Applied Discrete Structures

Alan Doerr and Kenneth Levasseur

Department Of Mathematical Sciences
University of Massachusetts Lowell

Version 2.0
March 2013

Home Blog Errata

Home: http://faculty.uml.edu/klevasseur/ADS2/
Blog: http://applieddiscretestructures.blogspot.com/
Errata: http://faculty.uml.edu/klevasseur/ADS2/errata.html

Previously published by Pearson Education, Inc. under the title *Applied Discrete Structures for Computer Science*

To our families
Donna, Christopher, Melissa, and Patrick Doerr
and
Karen, Joseph, Kathryn, and Matthew Levasseur

ISBN 978-1-105-55929-7
90000
9 781105 559297

Table of Contents

Preface - what a difference 21 years make!

Twenty-one years after the publication of the 2nd edition of *Applied Discrete Structures for Computer Science*, in 1989 the publishing and computing landscape have both changed dramatically. We signed a contract for the second edition with Science Research Associates but by the time the book was ready to print, SRA had been sold to MacMillan. Soon after, the rights had been passed on to Pearson Education, Inc. In 2010, the long-term future of printed textbooks is uncertain. In the meantime, textbook prices (both printed and e-books) have increased and a growing open source textbook market movement has started. One of our objectives in revisiting this text is to make it available to our students in an affordable format. In its original form, the text was peer-reviewed and was adopted for use at several universities throughout the country. For this reason, we see *Applied Discrete Structures* as not only an inexpensive alternative, but a high quality alternative.

As indicated above the computing landscape is very different from the 1980's and accounts for the most significant changes in the text. One of the most common programming languages of the 1980's, Pascal; and we used it to illustrate many of the concepts in the text. Although it isn't totally dead, Pascal is far from the mainstream of computing in the 21st century. In 1989, *Mathematica* had been out for less than a year — now a major force in scientific computing. The open source software movement also started in the 1980's and in 2005, the first version of Sage, an open-source alternative to *Mathematica* was first released. In *Applied Discrete Structures* we have replaced "Pascal Notes" with "*Mathematica* Notes" and "Sage Notes." Finally, 1989 was the year that World Wide Web was invented by Tim Berners-Lee. There wasn't a single www in the 2nd edition. In this version, we intend to make use of extensive web resources, including video demonstrations.

We would like to thank Tony Penta, Sitansu Mittra, and Dan Klain for using the preliminary versions of *Applied Discrete Structures*. The corrections and input they provided was appreciated.

We repeat the preface to *Applied Discrete Structures for Computer Science* below. Plans for the instructor's guide, which is mentioned in the preface are uncertain at this time.

Preface to Applied Discrete Structures for Computer Science, 2nd Ed.

We feel proud and fortunate that most authorities, including MAA and ACM, have settled on a discrete mathematics syllabus that is virtually identical to the contents of the first edition of Applied Discrete Structures for Computer Science. For that reason, very few topical changes needed to be made in this new edition, and the order of topics is almost unchanged. The main change is the addition of a large number of exercises at all levels. We have "fine-tuned" the contents by expanding the preliminary coverage of sets and combinatorics, and we have added a discussion of binary integer representation. We have also added an introduction including several examples, to provide motivation for those students who may find it reassuring to know that mathematics has "real" applications. "Appendix B—Introduction to Algorithms," has also been added to make the text more self-contained.

How This Book Will Help Students

In writing this book, care was taken to use language and examples that gradually wean students from a simpleminded mechanical approach and move them toward mathematical maturity. We also recognize that many students who hesitate to ask for help from an instructor need a readable text, and we have tried to anticipate the questions that go unasked.

The wide range of examples in the text are meant to augment the "favorite examples" that most instructors have for teaching the topics in discrete mathematics.

To provide diagnostic help and encouragement, we have included solutions and/or hints to the odd-numbered exercises. These solutions include detailed answers whenever warranted and complete proofs, not just terse outlines of proofs.

Our use of standard terminology and notation makes Applied Discrete Structures for Computer Science a valuable reference book for future courses. Although many advanced books have a short review of elementary topics, they cannot be complete.

How This Book Will Help Instructors

The text is divided into lecture-length sections, facilitating the organization of an instructor's presentation.

Topics are presented in such a way that students' understanding can be monitored through thought-provoking exercises. The exercises require an understanding of the topics and how they are interrelated, not just a familiarity with the key words.

An Instructor's Guide is available to any instructor who uses the text. It includes:

(a) Chapter-by-chapter comments on subtopics that emphasize the pitfalls to avoid;

(b) Suggested coverage times;

(c) Detailed solutions to most even-numbered exercises;

(d) Sample quizzes, exams, and final exams.

How This Book Will Help the Chairperson/Coordinator

The text covers the standard topics that all instructors must be aware of; therefore it is safe to adopt Applied Discrete Structures for Computer Science before an instructor has been selected.

The breadth of topics covered allows for flexibility that may be needed due to last-minute curriculum changes.

Since discrete mathematics is such a new course, faculty are often forced to teach the course without being completely familiar with it. An Instructor's Guide is an important feature for the new instructor.

What a Difference Five Years Makes!

In the last five years, much has taken place in regards to discrete mathematics. A review of these events is in order to see how they have affected the Second Edition of Applied Discrete Structures for Computer Science.

(1) Scores of discrete mathematics texts have been published. Most texts in discrete mathematics can be classified as one-semester or two-semester texts. The two-semester texts, such as Applied Discrete Structures for Computer Science, differ in that the logical prerequisites for a more thorough study of discrete mathematics are developed.

(2) Discrete mathematics has become more than just a computer science support course. Mathematics majors are being required to take it, often before calculus. Rather than reducing the significance of calculus, this recognizes that the material a student sees in a discrete mathematics/structures course strengthens his or her understanding of the theoretical aspects of calculus. This is particularly important for today's students, since many high school courses in geometry stress mechanics as opposed to proofs. The typical college freshman is skill-oriented and does not have a high level of mathematical maturity. Discrete mathematics is also more typical of the higher-level courses that a mathematics major is likely to take.

(3) Authorities such as MAA, ACM, and A. Ralson have all refined their ideas of what a discrete mathematics course should be. Instead of the chaos that characterized the early '80s, we now have some agreement, namely that discrete mathematics should be a course that develops mathematical maturity.

(4) Computer science enrollments have leveled off and in some cases have declined. Some attribute this to the lay-offs that have taken place in the computer industry; but the amount of higher mathematics that is needed to advance in many areas of computer science has also discouraged many. A year of discrete mathematics is an important first step in overcoming a deficiency in mathematics.

(5) The Educational Testing Service introduced its Advanced Placement Exam in Computer Science. The suggested preparation for this exam includes many discrete mathematics topics, such as trees, graphs, and recursion. This continues the trend toward offering discrete mathematics earlier in the overall curriculum.

Acknowledgments

The authors wish to thank our colleagues and students for their comments and assistance in writing and revising this text. Among those who have left their mark on this edition are Susan Assmann, Shim Berkovitz, Tony Penta, Kevin Ryan, and Richard Winslow.

We would also like to thank Jean Hutchings, Kathy Sullivan, and Michele Walsh for work that they did in typing this edition, and our department secretaries, Mrs. Lyn Misserville and Mrs. Danielle White, whose cooperation in numerous ways has been greatly appreciated.

We are grateful for the response to the first edition from the faculty and students of over seventy-five colleges and universities. We know that our second edition will be a better learning and teaching tool as a result of their useful comments and suggestions. Our special thanks to the following reviewers: David Buchthal, University of Akron; Ronald L. Davis, Millersville University; John W Kennedy, Pace University; Betty Mayfield, Hood College; Nancy Olmsted, Worcester State College; and Pradip Shrimani, Southern Illinois University. Finally, it has been a pleasure to work with Nancy Osman, our acquisitions editor, David Morrow, our development editor, and the entire staff at SRA.

A.W. D.

K.M.L.

Introduction

What Is Discrete Mathematics/Structures?

What is Discrete Mathematics?

As a general description one could say that discrete mathematics is the mathematics that deals with "separated" or discrete sets of objects rather than with continuous sets such as the real line. For example, the graphs that we learn to draw in high school are of continuous functions. Even though we might have begun by plotting discrete points on the plane, we connected them with a smooth, continuous, unbroken curve to form a straight line, parabola, circle, etc. The underlying reason for this is that hand methods of calculation are too laborious to handle huge amounts of discrete data. The computer has changed all of this.

Today, the area of mathematics that is broadly called "discrete" is that which professionals feel is essential for people who use the computer as a fundamental tool. It can best be described by looking at our Table of Contents. It involves topics like sets, logic, and matrices that students may be already familiar with to some degree. In this Introduction, we give several examples of the types of problems a student will be able to solve as a result of taking this course. The intent of this Introduction is to provide an overview of the text. Students should read the examples through once and then move on to Chapter One. After completing their study of discrete mathematics, they should read them over again.

We hope discrete mathematics is as fascinating and enjoyable to the student as it has been to us.

Example l.a. Analog-to-digital Conversion. A common problem encountered in engineering is that of analog-to-digital (a-d) conversion, where the reading on a dial, for example, must be converted to a numerical value. In order for this conversion to be done reliably and quickly, one must solve an interesting problem in graph theory. Before this problem is posed, we will make the connection between a-d conversion and the graph problem using a simple example. Suppose a dial in a video game can be turned in any direction, and that the positions will be converted to one of the numbers zero through seven in the following way. As depicted in Figure I.a.1, the angles from 0 to 360 are divided into eight equal parts, and each part is assigned a number starting with 0 and increasing clockwise. If the dial points in any of these sectors the conversion is to the number of that sector. If the dial is on the boundary, then we will be satisfied with the conversion to either of the numbers in the bordering sectors. This conversion can be thought of as giving an approximate angle of the dial, for if the dial is in sector k, then the angle that the dial makes with east is approximately 45 k°.

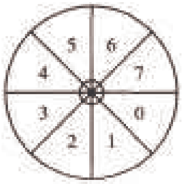


FIGURE l.a.1

Now that the desired conversion has been described, we will describe a "solution" that has one major error in it, and then identify how this problem can be rectified. All digital computers represent numbers in binary form, as a sequence of Os and Is called bits, short for binary digits. The binary representations of numbers 0 through 7 are:

$$0 = 000 = 0\times 4 + 0\times 2 + 0\times 1$$

$$1 = 001 = 0\times 4 + 0\times 2 + 1\times 1$$

$$2 = 010 = 0\times 4 + 1\times 2 + 0\times 1$$

$$3 = 011 = 0\times 4 + 1\times 2 + 1\times 1$$

$$4 = 100 = 1\times 4 + 0\times 2 + 0\times 1$$

$$5 = 101 = 1\times 4 + 0\times 2 + 1\times 1$$

$$6 = 110 = 1\times 4 + 1\times 2 + 0\times 1$$

$$7 = 111 = 1\times 4 + 1\times 2 + 1\times 1$$

We will discuss the binary number system in Chapter 1. The way that we could send those bits to a computer is by coating parts of the back of the dial with a metallic substance, as in Figure I.a.2. For each of the three concentric circles on the dial there is a small magnet. If a magnet lies under a part of the dial that has been coated with metal, then it will turn a switch ON, whereas the switch stays OFF when no metal is detected above a magnet. Notice how every ON/OFF combination of the three switches is possible given the way the back of the dial is coated.

If the dial is placed so that the magnets are in the middle of a sector, we expect this method to work well. There is a problem on certain boundaries, however. If the dial is turned so that the magnets are between sectors three and four, for example, then it is unclear what the result will be. This is due to the fact that each magnet will have only a fraction of the required metal above it to turn its switch ON. Due to expected irregularities in the coating of the dial, we can be safe in saying that for each switch either ON or OFF could be the result, and so if the dial is between sectors three and four, any number could be indicated. This problem does not occur between every sector. For example, between sectors 0 and 1, there is only one switch that cannot be predicted. No matter what the outcome is for the units switch in this case, the indicated sector must be either 0 or 1, which is consistent with the original objective that a positioning of the dial on a boundary of two sectors should produce the number of either sector.

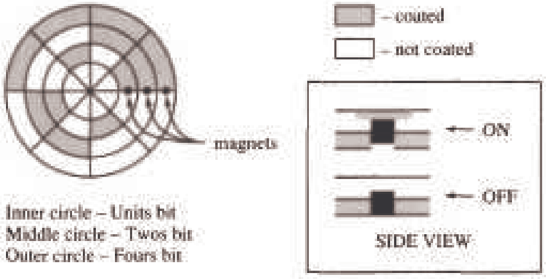


FIGURE I.a.2

Is there a way to coat the sectors on the back of the dial so that each of the eight patterns corresponding to the numbers 0 to 7 appears once, and so that between any two adjacent sectors there is only one switch that will have a questionable setting? One way of trying to answer this question is by using an undirected graph called the 3-cube (Figure I.a.3). In general, an undirected graph consists of vertices (the circled 0's and 1's in the 3-cube) and the edges, which are lines that connect certain pairs of vertices. Two vertices in the 3-cube are connected by an edge if the sequences of the three bits differ in exactly one position. If one could draw a path along the edges in the 3-cube that starts at any vertex, passes through every other vertex once, and returns to the start, then that sequence of bit patterns can be used to coat the back of the dial so that between every sector there is only one questionable switch. Such a path is not difficult to find; so we will leave it to you to find one, starting at 000 and drawing the sequence in which the dial would be coated.

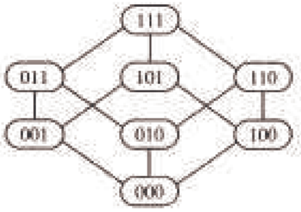


FIGURE I.a.3

Many A-D conversion problems require many more sectors and switches than this example, and the same kinds of problems can occur. The solution would be to find a path within a much larger yet similar graph. For example, there might be 1,024 sectors with 10 switches, resulting in a graph with 1,024 vertices. One of the objectives of this text will be to train you to understand the thought processes that are needed to attack such large problems. In Chapter 9 we will take a closer look at graph theory and discuss some of its applications.

