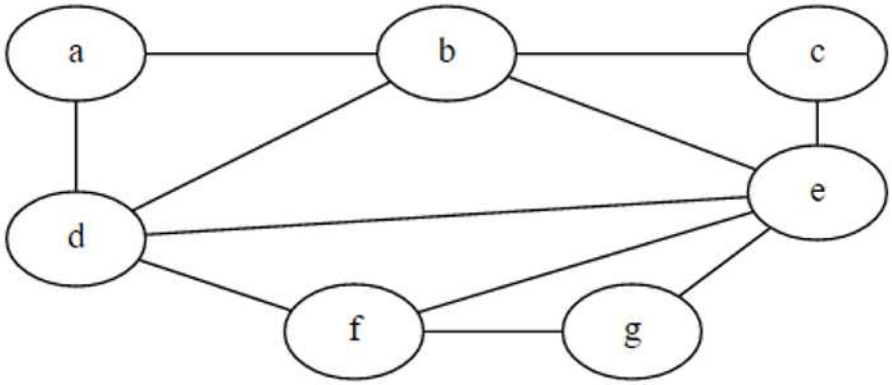
Problem 26.14
Consider the rooted tree shown below.



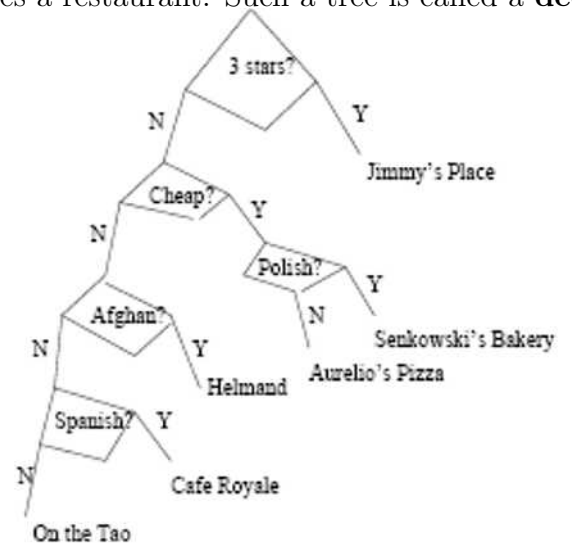
(i) Find the parent of g.
(ii) Find the ancestors of k.
(iii) Find the children of c.
(iv) Find the descendants of b.
(v) Find an example of a siblings.
(vi) Find the leaves.
(vii) Construct the subtree rooted at c.

Problem 26.15
Are the following binary trees different?

Problem 26.16
Find a spanning tree of the following graph.



Problem 26.17
The binary tree below gives an algorithm for choosing a restaurant. Each internal vertex asks a question. If we begin at the root, answer each question, and follow the appropriate edge, we will eventually arrive at a terminal vertex that chooses a restaurant. Such a tree is called a **decision tree**.



Construct a decision tree that sorts three given numbers a_1, a_2, a_3 in ascending order.

Index