One question might come to mind at this point. If the coating of the dial is no longer as it is in Figure I.a.2, how would you interpret the patterns that are on the back of the dial as numbers from 0 to 7? In Chapter 14 we will see that if a certain path is used, this "decoding" is quite easy.

The 3-cube and its generalization, the n-cube, play a role in the design of a multiprocessor called a hypercube. A multiprocessor is a computer that consists of several independent processors that can operate simultaneously and are connected to one another by a network of connections. In a hypercube with $M = 2^n$ processors, the processors are numbered 0 to $M - 1$. Two processors are connected if their binary representations differ in exactly one bit. The hypercube has proven to be the best possible network for certain problems requiring the use of a "supercomputer." Denning's article in the May-June 1987 issue of "American Scientist" provides an excellent survey of this topic.

Example I.b. Logic is the cornerstone of all communication, whether we wish to communicate in mathematics or in any other language. It is the study of sentences, or propositions, that take on the values true or false, 1 or 0 in the binary system. Its importance was recognized in the very early days of the development of logic (hardware) design, where Boolean algebra, the algebra of logic, was used to simplify electronic circuitry called gate diagrams. Consider the following gate diagram:

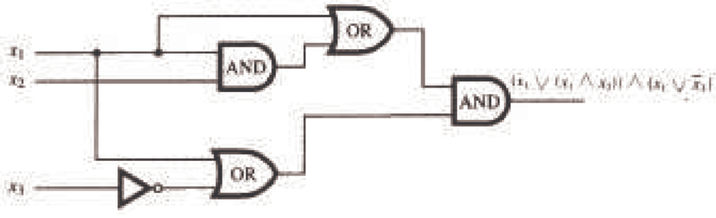


FIGURE I.b.1

Each symbol in this diagram is called a gate, a piece of hardware. In Chapter 13 we will discuss these circuits in detail. Assume that this circuitry can be placed on a chip which will have a cost dependent on the number of gates involved. A classic problem in logic design is to try to simplify this circuitry to one containing fewer gates. Indeed, the gate diagram can be reduced to

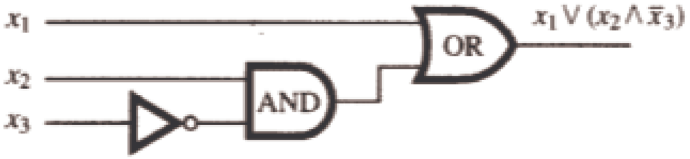


FIGURE I.b.2

The result is a less costly chip. Since a company making computers uses millions of chips, we have saved a substantial amount of money.

This use of logic is only the "tip of the iceberg." The importance of logic for computer scientists in particular, and for all people who use mathematics, cannot be overestimated. It is the means by which we can think and write clearly and precisely. Logic is used in writing algorithms, in testing the correctness of programs, and in other areas of computer science.

Example I.c. Suppose two students miss a class on a certain day and borrow the class notes in order to obtain copies. If one of them copies the notes by hand and the other walks to a "copy shop," we might ask which method is more efficient. To keep things simple, we will only consider the time spent in copying, not the cost. We add a few more assumptions: copying the first page by hand takes one minute and forty seconds (100 seconds); for each page copied by hand, the next page will take five more seconds to copy, so that it takes 1:45 to copy the second page, 1:50 to copy the third page, etc.; photocopiers take five seconds to copy one page; walking to the "copy shop" takes ten minutes, each way.

One aspect of the problem that we have not specified is the number of pages to be copied. Suppose the number of pages is n, which could be any positive integer. As with many questions of efficiency, one method is not clearly better than the other for all cases. Since the only variable in this problem is the number of pages, we can simply compare the copying times for different values of n. We will denote the time it takes (in seconds) to copy n pages manually by $t_h(n)$, and the time to copy n pages automatically by $t_a(n)$. Ideally, we would like to have formulas to represent the values of $t_h(n)$ and $t_a(n)$. The process of finding these formulas is an important one that we will examine in Chapter 8. The formula for $t_a(n)$ is not very difficult to derive from the given information. To copy pages automatically, one must walk for twenty minutes (1,200 seconds), and then for each page wait five seconds. Therefore, $t_a(n) = 1200 + 5\,n$

The formula for $t_h(n)$ isn't quite as simple. First, let $p(n)$ be the number of seconds that it takes to copy page n. From the assumptions, $p(1) = 100$, and if n is greater than one, $p(n) = p(n-1) + 5$. The last formula is called a *recurrence relation*. We will spend quite a bit of time discussing methods for deriving formulas from recurrence relations. In this case $p(n) = 95 + 5\,n$. Now we can see that if n is greater than one,

$$t_h(n) = p(1) + p(2) + \cdots + p(n) = t_h(n-1) + p(n) = t_h(n-1) + 5\,n + 95$$

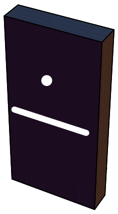
This is yet another recurrence relation. The solution to this one is $t_h(n) = 97.5\,n + 2.5\,n$.

Now that we have these formulas, we can analyze them to determine the values of n for which hand copying is most efficient, the values for which photocopying is most efficient, and also the values for which the two methods require the same amount of time.

WHAT IS DISCRETE STRUCTURES?

So far we have given you several examples of that area of mathematics called discrete mathematics. Where does the "structures" part of the title come from? We will look not only at the topics of discrete mathematics but at the structure of these topics. If two people were to explain a single concept, one in German and one in French, we as observers might at first think they were expressing two different ideas, rather than the same idea in two different languages. In mathematics we would like to be able to make the same distinction. Also, when we come upon a new mathematical structure, say the algebra of sets, we would like to be able to determine how workable it will be. How do we do this? We compare it to something we know, namely elementary algebra, the algebra of numbers. When we encounter a new algebra we ask ourselves how similar it is to elementary algebra. What are the similarities and the dissimilarities? When we know the answers to these questions we can use our vast knowledge of basic algebra to build upon rather than learning each individual concept from the beginning.

chapter 1



SET THEORY I

GOALS

In this chapter we will cover some of the basic set language and notation that will be used throughout the text. Venn diagrams will be introduced in order to give the reader a clear picture of set operations. In addition, we will describe the binary representation of positive integers (Section 1.4) and introduce summation notation and its generalizations (Section 1.5).

1.1 Set Notation and Relations

The term set is intuitively understood by most people to mean a collection of objects that are called elements (of the set). This concept is the starting point on which we will build more complex ideas, much as in-geometry where the concepts of point and line are left undefined.

Because a set is such a simple notion, you may be surprised to learn that it is one of the most difficult concepts for mathematicians to define to their own liking. For example, the description above is not a proper definition because it requires the definition of a collection. (How would you define "collection"?) Even deeper problems arise when you consider the possibility that a set could contain itself. Although these problems are of real concern to some mathematicians, they will not be of any concern to us.

Our first concern will be how to describe a set; that is, how do we most conveniently describe a set and the elements that are in it? If we are going to discuss a set for any length of time, we usually give it a name in the form of a capital letter (or occasionally some other symbol). In discussing set A, if x is an element of A, then we will write $x \in A$. On the other hand, if x is not an element of A, we write $x \notin A$. The most convenient way of describing the elements of a set will vary depending on the specific set.

Method 1: Enumeration. When the elements of a set are enumerated (or listed) it is traditional to enclose them in braces. For example, the set of binary digits is $\{0, 1\}$ and the set of decimal digits is $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. The choice of a name for these sets would be arbitrary; but it would be "logical" to call them B and D , respectively. The choice of a set name is much like the choice of an identifier name in programming. Some large sets can be enumerated without actually listing all the elements. For example, the letters of the alphabet and the integers from 1 to 100 could be described as

$A = \{a, b, c, \ldots, x, y, z\}$, and $G = \{1, 2, \ldots, 99, 100\}$.

The three consecutive "dots" are called an ellipsis. We use them when it is clear what elements are included but not listed. An ellipsis is used in two other situations. To enumerate the positive integers, we would write $\{1, 2, 3, \ldots\}$, indicating that the list goes on infinitely. If we want to list a more general set such as the integers between 1 and n, where n is some undetermined positive integer, we might write $\{1, \ldots, n\}$.

Method 2: Standard Symbols. Frequently used sets are usually given symbols that are reserved for them alone. For example, since we will be referring to the positive integers throughout this book, we will use the symbol $\mathbb{P}$ instead of writing $\{1, 2, 3, \ldots\}$. A few of the other sets of numbers that we will use frequently are:

$\mathbb{N}$ = the natural numbers = $\{0, 1, 2, 3, \ldots\}$.

$\mathbb{Z}$ = the integers = $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

$\mathbb{Q}$ = the rational numbers.

$\mathbb{R}$ = the real numbers.

$\mathbb{C}$ = the complex numbers.

Method 3: Set-Builder Notation. Another way of describing sets is to use set-builder notation. For example, we could define the rational numbers as

$$\mathbb{Q} = \{a/b : a, b \in \mathbb{Z}, b \neq 0\}$$

Note that in the set-builder description for the rational numbers:

(1) a/b indicates that a typical element of the set is a "fraction."

(2) The colon is read "such that" or "where," and is used interchangeably with a vertical line, |.

(3) $a, b \in \mathbb{Z}$ is an abbreviated way of saying a and b are integers.

(4) All commas in mathematics are read as "and."

The important fact to keep in mind in set notation, or in any mathematical notation, is that it is meant to be a help, not a hindrance. We hope that notation will assist us in a more complete understanding of the collection of objects under consideration and will enable us to describe it in a concise manner. However, brevity of notation is not the aim of sets. If you prefer to write $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$ instead of $a, b \in \mathbb{Z}$, you should do so. Also, there are frequently many different, and equally good, ways of describing sets. For example, $\{x \in \mathbb{R} \mid x^2 - 5x + 6 = 0\}$ and $\{x \mid x \in \mathbb{R} : x^2 - 5x + 6 = 0\}$ both describe the solution set $\{2, 3\}$.

A proper definition of the real numbers is beyond the scope of this text. It is sufficient to think of the real numbers as the set of points on a number line. The complex numbers can be defined using set-builder notation as $C = \{a + b i : a, b \in \mathbb{R}\}$, where $i^2 = -1$.
In the following definition we will leave the word "finite" undefined.

Definition: Finite Set. *A set is a finite set if it has a finite number of elements. Any set that is not finite is an infinite set.*

Definition: Cardinality. *Let A be a finite set. The number of different elements in A is called its cardinality and is denoted by* $|A|$.

As we will see later, there are different infinite cardinalities. We can't make this distinction now, so we will restrict cardinality to finite sets until later.

SUBSETS

Definition: Subset. *Let A and B be sets. We say that A is a subset of B (notation $A \subseteq B$) if and only if every element of A is an element of B.*

Example 1.1.1.

(a) If $A = \{3, 5, 8\}$ and $B = \{5, 8, 3, 2, 6\}$, then $A \subseteq B$.

(b) $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

(c) If $A = \{3, 5, 8\}$ and $B = \{5, 3, 8\}$, then A ⊆ B and $B \subseteq A$.

Definition: Equality. *Let A and B be sets. We say that A is equal to B (notation A = B) if and only if every element of A is an element of B and conversely every element of B is an element of A; that is, $A \subseteq B$ and $B \subseteq A$.*

Example 1.1.2.

(a) In Example 1.1.1c, $A = B$. Note that the ordering of the elements is unimportant.

(b) The number of times that an element appears in an enumeration doesn't affect a set. For example, if $A = \{1, 5, 3, 5\}$ and $B = \{1, 5, 3\}$, then $A = B$. Warning to readers of other texts: Some books introduce the concept of a multiset, in which the number of occurrences of an element matters.

A few comments are in order about the expression "if and only if" as used in our definitions. This expression means "is equivalent to saying," or more exactly, that the word (or concept) being defined can at any time be replaced by the defining expression. Conversely, the expression that defines the word (or concept) can be replaced by the word.

Occasionally there is need to discuss the set that contains no elements, namely the empty set, which is denoted by the Norwegian letter $\emptyset$. This set is also called the null set.

It is clear, we hope, from the definition of a subset, that given any set A we have $A \subseteq A$ and $\emptyset \subseteq A$. Both $\emptyset$ and A are called *improper subsets* of A. If $B \subseteq A$, $B \neq \emptyset$, and $B \neq A$, then B is called a *proper subset* of A.

EXERCISES FOR SECTION 1.1

A Exercises

1. List four elements of each of the following sets:

(a) $\{k \in \mathbb{P} \mid k - 1 \text{ is } a \text{ multiple of } 7\}$

(b) $\{x \mid x \text{ is } a \text{ fruit and } x' s \text{ skin is normally eaten}\}$

(c) $\{x \in \mathbb{Q} \mid x \in \mathbb{Z}\}$

(d) $\{2 n \mid n \in \mathbb{Z},\ n < 0\}$

(e) $\{s \mid s = 1 + 2 + \cdots + n,\ n \in \mathbb{P}\}$

2. List all elements of the following sets:

(a) $\left\{\frac{1}{n} \,\middle|\, n \in \{3, 4, 5, 6\}\right\}$

(b) $\{\alpha \in \text{ the alphabet } \mid \alpha \text{ precedes } F\}$

(c) $\{-k \mid k \in \mathbb{P}\}$

(d) $\{n^2 \mid n = -2, -1, 0, 1, 2\}$

(e) $\{n \in \mathbb{P} \mid n \text{ is a factor of } 24\}$

3, Describe the following sets using set-builder notation.

(a) $\{5, 7, 9, \ldots, 77, 79\}$

(b) the rational numbers that are strictly between -1 and 1

(c) the even integers

(d) $\{-18, -9, 0, 9, 18, 27, \ldots\}$

4. Use set-builder notation to describe the following sets:

(a) $\{1, 2, 3, 4, 5, 6, 7\}$

(b) $\{1, 10, 100, 1{,}000, 10{,}000\}$

(c) $\{1, 1/2, 1/3, 1/4, 1/5, \ldots\}$

(d) $\{0\}$

5. Let A = $\{0, 2, 3\}$, B = $\{2, 3\}$, and C = $\{1, 5, 9\}$. Determine which of the following statements are true. Give reasons for your answers.

a. $3 \in A$

b. $\{3\} \in A$

c. $\{3\} \subseteq A$

d. $B \subseteq A$

e. $A \subseteq B$

f. $\emptyset \subseteq C$

g. $\emptyset \in A$

h. $A \subseteq A$

C Exercise

6. One reason that we left the definition of a set vague is Russell's Paradox. Many mathematics and logic books contain an account of this paradox. Two references are Stoll and Quine. Find one such reference and read it.

1.2 Basic Set Operations

Definition: Intersection*. Let A and B be sets. The intersection of A and B (denoted by A $\bigcap$ B) is the set of all elements that are in both A and B. That is, A $\bigcap$ B $= \{x : x \in A$ and $x \in B)$.*

Example 1.2.1.

(a) Let $A = \{1,\ 3,\ 8\}$ and $B = \{-9,\ 22,\ 3\}$. Then $A \bigcap B = \{3\}$.

(b) Solving a system of simultaneous equations such as $x + y = 7$ and $x - y = 3$ can be viewed as an intersection. Let $A = \{(x,\ y) : x + y = 7,\ x,\ y \in \mathbb{R}\}$ and $B = \{(x,\ y) : x - y - 3,\ x,\ y \in \mathbb{R}\}$. These two sets are lines in the plane and their intersection, $A \bigcap B = \{(5,\ 2)\}$, is the solution to the system.

(c) $\mathbb{Z} \bigcap \mathbb{Q} = \mathbb{Z}$.

(d) If $A = \{3,\ 5,\ 9\}$ and $B = \{-5,\ 8\}$, then $A \bigcap B = \emptyset$.

Definition: Disjoint Sets. *Two sete are disjoint if they have no elements in common (as in Example 1.2.1 d). That is, A and B are disjoint if A $\bigcap$ B $= \emptyset$.*

Definition: Union. *Let A and B be sets. The union of A and B (denoted by A $\bigcup$ B) is the set of all elements that are in A or in B or in both A and B. That is, A $\bigcup$ B $= \{x : x \in A$ or $x \in B\}$.*

It is important to note in the set-builder notation for $A \bigcup B$, the word "or" is used in the inclusive sense; it includes the case where x is in both A and B.

Example 1.2.2.

(a) If $A = \{2,\ 5,\ 8\}$ and $B = \{7,\ 5,\ 22\}$, then $A \bigcup B = \{2,\ 5,\ 8,\ 7,\ 22\}$.

(b) $\mathbb{Z} \bigcup \mathbb{Q} = \mathbb{Q}$.

(c) $A \bigcup \emptyset = A$ for any set A.

Frequently, when doing mathematics, we need to establish a universe or set of elements under discussion. For example, the set $A = \{x : 81\,x^4 - 16 = 0\}$ contains different elements depending on what kinds of numbers we allow ourselves to use in solving the equation $81\,x^4 - 16 = 0$. This set of numbers would be our universe. For example, if the universe is the integers, then A is $\emptyset$. If our universe is the rational numbers, then A is $\{2/3,\ -2/3\}$ and if the universe is the complex numbers, then A is $\{2/3,\ -2/3,\ 2\,i/3,\ -2\,i/3\}$.

Definition: Universe. *The universe, or universal set, is the set of all elements under discussion for possible membership in a set.*

We normally reserve the letter U for a universe in general discussions.

VENN DIAGRAMS

When working with sets, as in other branches of mathematics, it is often quite useful to be able to draw a picture or diagram of the situation under consideration. A diagram of a set is called a Venn diagram. The universal set U is represented by the interior of a rectangle and the sets by disks inside the rectangle.

Example 1.2.3.

(a) $A \bigcap B$ is illustrated in Figure 1.2.1 by shading the appropriate region.

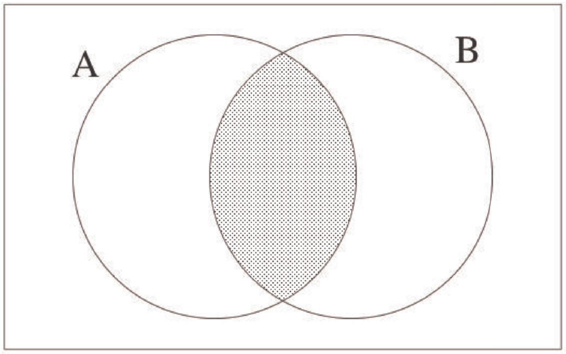


FIGURE 1.2.1 Venn diagram for intersection

(b) $A \bigcup B$ is illustrated in Figure 1.2.2.

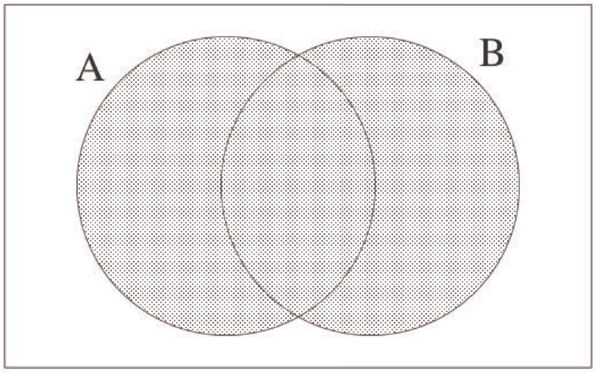


FIGURE 1.2.2 Venn diagram for union

In a Venn diagram, the region representing $A \cap B$ does not appear empty; however, in some instances it will represent the empty set. The same is true for any other region in a Venn diagram.

Definition: Complement. *Let A and B be sets. The complement of A relative to B (notation $B - A$) is the set of elements that are in B and not in A. That is, $B - A = \{x : x \in B \text{ and } x \notin A\}$. If U is the universal set, then $U - A$ is denoted by A^c and is called simply the complement of A. $A^c = \{x \in U : x \notin A\}$.*

Example 1.2.4.

(a) Let $S = \{1, 2, 3, \ldots, 10\}$ and $A = \{2, 4, 6, 8, 10\}$. Then $U - A = \{1, 3, 5, 7, 9\}$ and $A - U = \emptyset$

(b) If $U = \mathbb{R}$, then the complement of the rational numbers is the irrational numbers.

(c) $U^c = \emptyset$ and $\emptyset^c = U$.

(d) The Venn diagram of A - B is represented in Figure 1.2.3.

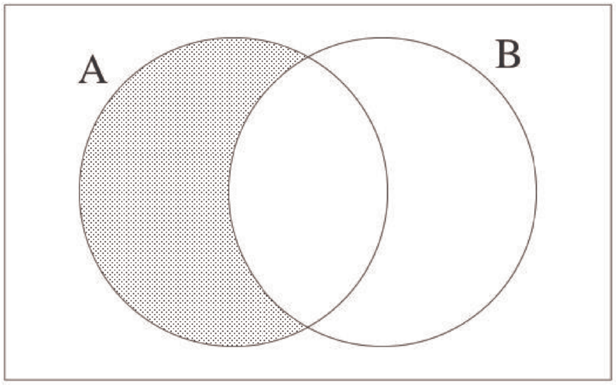


FIGURE 1.2.3 Venn diagram for $A - B$

(e) The Venn diagram of A^c is represented in Figure 1.2.4.

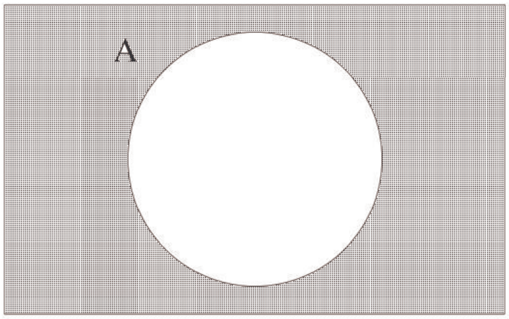


FIGURE 1.2.4 Venn diagram for A^c

(f) If $B \subseteq A$, then the Venn diagram of $A - B$ is in Figure 1.2.5.

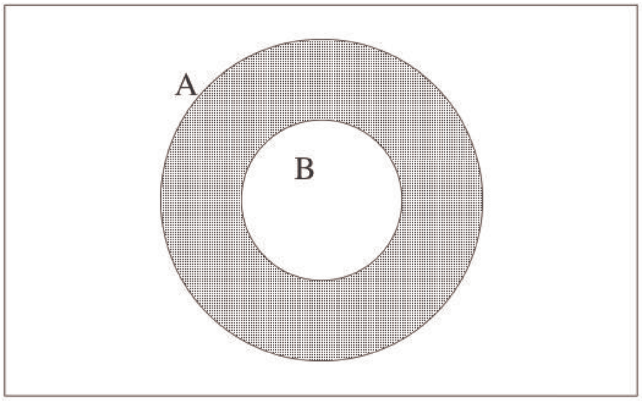


FIGURE 1.2.5 Venn diagram for $A - B$ where B is contained in A.

(g) In the universe of integers, the set of even integers, $\{\ldots, -4, -2, 0, 2, 4, \ldots\}$, has the set of odd integers as its complement.

Definition: Symmetric Difference. *Let A and B be sets. The symmetric difference of A and B (denoted by $A \oplus B$) is the set of all elements that are in AandB but not in both. That is, $A \oplus B = (A \cup B) - (A \cap B)$.*

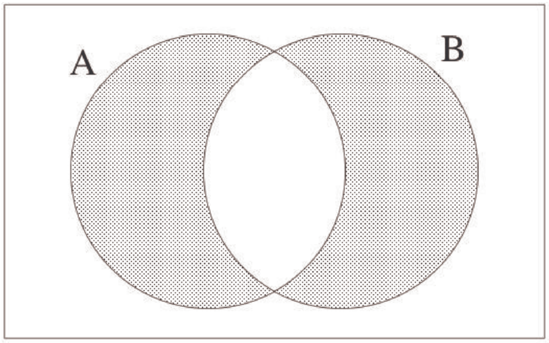
Example 1.2.5.

(a) Let $A = \{1, 3, 8\}$ and $B = \{2, 4, 8\}$. Then $A \oplus B = \{1, 2, 3, 4\}$.

(b) $A \oplus 0 = A$ and $A \oplus A = \emptyset$ for any set A.

(c) $\mathbb{R} \oplus \mathbb{Q} =$ the irrational numbers.

(d) The Venn diagram of A ⊕ B is represented in Figure 1.2.6.



Mathematica Note

One of the basic objects in *Mathematica* is a list. A list can be treated as a set. Here are a few examples. First we define **A** and **B** using the divisor function. This gives you all positive integers that divide evenly into a given positive integer, such as 525.

```
A = Divisors[525]
```

{1, 3, 5, 7, 15, 21, 25, 35, 75, 105, 175, 525}

```
B = Divisors[300]
```

{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 25, 30, 50, 60, 75, 100, 150, 300}

Here are the union and intersection of the two sets:

```
Union[A, B]
```

{1, 2, 3, 4, 5, 6, 7, 10, 12, 15, 20, 21, 25, 30, 35, 50, 60, 75, 100, 105, 150, 175, 300, 525}

```
Intersection[A, B]
```

```
{1, 3, 5, 15, 25, 75}
```

Notice the outputs from both expressions automatically sort the elements in ascending order. The intersection is quite significant. It is the set of common divisors of both 525 and 300. The largest of these divisions, 75, is the greatest common divisor of 525 and 300.

Here is the complement of **B** with respect to **A**.

```
Complement[A, B]
```

```
{7, 21, 35, 105, 175, 525}
```

There is no built-in Symmetric Difference function, but it can be defined:

```
SymmetricDifference[X_, Y_] := Complement[Union[X, Y], Intersection[X, Y]]
```

Now we can use the function:

```
SymmetricDifference[A, B]
```

```
{2, 4, 6, 7, 10, 12, 20, 21, 30, 35, 50, 60, 100, 105, 150, 175, 300, 525}
```

The empty set is { }.

```
SymmetricDifference[A, A]
```

```
{}
```

What corresponds to set-builder notation in *Mathematica* is the function **Select**. For example, the set of all integers from 1 to 1000 whose digits add up to 10 could be described in set builder notation as $\{n \in \mathbb{Z} \mid 1 \leq n \leq 1000, \text{ sum of digits of } n = 10\}$. We can produce that set using **Select**.

```
Select[Range[1, 1000], Function[n, Apply[Plus, IntegerDigits[n]] == 10]]
```

```
{19, 28, 37, 46, 55, 64, 73, 82, 91, 109, 118, 127, 136, 145, 154, 163, 172, 181, 190, 208, 217, 226,
  235, 244, 253, 262, 271, 280, 307, 316, 325, 334, 343, 352, 361, 370, 406, 415, 424, 433, 442, 451, 460,
  505, 514, 523, 532, 541, 550, 604, 613, 622, 631, 640, 703, 712, 721, 730, 802, 811, 820, 901, 910}
```

An alternate form of the second argument to this expression, using a "pure function" is

```
Select[Range[1, 1000], Apply[Plus, IntegerDigits[#]] == 10 &]
```

```
{19, 28, 37, 46, 55, 64, 73, 82, 91, 109, 118, 127, 136, 145, 154, 163, 172, 181, 190, 208, 217, 226,
  235, 244, 253, 262, 271, 280, 307, 316, 325, 334, 343, 352, 361, 370, 406, 415, 424, 433, 442, 451, 460,
  505, 514, 523, 532, 541, 550, 604, 613, 622, 631, 640, 703, 712, 721, 730, 802, 811, 820, 901, 910}
```

EXERCISES FOR SECTION 1.2

A Exercises

1. Let $A = \{0, 2, 3\}$, $B = \{2, 3\}$, $C = \{1, 5, 9\}$, and let the universal set be $U = \{0, 1, 2, \ldots, 9\}$. Determine:

(a) $A \cap B$

(b) $A \cup B$

(c) $B \cup A$

(d) $A \cup C$

(e) $A - B$

(f) $B - A$

(g) A^c

(h) C^c

(i) $A \cap C$

(j) $A \oplus B$

2. Let A, B, and C be as in Exercise 1, let $D = \{3,\ 2\}$, and let $E = \{2,\ 3,\ 2\}$. Determine which of the following are true. Give reasons for your decisions.

(a) $A = B$

(b) $B = C$

(c) $B = D$

(d) $E = D$

(e) $A \cap B = B \cap A$

(f) $A \cup B = B \cup A$

(g) $A - B = B - A$

(h) $A \oplus B = B \oplus A$

3. Let $U = \{1, 2, 3, \ldots, 9\}$. Give examples of sets A, B, and C for which:

(a) $A \cap (B \cap C) = (A \cap B) \cap C$

(b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(c) $(A \cup B)^c = A^c \cap B^c$

(d) $A \cup A^c = U$

(e) $A \subseteq A \cup B$

(f) $A \cap B \subseteq A$

4. Let $U = \{1,\ 2,\ 3,\ \ldots,\ 9\}$. Give examples to illustrate the following facts:

(a) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

(b) $A - B \neq B - A$

(c) If $U = A \cup B$ and $\mathrm{A} \cap \mathrm{B} = \emptyset$, it always follows that $A = U - B$.

(d) $A \times (B \cap C) = (A \times B) \cap (A \times C)$

B Exercises

5. What can you say about A if $U = \{1,\ 2,\ 3,\ 4,\ 5\}$, $B = \{2,\ 3\}$, and (separately)

(a) $A \cup B = \{1,\ 2,\ 3, 4\}$

(b) $A \cap B = \{2\}$

(c) $A \oplus B = \{3,\ 4,\ 5\}$

6. Suppose that U is an infinite universal set, and A and B are infinite subsets of U. Answer the following questions with a brief explanation.

(a) Must A^c be finite?

(b) Must $A \cup B$ infinite?

(c) Must $A \cap B$ be infinite?

7. Given that U = all students at a university, D = day students, M = mathematics majors, and G = graduate students. Draw Venn diagrams illustrating this situation and shade in the following sets:

(a) evening students

(b) undergraduate mathematics majors

(c) non-math graduate students

(d) non-math undergraduate students

8. Let the sets D, M, G, and U be as in exercise 7. Let $|U| = 16,000$, $|D| = 9,000$, $|M| = 300$, and $|G| = 1,000$. Also assume that the number of day students who are mathematics majors is 250, fifty of whom are graduate students, that there are 95 graduate mathematics majors, and that the total number of day graduate students is 700. Determine the number of students who are:

(a) evening students

(b) nonmathematics majors

(c) undergraduates (day or evening)

(d) day graduate nonmathematics majors

(e) evening graduate students

(f) evening graduate mathematics majors

(g) evening undergraduate nonmathematics majors

C Exercise

9. (a) Evaluate the following expressions in *Mathematica* to learn more about **`Select`** and to learn about **`PrimeQ`**.

```
? Select

? PrimeQ
```

(b) Use *Mathematica* to list all primes between 2000 and 2099, inclusive.

10. (a) Evaluate the following expression in *Mathematica* to learn about **`SquareFree`**

```
? SquareFreeQ
```

(b) Use *Mathematica* to list all square-free integers between 2000 and 2099, inclusive.

1.3 Cartesian Products and Power Sets

Definition: Cartesian Product. *Let A and B be sets. The Cartesian product of A and B, denoted by* $A \times B$, *is defined as follows:* $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$, *that is,* $A \times B$ *is the set of all possible ordered pairs whose first component comes from A and whose second component comes from B.*

Example 1.3.1. Notation in mathematics is often developed for good reason. In this case, a few examples will make clear why the symbol × is used for Cartesian products.

(a) Let A = {1, 2, 3} and B = {4, 5}. Then A × B = {(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5)}. Note that $|A \times B| = 6 = |A| \times |B|$.

(b) $A \times A = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$. Note that $|A \times A| = 9 = |A|^2$.

These two examples illustrate the general rule: If A and B are finite sets, then $|A \times B| = 6 = |A| \times |B|$.

We can define the Cartesian product of three (or more) sets similarly. For example, $A \times B \times C = \{(a, b, c) : a \in A, b \in B, c \in C\}$. It is common to use exponents if the sets in a Cartesian product are the same:

$$A^2 = A \times A \ ,$$

$$A^3 = A \times A \times A$$

$$\ldots$$

and in general,

$$A^n = \{(a_1, a_2, \ldots, a_n) : \text{each } a \in A\}.$$

Power Sets

Definition: Power Set. *If A is any set, the power set of A is the set of all subsets of A, denoted* $\mathcal{P}(A)$.

The two extreme cases, theempty set and all of A, are both included in $\mathcal{P}(A)$.

Example 1.3.2.

(a) $\mathcal{P}(\emptyset) = \{\emptyset\}$

(b) $\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$

(c) $\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

We will leave it to you to guess at a general formula for the number of elements in the power set of a finite set. In Chapter 2, we will discuss counting rules that will help us derive this formula.

EXERCISES FOR SECTION 1.3

A Exercises

1. Let $A = \{0, 2, 3\}$, $B = \{2, 3\}$, $C = \{1, 4\}$, and let the universal set be $U = \{0, 1, 2, 3, 4\}$. List the elements of

(a) $A \times B$

(b) $B \times A$

(c) $A \times B \times C$

(d) $U \times \emptyset$

(e) $A \times A^c$

(f) B^2

(g) B^3

(h) $B \times \mathcal{P}(B)$

2. Suppose that you are about to flip a coin and then roll a die. Let A = {HEAD, TAIL} and B = {1, 2, 3, 4, 5, 6}.

(a) What is $|A \times B|$?

(b) How could you interpret the set $A \times B$?

3. List all two-element sets in $\mathcal{P}(\{a, b, c\})$

4. List all three-element sets in $\mathcal{P}(\{a, b, c, d\})$.

5. How many singleton (one-element) sets are there in $\mathcal{P}(A)$ if $|A| = n$?

6. A person has four coins in his pocket: a penny, a nickel, a dime, and a quarter. How many different sums of money can he take out if he removes 3 coins at a time?

7. Let $A = \{+, -\}$ and $B = \{00, 01, 10, 11\}$.

(a) List the elements of $A \times B$

(b) How many elements do A^4 and $(A \times B)^3$ have?

B Exercises

8. Let $A = \{●, □, ⊗\}$ and $B = \{□, ⊖, ●\}$.

(a) List the elements of $A \times B$ and $B \times A$. The parentheses and comma in an ordered pair are not necessary in cases such as this where the elements of each set are individual symbol.

(b) Identify the intersection of $A \times B$ and $B \times A$. for the case above, and then guess at a general rule for the intersection of $A \times B$ and $B \times A$. where A and B are any two sets.

9. Let A and B be nonempty sets. When are $A \times B$ and $B \times A$. equal?

1.4 Binary Representation of Positive Integers

Recall that the set of positive integers, $\mathbb{P}$, is $\{1, 2, 3, \ldots\}$. Positive integers are naturally used to count things. There are many ways to count and many ways to record, or represent, the results of counting. For example, if we wanted to count five hundred twenty-three apples, we might group the apples by tens. There would be fifty-two groups of ten with three single apples left over. The fifty-two groups of ten could be put into five groups of ten tens (hundreds), with two tens left over. The five hundreds, two tens, and three units is recorded as 523. This system of counting is called the base ten positional system, or decimal system. It is quite natural for us to do grouping by tens, hundreds, thousands, . . . , since it is the method that all of us use in everyday life.

The term positional refers to the fact that each digit in the decimal representation of a number has a significance based on its position. Of course this means that rearranging digits will change the number being described. You may have learned of numeraton systems in which the position of symbols does not have any significance (e.g., the ancient Egyptian system). Most of these systems are merely curiosities to us now.

The binary number system differs from the decimal number system in that units are grouped by twos, fours, eights, etc. That is, the group sizes are powers of two instead of powers of ten. For example, twenty-three can be grouped into eleven groups of two with one left over. The eleven twos can be grouped into five groups of four with one group of two left over. Continuing along the same lines, we find that twenty-three can be described as one sixteen, zero eights, one four, one two, and one one, which is abbreviated $10\,111_{\text{two}}$, or simply 10111 if the context is clear.

The process that we used to determine the binary representation of 23 can be described in general terms to determine the binary representation of any positive integer n. A general description of a process such as this one is called an algorithm. Since this is the first algorithm in the book, we will first write it out using less formal language than usual, and then introduce some "algorithmic notation."

Step One: Start with an empty list of bits.

Step Two: Assign the variable **k** the value n.

Step Three: While **k**'s value is positive, continue doing the following three steps, and when **k** becomes zero, stop. First, divide **k** by 2, obtaining a quotient **q** (often denoted k div 2) and a remainder **r** (denoted k mod 2). Second, attach **r** to the left-hand side of the list of bits. Third, assign the variable **k** the value of **q**.

Example 1.4.1. Determine the binary representation of 41.

$\boldsymbol{k} = 2\times \boldsymbol{q} + r \longrightarrow$ add r to the list

$41 = 2 \times 20 + 1$ List = 1

$20 = 2 \times 10 + 0$ List = 01

$10 = 2\times 5 + 0$ List = 001

$5 = 2\times 2 + 1$ List =1001

$2 = 2\times 1 + 0$ List = 01001

$1 = 2 \times 0 + 1$ List = 101001

Therefore, $41 = 101\,001_{\text{two}}$

The notation that we will use to describe this algorithm and all others is called pseudocode, an informal variation of the instructions that are commonly used in many computer languages. Read the following description carefully, comparing it with the informal description above. Appendix B, which contains a general discussion of the components of the algorithms in this book, should clear up any lingering questions. Anything after // are comments.

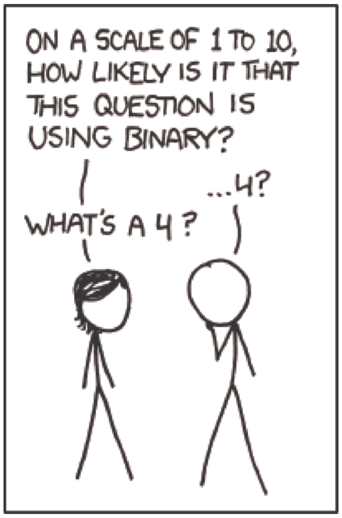
Algorithm 1.4.1: Algorithm for Determining the Binary Representation of a Positive Integer.

Input: a positive integer n.

Output: the binary representation of n in the form of a list of bits, with units bit last, twos bit next to last, etc.

```
(1) k:=n                        //initialize k
(2) L := an empty list          //initialize L
(3) While k > 0 do
     (3.1)  q := k div 2        //divide k by 2
            r:=  k mod 2
     (3.2) L: = prepend r to L  //Add r to the front of L
     (3.3) k:= q                //reassign k
```

Now that you've read this section, you should get this joke from the xkcd.com.


ON A SCALE OF 1 TO 10, HOW LIKELY IS IT THAT THIS QUESTION IS USING BINARY?
WHAT'S A 4?
...4?

EXERCISES FOR SECTION 1.4

A Exercises

1. Find the binary representation of each of the following positive integers: (a) 31 (b) 32 (c) 10 (d) 100

2. Find the binary representation of each of the following positive integers: (a) 64 (b) 67 (c) 28 (d) 256

3. What positive integers have the following binary representations? (a) 10010 (b) 10011 (c) 101010 (d) 10011110000

4. What positive integers have the following binary representations? (a) 100001 (b) 1001001 (c) 1000000000 (d) 1001110000

5. The example, decimal 1000 has 10 bits since it is $1\,111\,101\,000_{\text{two}}$ You might save some time by thinking of how 10 can be arrived at without finding the exact binary representation. How many bits do the binary representations of the following decimal numbers have?

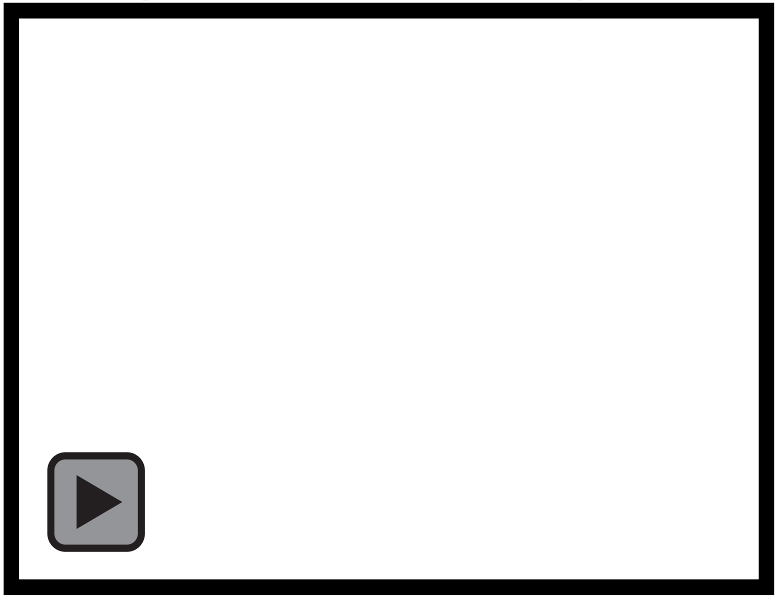
(a) 2011 (b) 4000 (c) 4500 (d) 2^{50}

B Exercises

6. Let m be a positive integer with n-bit binary representation: $a_{n-1}\, a_{n-2} \cdots a_1\, a_0$ with $a_{n-1} = 1$ What are the smallest and largest values that m could have?

7. If a positive integer is a multiple of 100, we can identify this fact from its decimal representation, since it will end with two zeros. What can you say about a positive integer if its binary representation ends with two zeros?

8. Can a multiple of ten be easily identified from its binary representation?



1.5 Summation Notation and Generalizations

Most operations such as addition of numbers are introduced as binary operations. That is, we are taught that two numbers may be added together to give us a single number. Before long, we run into situations where more than two numbers are to be added. For example, if four numbers, a_1, a_2, a_3, and a_4 are to be added, their sum may be written down in several ways, such as $((a_1 + a_2) + a_3) + a_4$ or $(a_1 + a_2) + (a_3 + a_4)$. In the first expression, the first two numbers are added, the result is added to the third number, and that result is added to the fourth number. In the second expression the first two numbers and the last two numbers are added and the results of these additions are added. Of course, we know that the final results will be the same. This is due to the fact that addition of numbers is an associative operation. For such operations, there is no need to describe how more than two objects will be operated on.

A sum of numbers such as $a_1 + a_2 + a_3 + a_4$ is called a series and is often written $\sum_{k=1}^{4} a_k$ in what is called summation notation.

We first recall some basic facts about series that you probably have seen before. A more formal treatment of sequences and series is covered in Chapter 8. The purpose here is to give the reader a working knowledge of summation notation and to carry this notation through to intersection and union of sets and other mathematical operations.

A finite series is an expression such as $a_1 + a_2 + a_3 + \ldots + a_n = \sum_{k=1}^{n} a_k$

In 2 a,, / is referred to as the index, or the index of summation; the value below the summation symbol is the initial index and the value above the summation symbol is the terminal index. The a, are called the terms of the series. The initial index of a summation may be different from 1.

Example 1.5.1.

(a) $\sum_{i=1}^{4} a_i = a_1 + a_2 + a_3 + a_4$

(b) $\sum_{k=0}^{5} b_k = b_0 + b_1 + b_2 + b_3 + b_4 + b_5$

(c) $\sum_{i=-2}^{2} c_i = c_{-2} + c_{-1} + c_0 + c_1 + c_2$

Example 1.5.2. If the terms in series are more specific, the sum can often be simplified. For example,

(a) $\sum_{i=1}^{4} i^2 = 1^2 + 2^2 + 3^2 + 4^2 = 30$

(b) $$\begin{aligned}\sum_{i=1}^{5} (2\,i - 1) &= (2 \times 1 - 1) + (2 \times 2 - 1) + (2 \times 3 - 1) + (2 \times 4 - 1) + (2 \times 5 - 1)\\ &= 1 + 3 + 5 + 7 + 9\\ &= 25\end{aligned}$$

Summation notation can be generalized to many mathematical operations, for example,

$$A_1 \cap A_2 \cap A_3 \cap A_4 = \bigcap_{i=1}^{4} A_i$$

Definition: Generalized Set Operations. *Let A_1, A_2, …, A_n be sets, then:*

(1) $A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$

(1) $A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$

(1) $A_1 \times A_2 \times \cdots \times A_n = \mathop{\times}_{i=1}^{n} A_i$

(1) $A_1 \oplus A_2 \oplus \cdots \oplus A_n = \bigoplus_{i=1}^{n} A_i$

Example 1.5.3. If $A_1 = \{0, 2, 3\}$, $A_2 = \{1, 2, 3, 6\}$, and $A_3 = \{-1, 0, 3, 9\}$, then

$$\bigcap_{i=1}^{4} A_i = A_1 \cap A_2 \cap A_3 = \{3\}$$

and

$$\bigcup_{i=1}^{4} A_i = A_1 \bigcup A_2 \bigcup A_3 = \{-1, 0, 1, 2, 3, 6, 9\}$$

With this notation it is quite easy to write lengthy expressions in a fairly compact form. For example, the statement

$$A \bigcap (B_1 \bigcup B_2 \bigcup \cdots \bigcup B_n) = (A \bigcap B_1) \bigcup (A \bigcap B_2) \bigcup \cdots \bigcup (A \bigcap B_n)$$

becomes

$$A \bigcap \left(\bigcup_{i=1}^{n} B_i \right) = \bigcup_{i=1}^{n} (A \bigcap B_n)$$

EXERCISES FOR SECTION 1.5

A Exercises

1. Calculate the following series:

(a) $\sum_{i=1}^{3} (2 + 3\,i)$

(b) $\sum_{i=-2}^{1} i^2$

(c) $\sum_{j=0}^{n} 2^j$ for $n = 1, 2, 3, 4$

(d) $\sum_{k=1}^{n} (2\,k - 1)$ for $n = 1, 2, 3, 4$

2. Calculate the following series:

(a) $\sum_{k=1}^{3} i^n$ for $n = 1, 2, 3, 4$

(b) $\sum_{i=1}^{5} 20$

(c) $\sum_{j=0}^{3} (n^j + 1)$ for $n = 1, 2, 3, 4$

(d) $\sum_{k=-n}^{n} k$ for $n = 1, 2, 3, 4$

3. (a) Express the formula $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$ without using summation notation.

(b) Verify this formula for $n = 3$.

(c) Repeat parts (a) and (b) for $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$

4. Verify the following properties for $n = 3$.

(a) $\sum_{i=1}^{n} (a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i$

(b) $c\left(\sum_{i=1}^{n} a_i\right) = \sum_{i=1}^{n} c\,a_i$

5. Rewrite the following without summation sign for $n = 3$. It is not necessary that you understand or expand the notation $\binom{n}{k}$ at this point.

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

6. (a) Draw the Venn diagram for $\bigcap_{i=1}^{4} A_i$.

(b) Express in "expanded format":

$$A \cup \left(\bigcap_{i=1}^{n} B_i \right) = \bigcap_{i=1}^{n} (A \cup B_n).$$

7. For any positive integer k, let $A_k = \{x \in \mathbb{Q} : k - 1 < x \leq k\}$ and $B_k = \{x \in \mathbb{Q} : -k < x < k\}$. What are the following sets?

(a) $\bigcup_{i=1}^{5} A_i$

(b) $\bigcup_{i=1}^{5} B_i$

(c) $\bigcap_{i=1}^{5} A_i$

(d) $\bigcap_{i=1}^{5} B_i$

8. For any positive integer k, let $A = \{x \in \mathbb{Q} : 0 < x < 1/k\}$ and $B_k = \{x \in \mathbb{Q} : 0 < x < k\}$. What are the following sets?

(a) $\bigcup_{i=1}^{\infty} A_i$

(b) $\bigcup_{i=1}^{\infty} B_i$

(c) $\bigcap_{i=1}^{\infty} A_i$

(d) $\bigcap_{i=1}^{\infty} B_i$

9. The symbol Π is used for the product of numbers in the same way that Σ is used for sums. For example,

$$\prod_{i=1}^{5} x_i = x_1 \, x_2 \, x_3 \, x_4 \, x_5$$

Evaluate the following:

(a) $\prod_{i=1}^{3} i^2$

(b) $\prod_{i=1}^{3} (2\,i + 1)$

10. Evaluate

(a) $\prod_{k=0}^{3} 2^k$

(b) $\prod_{k=1}^{100} \frac{k}{k+1}$

SUPPLEMENTARY EXERCISES FOR CHAPTER 1

Section 1.1

1. Enumerate the elements in the following sets:

(a) $\{x \in \mathbb{R} \mid x^2 - 3x + 2 = 0\}$

(b) $\{x \in \mathbb{R} \mid x^2 + 1 = 0\}$

(c) $\{x \in \mathbb{C} \mid x^2 + 1 = 0\}$

Section 1.2

2. Let $U = \{0, 1, 2, 3, \ldots, 9\}$, $A = \{0, 2, 3\}$, $B = \{2, 3\}$, $C = \{1, 5, 9\}$.

Determine:

(a) $(A \cup B) \cap C$

(b) $A^c \cap B^c$

(c) $(A \cup B)^c$

3. Let $U = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $A = \{x \in U$: x is a multiple of 3$\}$, and $B = \{x \in U: x^2 - 5 \geq 0\}$.

Determine:

(a) $A \cup B$

(b) $A \cap B$

(c) B^c

4. Let A, B, and C be subsets of some universal set U. Draw Venn diagrams to illustrate each of the following expressions:

(a) $(A \cap B)^c$ (e) $A^c \cap B^c \cap C^c$

(b) $A^c \cup B^c$ (f) $A^c \cap B^c \cup C^c$

(c) $A \cap (B \cup C)$ (g) $A^c \cap (B \cup C)^c$

(d) $(A \cap B) \cup (A \cap C)$ (h) $(A^c \cap B^c) \cup (A^c \cap C^c)$

5. Let $A = \{1,2,3,4,5,6\}$, $B = \{2,5,7,9, 12\}$, and $C = \{4,7,9,15,23\}$.

(a) Verify the formula: $\#(A \cup B) = \#A + \#B - \#(A \cap B)$ for this example.

(b) Use the formula in part (a) to compute:

$\#(A \cup C)$, $\#(B \cup C)$, $\#(A \cap B)$

(c) Use the formula of part (a) to derive a formula for $\#(A \cup B \cup C)$. Verify your formula for this example.

6. $U = \{1, 2, 3, 4, 5, 6, 7, 8\}$, $A = \{a \in U \mid a^2$ is even$\}$, and $B = \{a \in U \mid$ a + 1 is a multiple of three$\}$

(a) $A = \{$____$\}$ (List)

(b) $B = \{$____$\}$ (List)

(c) $A^c =$ ____

(d) $A \cap B =$____

Section 1.3

7. Let $U = \{0, 1, 2, 3, \ldots, 9\}$, $A = \{2, 4, 6\}$, $B = \{4\}$, $C = \{1, 5\}$.

Determine:

(a) B^2 (d) $B \times A$

(b) $A \times B$ (e) $(A \times B) \times C$

(c) B^3

8. Let A, B, and C be sets where $|A| = 2$, $|B| = 3$, and $|C| = 4$.

(a) Give an example showing that $A \times B \times C \neq A \times C \times B$, and explain why the two sets are not equal.

(b) Is $|A \times B \times C| = |A \times C \times B|$

9. Let $A = \{1, 2\}$. Determine $|\mathcal{P}(A) \times \mathcal{P}(A)|$ and then list all elements of $\mathcal{P}(A) \times \mathcal{P}(A)$.

10. Let $A = \{a, b, c, d\}$. Determine which of the following are true:

(a) $\{b\} \in \mathcal{P}(\text{A})$ (d) $b \in \mathcal{P}(A)$

(b) $A \in \mathcal{P}(\text{A})$ (e) $\emptyset \in \mathcal{P}(A)$

(c) $\mathcal{P}(\text{A}) \in \mathcal{P}(\text{A})$ (f) $\mathcal{P}(A) \subseteq \mathcal{P}(A)$

Section 1.4

11. The addition rules for binary numbers are:

$0 + 0 = 0$,

$1 + 0 = 0 + 1 = 1$,

$1 + 1 = 0$ and carry 1 to the next column

and $1 + 1 + 1 = 1$ and carry 1 to the next column.

$$\begin{array}{lrl} \text{For example:} & 11111 & \longleftarrow \text{carries} \\ 31_{\text{ten}} = & 11111 & \\ 11_{\text{ten}} = & \underline{1011} & \\ & 101010 = 42_{\text{ten}} & \end{array}$$

Express and compute the following sums with binary numbers; verify your result by converting back to base ten.

(a) $31 + 32$ (b) $64 + 11$ (c) $13 + 15 + 9$

12. Compute the following sums and express the result in both binary and decimal form.

(a) $10010 + 10011$ (c) $1101.11 + 100.1$

(b) $101001 + 1101$

13. Multiplication of binary numbers is a process similar to decimal multiplication. The rules for binary multiplication are: $0 \cdot 0 = 0$, $1 \cdot 0 = 0 \cdot 1 = 0$, $1 \cdot 1 = 1$. Compute the following products and verify by converting numbers to base ten:

(a) $1001 \cdot 11$ (b) $1001 \cdot 1101$

14. How are multiplication and division by two accomplished in the binary number system?

Section 1.5

15. Let $A_n = \{k \in \mathbb{N} : k \leq 3n\}$ for each $n \in \mathbb{N}$. List the elements.

(a) A_n for $n = 0, 1, 2, 3$

(b) $\bigcap_{n=1}^{3} A_n$

(c) $\bigcap_{n=0}^{3} A_n$

(d) $\bigcup_{n=1}^{3} A_n$

(e) $\bigcup_{n=0}^{3} A_n$

16. Expand each of the following and convince yourself that they are true. Assume that $m, n \in \mathbb{N}$ with m $<$ n, and c, $x_n \in \mathbb{R}$.

(a) $\displaystyle\sum_{i=1}^{n} x_i = \sum_{i=1}^{n-1} x_i + x_n$

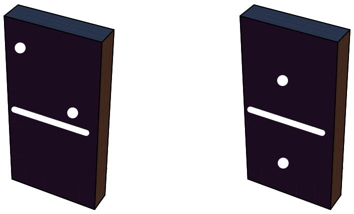
(b) $\displaystyle\sum_{i=1}^{n} (x_i + y_i) = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i$

(c) $\displaystyle\sum_{i=1}^{n} c\, x_i = c \sum_{i=1}^{n} x_i$

(d) $\displaystyle\sum_{i=1}^{n} x_i = \sum_{i=1}^{m} x_i + \sum_{i=m+1}^{n} x_i$

17. Which of the above are true if $+$ is replaced with $\cdot$ and $\sum$ is replaced with $\prod$? Explain.

chapter 2



COMBINATORICS

GOALS

Throughout this book we will be counting things. In this chapter we will outline some of the tools that will help us count.

Counting occurs not only in highly sophisticated applications of mathematics to engineering and computer science but also in many basic applications. Like many other powerful and useful tools in mathematics, the concepts are simple; we only have to recognize when and how they can be applied.

2.1 Basic Counting Techniques—The Rule of Products

WHAT IS COMBINATORICS?

One of the first concepts our parents taught us was the "art of counting." We were taught to raise three fingers to indicate that we were three years old. The question of "how many" is a natural and frequently asked question. Combinatorics is the "art of counting." It is the study of techniques that will help us to count the number of objects in a set quickly. Highly sophisticated results can be obtained with this simple concept. The following examples will illustrate that many questions concerned with counting involve the same process.

Example 2.1.1. A snack bar serves five different sandwiches and three different beverages. How many different lunches can a person order? One way of determining the number of possible lunches is by listing or enumerating all the possibilities. One systematic way of doing this is by means of a tree, as in Figure 2.1.1.

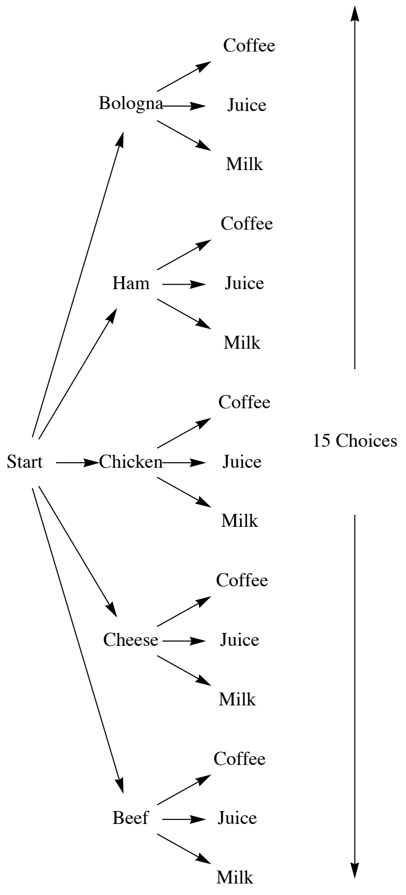


FIGURE 2.1.1 Tree solution for Example 2.1.1

Every path that begins at the position labeled START and goes to the right can be interpreted as a choice of one of the five sandwiches followed by a choice of one of the three beverages. Note that considerable work is required to arrive at the number fifteen this way; but we also get more than just a number. The result is a complete list of all possible lunches. If we need to answer a question that starts with "How many . . . ," enumeration would be done only as a last resort. In a later chapter we will examine more enumeration techniques.

An alternative method of solution for this example is to make the simple observation that there are five different choices for sandwiches and three different choices for beverages, so there are $5 \cdot 3 = 15$ different lunches that can be ordered.

A listing of possible lunches a person could have is: {(BEEF, milk), (BEEF, juice), (BEEF, coffee), ..., (BOLOGNA, coffee)}.

Example 2.1.2. Let $A = \{a, b, c, d, e\}$ and $B = \{1, 2, 3\}$. From Chapter 1 we know how to list the elements in $A \times B = \{(a, 1), (a, 2), (a, 3), ..., (e, 3)\}$. The reader is encouraged to compare Figure 2.1.1 for this example. Since the first entry of each pair can be any one of the five elements a, b, c, d, and e, and since the second can be any one of the three numbers 1, 2, and 3, it is quite clear there are $5 \cdot 3 = 15$ different elements in A x B.

Example 2.1.3. A person is to complete a true-false questionnaire consisting often questions. How many different ways are there to answer the questionnaire? Since each question can be answered either of two ways (true or false), and there are a total of ten questions, there are $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10} = 1024$ different ways of answering the questionnaire. The reader is encouraged to visualize the tree diagram of this example, but not to draw it!

We formalize the procedures developed in the previous examples with the following rule and its extension.

THE RULE OF PRODUCTS

Rule Of Products: If two operations must be performed, and If the first operation can always be performed p_1 different ways and the second operation can always be performed p_2 different ways, then there are $p_1 \cdot p_2$ different ways that the two operations can be performed.

Note: It is important that p_2 does not depend on the option that is chosen in the first operation. Another way of saying this is that p_2 is independent of the first operation. If p_2 is dependent on the first operation, then the rule of products does not apply.

Example 2.1.4. Assume in Example 2.1.1 that coffee is not served with a beef or chicken sandwich, then by inspection of Figure 2.1.1 we see that there are only thirteen different choices for lunch. The rule of products does not apply, since the choice of beverage depends on one's choice of a sandwich.

Extended Rule Of Products. The rule of products can be extended to include sequences of more than two operations. If n operations must be performed, and the number of options for each operation is $p_1, p_2, \ldots$, and p_n, respectively, with each p_i independent of previous choices, then the n operations can be performed

$$p_1 \cdot p_2 \cdot \cdots \cdot p_n = \prod_{i=1}^{n} p_i$$

Example 2.1.5. A questionnaire contains four questions that have two possible answers and three questions with five possible answers. Since the answer to each question is independent of the answers to the other questions, the extended rule of products applies and there are $2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 5 = 2^4 5^3 = 2000$ different ways to answer the questionnaire. In Chapter 1 we introduced the power set of a set A, P(A), which is the set of all subsets of A. Can we predict how many elements are in P(A) for a given finite set A? The answer is yes, and in fact $|\mathcal{P}(A)| = 2^n$. The ease with which we can prove this fact demonstrates the power and usefulness of the rule of products. Do not underestimate the usefulness of simple ideas.

Theorem 2.1.1. *If A is a finite set, then* $|\mathcal{P}(A)| = 2^{|A|}$.

Proof: Let $B \in \mathcal{P}(A)$ and assume $|A| = n$. Then for each element $x \in A$ there are two choices, either $x \in B$ of $x \notin B$. Since there are n elements of A we have, by the rule of products, $\underbrace{2 \cdot 2 \cdot \cdots \cdot 2}_{n \text{ factors}} = 2^n$ different subsets of A. Therefore, $|\mathcal{P}(A)| = 2^n$ ■

EXERCISES FOR SECTION 2.1

A Exercises

1. In horse racing, to bet the "daily double" is to select the winners of the first two races of the day. You win only if both selections are correct. In terms of the number of horses that are entered in the first two races, how many different daily double bets could be made?

2. Professor Shortcut records his grades using only his students' first and last initials. What is the smallest class size that will definitely force Prof. S. to use a different system?

3. A certain shirt comes in four sizes and six colors. One also has the choice of a dragon, an alligator, or no emblem on the pocket. How many different shirts could you order?

4. A builder of modular homes would like to impress his potential customers with the variety of styles of his houses. For each house there are blueprints for three different living rooms, four different bedroom configurations, and two different garage styles. In addition, the outside can be finished in cedar shingles or brick. How many different houses can be designed from these plans?

5. The Pi Mu Epsilon mathematics honorary society of Outstanding University wishes to have a picture taken of its six officers. There will be two rows of three people. How many different way can the six officers be arranged?

6. An automobile dealer has several options available for each of three different packages of a particular model car: a choice of two styles of seats in three different colors, a choice of four different radios, and five different exteriors. How many choices of automobile does a customer have?

7. A clothing manufacturer has put out a mix-and-match collection consisting of two blouses, two pairs of pants, a skirt, and a blazer. How many outfits can you make? Did you consider that the blazer is optional? How many outfits can you make if the manufacturer adds a sweater to the collection?

8. As a freshman, suppose you had to take two of four lab science courses, one of two literature courses, two of three math courses, and one of seven physical education courses. Disregarding possible time conflicts, how many different schedules do you have to choose from?

9. (a) Suppose each single character stored in a computer uses eight bits. Then each character is represented by a different sequence of eight 0's and l's called a bit pattern. How many different bit patterns are there? (That is, how many different characters could be represented?)

(b) How many bit patterns are palindromes (the same backwards as forwards)?

(c) How many different bit patterns have an even number of 1's?

10. Automobile license plates in Massachusetts usually consist of three digits followed by three letters. The first digit is never zero. How many different plates of this type could be made?

11. (a) Let $A = \{a, b, c, d\}$. Determine the number of different subsets of A.

(b) Let $A = \{1, 2, 3, 4, 5\}$. Determine the number of proper subsets of A.

12. How many integers from 100 to 999 can be written with no 7's?

13. Consider three persons, A, B, and C, who are to be seated in a row of three chairs. Suppose A and B are identical twins. How many seating arrangements of these persons can there be:

(a) If you are a total stranger?

(b) If you are A and B's mother?

(This problem is designed to show you that different people can have different correct answers to the same problem.)

14. How many ways can a student do a ten-question true-false exam if he or she can choose not to answer any number of questions?

15. Suppose you have a choice of fish, lamb, or beef for a main course, a choice of peas or carrots for a vegetable, and a choice of pie, cake, or ice cream for dessert. If you must order one item from each category, how many different dinners are possible?

16. Suppose you have a choice of vanilla, chocolate, or strawberry for ice cream, a choice of peanuts or walnuts for chopped nuts, and a choice of hot fudge or marshmallow for topping. If you must order one item from each category, how many different sundaes are possible?

B Exercises

17. A questionnaire contains six questions each having yes-no answers. For each yes response, there is a follow-up question with four possible responses.

(a) Draw a tree diagram that illustrates how many ways a single question in the questionnaire can be answered.

(b) How many ways can the questionnaire be answered?

18. Ten people are invited to a dinner party. How many ways are there of seating them at a round table? If the ten people consist of five men and five women, how many ways are there of seating them if each man must be surrounded by two women around the table?

19. How many ways can you separate a set with n elements into two nonempty subsets if the order of the subsets is immaterial? What if the order of the subsets is important?

20. A gardener has three flowering shrubs and four nonflowering shrubs. He must plant these shrubs in a row using an alternating pattern, that is, a shrub must be of a different type from that on either side. How many ways can he plant these shrubs? If he has to plant these shrubs in a circle using the same pattern, how many ways can he plant this circle? Note that one nonflowering shrub will be left out at the end.

2.2 Permutations

A number of applications of the rule of products are of a specific type, and because of their frequent appearance they are given a designation all their own— permutations. Consider the following examples.

Example 2.2.1. How many different ways can we order the three different elements of the set A = {a, b, c}? Since we have three choices for position one, two choices for position two, and one choice for the third position, we have, by the rule of products, 3-2-1 = 6 different ways of ordering the three letters. We illustrate through a tree diagram:

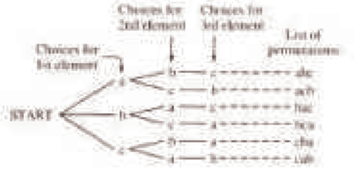


Figure 2.2.1

Each of the six orderings is called a permutation of the set A.

Example 2.2.2. A student is taking five courses in the fall semester. How many different ways can the five courses be listed? There are 5x4x3x2x1= 120 different permutations of the set of courses.

In each of the above examples of the rule of products we observe that:

(1) We are asked to order or arrange elements from a single set.

(2) Each element is listed exactly once in each list (permutation). So if there are n choices for position one in a list, there are n - 1 choices for position two, n - 2 choices for position three, etc.

Example 2.2.3. The alphabetical ordering of the players of a baseball team is one permutation of the set of players. Other orderings of the players' names might be done by batting average, age, or height. The information that determines the ordering is called the key. We would expect that each key would give a different permutation of the names. If there are twenty-five players on the team, there are $25 \cdot 24 \cdot 23 \cdot \cdots \cdot 2 \cdot 1$ different permutations of the players.

We now develop notation that will be useful for permutation problems.

Definition: Factorials. *If n is a positive integer then n factorial is the product of the first n positive integers and is denoted ni. Additionally, we define zero factorial to be 1.*

$$0! = 1$$

$$1! = 1$$

$$2! = 2 \cdot 1 = 2$$

$$3! = 3 \cdot 2 \cdot 1 = 6$$

$$n! = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 2 \cdot 1 = \prod_{k=1}^{n} k$$

Note that $4!$ is 4 times $3!$, or 24, and $5!$ is 5 times $4!$, or 120. In addition, note that as n grows in size, $n!$ grows extremely quickly. For example, $11! = 39\,916\,800$. If the answer to a problem happens to be $25!$, for example, you would never be expected to write that number out completely. However,

a problem with an answer of $\frac{25!}{23!}$ can be reduced to $25 \cdot 24$, or 600.

So if $|A| = n$, there are $n!$ ways of permuting all n elements of A. We next consider the more general situation where we would like to permute k elements of a set of n objects, $k \leq n$.

Example 2.2.4. A club of twenty-five members will hold an election for president, secretary, and treasurer in that order. Assume a person can hold only one position. How many ways are there of choosing these three officers? By the rule of products there are $25 \cdot 24 \cdot 23$ ways of making a selection.

Definition: Permutation. *An ordered arrangement of k elements selected from a set of n elements, $0 < k \leq n$, where no two elements of the arrangement are the same, is called a permutation of n objects taken k at a time. The total number of such permutations is denoted by $P(n;\ k)$.*

Theorem 2.2.1. *The number of possible permutations of k elements taken from a set of n elements is* $P(n;\ k) = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (n-k+1) = \frac{n!}{(n-k)!} = \sum_{j=0}^{k-1} (n-j)$

Proof: Case I: If $k = n$ we have $P(n;\ n) = \frac{n!}{(n-n)!} = n!$, which is simply the rule of products as applied in Example 2.2.3.

Case II: If $0 < k < n$ then, as in Example 2.2.4, we have k positions to fill with n elements and position 1 can be filled by any one of n elements

position 2 can be filled by any one of $n - 1$ elements

position 3 can be filled by any one of $n - 2$ elements

$\ddots$

position k can be filled by any one of $n - k + 1$ elements.

Hence, by the rule of products, $P(n; k) = n \cdot (n - 1) \cdot (n - 2) \cdot \cdots \cdot (n - k + 1)$. Also,

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

It is important to note that the derivation of the permutation formula given in Theorem 2.2.1 was done solely through the rule of products. This serves to reiterate our introductory remarks in this section that permutation problems are really rule-of-products problems. Every permutation problem can be done by the rule of products. We close this section with several examples solved by both methods.

Example 2.2.5. A club has eight members eligible to serve as president, vice-president, and treasurer. How many ways are there of choosing these officers?

Solution 1: Using the rule of products. There are eight possible choices for the presidency, seven for the vice-presidency, and six for the office of treasurer. By the rule of products there are $8 \times 7 \times 6 = 336$ ways of choosing these officers.

Solution 2: Using the permutation formula. We want the total number of permutations of eight objects taken three at a time:

$$P(8, 3) = \frac{8!}{(8-3)!} = \frac{8 \times 7 \times 6 \times 5!}{5!} = 8 \cdot 7 \cdot 6 = 336$$

Example 2.2.6. Example 2.2.2 revisited. Solution 2: Using the permutation formula. We want the total number of permutations of five courses taken five at a time:

$$P(5; 5) = \frac{5!}{(5-5)!} = \frac{5!}{0!} = 120$$

Example 2.2.7. Consider the digits 1, 2, 3, 4, and 5.

(a) How many three-digit numbers can be formed if no repetition of digits can occur?

(b) How many three-digit numbers can be formed if repetition of digits is allowed?

Solution to (a):

Solution 1: Using the rule of products. We have any one of five choices for digit one, any one of four choices for digit two, and three choices for digit three. Hence, $5 \cdot 4 \cdot 3 = 60$ different three-digit numbers can be formed.

Solution 2; Using the permutation formula. We want the total number of permutations of five digits taken three at a time:

$$P(5; 3) = \frac{5!}{(5-3)!} = \frac{5}{2!} = \frac{5 \times 4 \times 3 \times 2 \times 1}{2 \times 1} = 5 \times 4 \times 3 = 60$$

Solution to (b): The definition of permutation indicates ". . .no two elements in each list are the same." Hence the permutation formula cannot be used. However, the rule of products still applies. We have any one of five choices for the first digit, five choices for the second, and five for the third. So there are $5 \cdot 5 \cdot 5 = 125$ possible different three-digit numbers if repetition is allowed.

EXERCISES FOR SECTION 2.2

A Exercises

1. If a raffle has three different prizes and there are 1,000 raffle tickets sold, how many different ways can the prizes be distributed?

2. (a) How many three-digit numbers can be formed from the digits 1, 2, 3 if no repetition of digits is allowed? List the three-digit numbers.

(b) How many two-digit numbers can be formed if no repetition of digits is allowed? List them.

(c) How many two-digit numbers can be obtained if repetition is allowed?

3. How many eight-letter words can be formed from the 26 letters in the alphabet? Even without concerning ourselves about whether the words make sense, there are two interpretations of this problem. Answer both.

4. Let A be a set with $| A | = n$.

(a) Determine $| A^3 |$.

(b) Determine $| \{(a, b, c) \in A^3 \mid \text{each coordinate is different}\} |$.

5. The state finals of a high school track meet involves fifteen schools. How many ways can these schools be listed in the program?

6. Consider the three-digit numbers that can be formed from the digits 1, 2, 3, 4, 5 with no repetition of digits allowed.

(a) How many of these are even numbers?

(b) How many are greater than 250?

7. (a) How many ways can the coach at Tall U. fill the five starting positions on a basketball team if each of his 15 players can play any position? (b) What is the answer if the center must be one of two people?

8. (a) How many ways can a gardener plant five different species of shrubs in a circle?

(b) What is the answer if two of the shrubs are the same?

(c) What is the answer if all the shrubs are identical?

9. The president of the Math and Computer Club would like to arrange a meeting with six attendees, the president included. There will be three computer science majors and three math majors at the meeting. How many ways can the six people be seated at a circular table if the president does not want people with the same majors to sit next to one other?

B Exercises

10. Six people apply for three identical jobs and all are qualified for the positions. Two will work in New York and the other one will work in San Diego. How many ways can the positions be filled?

11. (a) Let $A = \{1, 2, 3, 4\}$. Determine the cardinality of $\{(a_1, a_2) \in A^2 \mid a_1 \neq a_2\}$

(b) What is the answer to part (a) if $\mid A \mid = n$?

(c) Assume that A is a set with cardinality n. Determine the number of m-tuples in A m where each coordinate is different from the other coordinates. Break your answer down into cases $m > n$ and m ≤ n.

2.3 Partitions of Sets and the Laws of Addition

One way of counting the number of students in your class would be to count the number in each row and to add these totals. Of course this problem is simple because there are no duplications, no person is sitting in two different rows. The basic counting technique that you used involves an extremely important first step, namely that of partitioning a set. The concept of a partition must be clearly understood before we proceed further.

Definition: Partition. *A partition of set A is a set of one or more nonempty subsets of A: $A_1, A_2, \ldots$ such that:*

(a) $A_1 \cup A_2 \cup \cdots = A$ *and*

(b) the subsets are mutually disjoint: that is, $A_i \cap A_j = \emptyset$ *for* $i \neq j$.

The subsets in a partition are often referred to as blocks. Note how our definition allows us to partition infinite sets, and to partition a set into an infinite number of subsets. Of course, if A is finite the number of subsets can be no larger than $|A|$.

Example 2.3.1. Let $A = \{a, b, c, d\}$. Three partitions of A are:

1. $\{\{a\}, \{b\}, \{c, d\}\}$

2. $\{\{a, b\}, \{c, d\}\}$

3. $\{\{a\}, \{b\}, \{c\}, \{d\}\}$

Example 2.3.2. Two examples of partitions of $\mathbb{Z}$ are $\{\{n\} \mid n \in \mathbb{Z}\}$ and $\{\{n \mid n \in \mathbb{Z},\ n < 0\}, \{0\}, \{n \mid n \in \mathbb{Z},\ n > 0\}\}$. The set of subsets $\{\{n \in \mathbb{Z} \mid n \geq 0\}, [n \in \mathbb{Z} \mid n \leq 0\}\}$ is not a partition because the two subsets have a nonempty intersection. A second example of a non-partition is $\{\{n \in \mathbb{Z} : |n| = k\} \mid k = -1, 0, 1, 2, \ldots\}$. One of the blocks, $\{n \in \mathbb{Z} : |n| = -1\}$ is empty.

One could also think of the concept of partitioning a set as a "packaging problem." How can one "package" a carton of, say, twenty-four cans? We could use: four six-packs, three eight-packs, two twelve-packs, etc. In all cases: (a) the sum of all cans in all packs must be twenty-four, and (b) a can must be in one and only one pack.

Basic Law Of Addition: *If A is a finite set, and if* $\{A_1, A_2, \ldots, A_n\}$ *is a partition of A, then*

$$\left|A\right| = \left|A_1\right| + \left|A_2\right| + \cdots + \left|A_n\right| = \sum_{k=1}^{n} |A_k|$$

The basic law of addition can be rephrased as follows: If A is a finite set where $A = A_1 \cup A_2 \cup \cdots \cup A_n$ and where $A_i \cap A_j = \emptyset$ whenever $i \neq j$, then

$$|A| = |A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$$

Example 2.3.3. The number of students in a class could be determined by adding the numbers of students who are freshmen, sophomores, juniors, and seniors, and those who belong to none of these categories. However, you probably couldn't add the students by major, since some students may have double majors.

Example 2.3.4. The sophomore computer science majors were told they must take one and only one of the following courses, Cryptography, Data Structures, or Java script, in a given semester. The numbers in each course, respectively, for sophomore CS majors, were 75, 60, 55. How many sophomore C.S. majors are there? The Law of Addition applies here. There are exactly 75 + 60 + 55 = 190 CS majors since the rosters of the three courses listed above would be a partition of the CS majors

Example 2.3.5. It was determined that all sophomore computer science majors took at least one of the following courses: Cryptography, Data Structures, or Java script. Assume the number in each course was as in Example 2.3.4. Further investigation indicated ten of them took all three courses, twenty-five took Calculus and Data Structures, twelve took Calculus and Compiler Construction, and fifteen took Data Structures and Compiler Construction. How many sophomore C.S. majors are there?

Example 2.3.4 is a simple application of the law of addition; in Example 2.3.5, however, some students are taking two or more courses, so a simple application of the law of addition would lead to double or triple counting. We rephrase Example 2.3.5 in the language of sets to describe the situation more explicitly if we let:

A = the set of all sophomore computer science majors

A_1 = the set of all sophomore CS majors who took Cryptography

A_2 = the set of all sophomore CS majors who took Data Structures

A_3 = the set of all sophomore CS majors who took javascript.

Since all sophomore CS majors must take at least one of the courses, the number we want is:

$$\begin{aligned} |A| &= |A_1 \cup A_2 \cup A_3| \\ &= |A_1| + |A_2| + |A_2| - \text{duplicates} \end{aligned}$$

A Venn diagram is helpful to visualize the problem. In this case the universal set U can stand for any reasonable set, for example, the set of all students in the university.

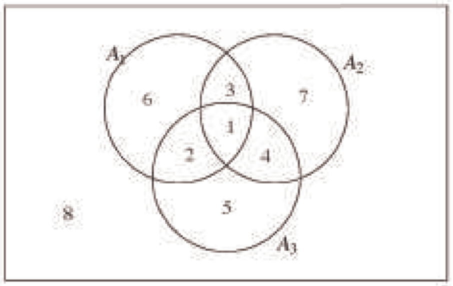


Figure 2.3.1

We see that the whole universal set is naturally partitioned into subsets that are labeled by the numbers 1 through 8, and the set A is partitioned into subsets labeled 1 through 7. Note also that students in the subsets labeled 2,3, and 4 are double counted, and those in the subset labeled 1 are triple counted, in the sense that they have already been subtracted from the total twice. So

$$\begin{aligned} |A| &= |A_1 \cup A_2 \cup A_3| \\ &= |A_1| + |A_2| + |A_3| - \text{duplicates} \\ &= |A_1| + |A_2| + |A_3| - (\text{duplicates} - \text{triplicates}) \\ &= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3| \\ &= 75 + 60 + 55 - 25 - 12 - 15 + 10 = 148 \end{aligned}$$

Note that an alternate approach to this example could be to let $A = U$; in this case the subset labeled 8, namely $(A_1 \cup A_2 \cup A_3)^c$, is the set of sophomore C. S. students who took none of the three courses, which is $\emptyset$. The concepts discussed in this latest basic counting technique give rise to the following two formulas:

Laws of Addition (Inclusion-Exclusion Laws)

1. If A_1 and A_2 are finite sets, then $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

2. If $A_1, A_2,$ and A_3 are finite sets, then

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| = {} & |A_1| + |A_2| + |A_3| \\ & - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\ & + |A_1 \cap A_2 \cap A_3| \end{aligned}$$

In this section we saw that being able to partition a set into disjoint subsets gives rise to a handy counting technique. Given a set, there are many ways to partition depending on what one would wish to accomplish. One natural partitioning of sets is apparent when one draws a Venn diagram. This particular partitioning of a set will be discussed further in Chapters 4 and 13.

EXERCISES FOR SECTION 2.3

A Exercises

1. Find all partitions of the set $A = \{a, b, c\}$.

2. Which of the following collections of subsets of the plane, $\mathbb{R} \times \mathbb{R}$, are partitions?

(a) $\{\{(x, y) \mid x + y = c\} \mid c \in \mathbb{R}\}$

(b) The set of all circles in $\mathbb{R} \times \mathbb{R}$.

(c) The set of all circles in $\mathbb{R} \times \mathbb{R}$ centered at $(0, 0)$, together with $\{(0, 0)\}$.

(d) $\{\{(x, y)\} \mid (x, y) \in \mathbb{R} \times \mathbb{R}\}$

3. A student, on an exam paper, defined the term partition the following way: "Let A be a set. A partition of A is any set of nonempty subsets $A_1, A_2, \ldots, A_n$ of A such that each element of A is in one of the subsets A_i." Is this definition correct? Why?

4. Let A_1 and A_2 be subsets of a set A. Draw a Venn diagram of this situation and shade in the subsets: $A_1 \cap A_2$, $A_1^c \cap A_2$, $A_1 \cap A_2^c$, and $A_1^c \cap A_2^c$. Use the resulting diagram and the definition of partition to convince yourself that subset of these four subsets that are nonempty form a partition of A.

5. Show that $\{\{2n \mid n \in \mathbb{Z}), \{2n + 1 \mid n \in \mathbb{Z}\}\}$ is a partition of $\mathbb{Z}$. Describe this partition using only words.

6. (a) A group of 30 students were surveyed and it was found that 18 of them took Calculus and 12 took C++. If all students took at least one course, how many took both Calculus and C++? Illustrate using a Venn diagram.

(b) What is the answer to the question in part (a) if five students did not take either of the two courses? Illustrate using a Venn diagram.

7. A survey of 90 people, 47 of them played tennis and 42 of them swam. If 17 of the them participated in both activities, how many of them participated in neither.

8. A survey of 300 people indicated:

60 owned an iPhone 75 owned an Blackberry, and 30 owned an Android. Furthermore, 40 owned both an iPhone and Blackberry, 12 owned both an iPhone and Android, and 8 owned a Blackberry and an Android. Finally, 3 owned all three phones

(a) How many people surveyed owned none of the three phones?

(b) How many people owned an Blackberry but not an iPhone?

(c) How many owned a Blackberry but not an Android?

B Exercises

9. (a) Use Inclusion-exclusion Law 1 to derive Law 2. Note, a knowledge of basic set laws is needed for this exercise, (b) State and derive the Inclusion-exclusion law for four sets.

10. To complete your spring schedule, you must add Calculus and Physics. At 9:30, there are three Calculus sections and two Physics sections; while at 11:30, there are two Calculus sections and three Physics sections. How many ways can you complete your schedule if your only open periods are 9:30 and 11:30?

C Exercise

11. The definition of $\mathbb{Q} = \{a/b \mid a,\ b \in \mathbb{Z},\ b \neq 0\}$ given in Chapter 1 is at best awkward, since, if we use the definition to list elements in $\mathbb{Q}$, we will have duplications, that is, $\frac{1}{2}$, $\frac{-1}{-2}$, $\frac{2}{4}$ etc. Try to write a more precise definition of the rational numbers so that there is no duplication of elements.

2.4 Combinations and the Binomial Theorem

COMBINATIONS

In Section 2.1 we investigated the most basic concept in combinatorics, namely, the rule of products. Even though in this section we investigate other counting formulas, it is of paramount importance to keep this fundamental process in mind. In Section 2.2 we saw that a subclass of rule-of-products problems appears so frequently that we gave them a special designation, namely, permutations, and we derived a formula as a computational aid to assist us. In this section we will investigate another major subclass of the rule-of-product formula, namely, that given the name combinations.

In many rule-of-products applications the permutation or order is important, as in the situation of the order of putting on one's socks and shoes; in some cases it is not important, as in placing coins in a vending machine or in the listing of the elements of a set. Order is important in permutations. Order is not important in combinations.

Example 2.4.1. How many different ways are there to permute three letters from the set $A = \{a, b, c, d\}$? From the permutation formula of Section 2.2 there are $P(4;\ 3) = \frac{4!}{(4-3)!} = 24$ different orderings of three letters from A.

Example 2.4.2. How many ways can we simply list, or choose, three letters from the set $A = \{a, b, c, d\}$? Note here that we are not concerned with the order of the three letters. By trial and error, certainly abc, abd, acd, and bed are the only listings possible. A slightly more elegant approach would be to rephrase the question in terms of sets. What we are looking for is all three-element subsets of the set A. Order is not important in sets. The notation for choosing 3 elements from 4 is most commonly $\binom{4}{3}$ or occasionally $C(4; 3)$, either of which is read "4 choose 3" or the number of combinations for four objects taken three at a time.

Definition: Binomial Coefficient. *The binomial coefficient* $\binom{n}{k}$ *or* $C(n;\ k)$ *represents the number of combinations of n objects taken k at a time, and is read "n choose k."*

We would now like to investigate the relationship between permutation and combination problems in order to derive a formula for $\binom{n}{k}$. Let us reconsider the above examples. There are $3\,! = 6$ different orderings for each of the three-element subsets of A. Table 2.4.1 lists each subset of A and all permutations of each subset on the same line.

3 – element subsets of A	Permutations of each subset
abc	abc, acb, bca, bac, cab, cba
abd	abd, adb, bda, bad, dab, dba
acd	acd, adc, cda, cad, dac, dca
bcd	bcd, bdc, cdb, cbd, dbc, dcb

Table 2.4.1

Hence, $\binom{4}{3} = \frac{1}{6} P(4; 3) = 4$. We generalize this result in the following theorem:

Theorem 2.4.1. *If A is any finite set of n elements, the number of k-element subsets of A is:*

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}, \quad \textit{where } 0 \leq k \leq n.$$

Proof: There are $k\,!$ ways of ordering each of the k objects in any set of k elements. Therefore

$$\binom{n}{k} = \frac{1}{k!} P(n;\, k) = \frac{1}{k!} \cdot \frac{n!}{(n-k)!} = \frac{n!}{k!\,(n-k)!} \ \blacksquare$$

Alternate Proof: To "construct" a permutation of k objects from a set of n elements, we can first choose one of the subsets of objects and second, choose one of the $k!$ permutations of those objects. By the rule of products,

$$P(n;\, k) = \binom{n}{k} k\,!$$

and solving for $\binom{n}{k}$ we get

$$\binom{n}{k} = \frac{1}{k!} P(n;\, k) = \frac{n!}{k!\,(n-k)!} \ \blacksquare$$

Example 2.4.3. Assume an evenly balanced coin is tossed five times. In how many ways can three heads be obtained? This is a combination problem, because the order in which the heads appear does not matter. The number of ways to get three heads is

$$\binom{5}{3} = \frac{5!}{3!\,(5-3)!} = \frac{5 \times 4}{2 \times 1} = 10$$

Example 2.4.4. Determine the total number of ways a fair coin can land if tossed five times. The four tosses can produce any one of the following mutually exclusive, disjoint events: 5 heads, 4 heads, 3 heads, 2 heads, 1 head, or 0 heads. Hence by the law of addition we have:

$$\binom{5}{0}+\binom{5}{1}+\binom{5}{2}+\binom{5}{3}+\binom{5}{4}+\binom{5}{5}= 1 + 5 + 10 + 10 + 5 + 1 = 32$$

Of course, we could also have applied the extended rule of products, and since there are two possible outcomes for each of the five tosses, we have $2\times 2\times 2\times 2\times 2 = 2^5 = 32$ ways. You might think that doing this counting two ways is a waste of time but solving a problem two different ways often is instructive and leads to valuable insights. In this case, it suggests a general formula for the sum $\sum_{k=0}^{n}\binom{n}{k}$. In the case of n = 5, we get 2^5, so it is reasonable to expect that the general sum is 2^n, and it is.

Example 2.4.5. A committee usually starts as an unstructured set of people selected from a larger membership. Therefore, a committee can be thought of as a combination. If a club of 25 members has a five-member social committee, there are $\binom{25}{5} = 53\,130$ different possible social committees. If any structure or restriction is placed on the way the social committee is to be selected, the number of possible committees will probably change. For example, if the club has a rule that the treasurer must be on the social committee, then the number of possibilities is reduced to $\binom{24}{4} = 10\,626$. If we further require that a chairperson other than the treasurer be selected for the social committee, we have $\binom{24}{4}\times 4 = 42\,504$ different possible social committees. The choice of the four non-treasurers accounts for the $\binom{24}{4}$ and the choice of a chairperson accounts for the 4.

Example 2.4.6. There is $\binom{n}{0} = 1$ way of choosing a combination of zero elements from a set of n, and there is $\binom{n}{n} = 1$ way of choosing a combination of n elements from a set of n.

THE BINOMIAL THEOREM

The binomial theorem gives us a formula for expanding $(x + y)^n$ where n is a nonnegative integer. The coefficients of this expansion are precisely the binomial coefficients that we have used to count combinations. From high school algebra we can certainly compute $(x + y)^n$ for $n = 0, 1, 2, 3, 4, 5$ as given in the following table:

$(x+y)^0 = 1$	1
$(x+y)^1 = x + y$	1 1
$(x+y)^2 = x^2 + 2\,y\,x + y^2$	1 2 1
$(x+y)^3 = x^3 + 3\,y\,x^2 + 3\,y^2\,x + y^3$	1 3 3 1
$(x+y)^4 = x^4 + 4\,y\,x^3 + 6\,y^2\,x^2 + 4\,y^3\,x + y^4$	1 4 6 4 1
$(x+y)^5 = x^5 + 5\,y\,x^4 + 10\,y^2\,x^3 + 10\,y^3\,x^2 + 5\,y^4\,x + y^5$	1 5 10 10 5 1

TABLE 2.4.2

In the expansion of $(x + y)^5$ we note that the coefficient of the third term is $\binom{5}{2} = 10$, and that of the sixth term is $\binom{5}{5} = 1$. We can rewrite the expansion as $\binom{5}{0}x^5 + \binom{5}{1}y\,x^4 + \binom{5}{2}y^2\,x^3 + \binom{5}{3}y^3\,x^2 + \binom{5}{4}y^4\,x + \binom{5}{5}y^5$

In summary, in the expansion of $(x + y)^n$ we note:

1. The first term is x^n and the last term is y^n .

2. With each successive term, exponents of x decrease by 1 as those of y increase by 1. For any term the sum of the exponents is n.

3. The coefficient of $x^{n-k}\,y^k$, the $(\,k + 1\,)^{\text{st}}$ term, is $\binom{n}{k}$.

4. The triangular array of numbers in Table 2.4.2 is called Pascal's triangle after the seventeenth-century French mathematician Blaise Pascal. Note that each number in the triangle other than the 1's at the ends of each row is the sum of the two numbers to the right and left of it in the row above.

Theorem 2.4.2: The Binomial Theorem. *If n ≥ 0, and x and y are numbers, then*

$$(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}\,y^k$$

This theorem will be proven using a procedure called mathematical induction, which will be introduced in Chapter 3.

Example 2.4.8. Find the third term in the expansion of $(x - y)^4$. Since $(x - y)^4 = (x + (-y))^4$, the third term is

$$\binom{4}{2} = x^{4-2}(-y)^2 = 6\,x^2\,y^2.$$

Example 2.4.9. Expand $(3\,x\,-\,2)^3$. If we replace x and y in the Binomial Theorem with $3\,x$ and -2, respectively you get

$$\begin{aligned}(3\,x-2)^3 &= \sum_{k=0}^{3}\binom{3}{k}(3\,x)^{3-k}\,(-2)^k\\ &= \binom{3}{0}(3\,x)^3\,(-2)^0+\binom{3}{1}(3\,x)^2\,(-2)^1+\binom{3}{2}(3\,x)^1\,(-2)^2+\binom{3}{3}(3\,x)^0\,(-2)^3\\ &= 27\,x^3-54\,x^2+36\,x-8\end{aligned}$$

Mathematica Note

Mathematica has a built-in function for binomial coefficients, **`Binomial`**. Unlike the examples we've concentrated on that can be done without technology, you can compute extremely large values. For example, a bridge hand is a 13 element subset of a standard 52 card deck — the order in which the cards come to the player doesn't matter. From the point of view of a single player, the number of possible bridge hands is $\binom{52}{13}$, which is easily computed with *Mathematica*:

```
Binomial [52, 13]
```

```
635013559600
```

In bridge, the location of a hand in relation to the dealer has some bearing on the game. An even truer indication of the number of possible hands takes into account *each* player's possible hand. It is customary to refer to bridge positions as West, North, East and South. We can apply the rule of product to get the total number of bridge hands with the following logic. West can get any of the $\binom{52}{13}$ hands identified above. Then North get 13 of the remaining 39 cards and so has $\binom{39}{13}$ possible hands. East then get 13 of the 26 remaining cards, which has $\binom{26}{13}$ possibilities. South gets the remaining cards. Therefore the number of bridge hands is

```
Binomial[52, 13] Binomial [39, 13] Binomial [26, 13]
```

```
53644737765488792839237440000
```

Sage Note

Sage will do the same calculations for bridge hands just as easily. From a command line interface the calculations look like this:

```
sage: binomial(52,13)
635013559600
sage: binomial(52,13)*binomial(39,13)*binomial(26,13)
53644737765488792839237440000
```

The syntax is different, but the results are the same.

EXERCISES FOR SECTION 2.4

A Exercises

1. The judiciary committee at a college is made up of three faculty members and four students. If ten faculty members and 25 students have been nominated for the committee, how many judiciary committees are possible?

2. Suppose that a single character is stored in a computer using eight bits.

(a) How many bit patterns have exactly three 1 's?

(b) How many bit patterns have at least two 1 's?

3. How many subsets of $\{1,\ \ldots,\ 10\}$ contain at least seven elements?

4. The congressional committees on mathematics and computer science are made up of five congressmen each, and a congressional rule is that the two committees must be disjoint. If there are 385 members of congress, how many ways could the committees be selected?

5. Expand $(2\,x\,-\,3\,y)^4$

6. Find the fourth term of the expansion of $(x — 2\,y)^6$.

7. (a) A poker game is played with 52 cards. How many "hands" of five cards are possible?

(b) If there are four people playing, how many five-card "hands" are possible on the first deal?

8. A flush in a five-card poker hand is five cards of the same suit. How many spade flushes are possible in a 52-card deck? How many flushes are possible in any suit?

9. How many five-card poker hands using 52 cards contain exactly two aces?

10. In poker, a full house is three-of-a-kind and a pair in one hand; for example, three fives and two queens. How many full houses are possible from a 52- card deck?

11. A class of twelve computer science students are to be divided into three groups of 3, 4, and 5 students to work on a project. How many ways can this be done if every student is to be in exactly one group?

B Exercises

12. Explain in words why the following equalities are true and then verify the equalities using the formula for binomial coefficients.

(a) $\binom{n}{1} = n$

(b) $\binom{n}{k} = \binom{n}{n-k}$, $0 \leq k \leq n$.

13. There are ten points $P_1, P_2, \ldots, P_n$ on a plane, no three on the same line.

(a) How many lines are determined by the points?

(b) How many triangles are determined by the points?

14. How many ways can n persons be grouped into pairs when n is even? Assume the order of the pairs matters, but not the order within the pairs. For example, if $n = 4$, the different groupings would be

{{1, 2}, {3, 4}}   {{3, 4}, {1, 2}}
{{1, 3}, {2, 4}}   {{2, 4}, {1, 3}}
{{1, 4}, {2, 3}}   {{2, 3}, {1, 4}}

15. Use the binomial theorem to prove that if A is a finite set, $\left|\,\mathcal{P}(A)\,\right| = 2^{|A|}$. Hint: see Example 2.4.7.

16. (a) A state's lottery involves choosing six different numbers out of a possible 36. How many ways can a person choose six numbers?

(b) What is the probability of a person winning with one bet?

17. Use the binomial theorem to calculate 9998^3 Note that $9998^3 = (10\,000 - 2)^3$.

18. Suppose two gamblers are playing poker and are dealt five cards each. Use technology to determine the number of possible ways the hands could be dealt. Assume, as in bridge, the order of the hands matters.

SUPPLEMENTARY EXERCISES FOR CHAPTER 2

Section 2.1

1. A university would like to determine how many different three-digit telephone extensions can be made using the digits $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$

(a) if the three digits must be different

(b) if the three digits can include duplications.

2. A typical telephone number in most larger cities involves a seven-digit number using the digits $0,\ 1,\ 2,\ \ldots,\ 9$. The first three digits are referred to as the office code, and are frequently the same for smaller cities.

(a) How many different telephone numbers can one create using only the last four digits? What if all four digits must be different?

(b) How many different telephone numbers can be created using all seven digits? What if the first digit cannot be the number 0?

3. (a) Let $A = \{a,\ b,\ c,\ d,\ e\}$ and $B = \{1,\ 2,\ 3\}$. Draw a tree diagram similar to Figure 2.1.1 to illustrate $A \times B$.

(b) Let A and B be sets where $|A| = m$ and $|B| = n$. Use a tree diagram to prove $|A \times B| = |A| \times |B|$.

4. In a business meeting involving four executives, each person shakes every other person's hand. How many handshakes will occur?

5. How many ways can three couples be seated at a round table? (This problem may be harder than it seems.)

(a) The first way to consider seating them is as each couple as a unit.

(b) The second way is that the people in a couple may switch seats. How does this affect the seating plan?

6. For the main course at a restaurant you have the choice of beef (prepared three ways), chicken (fried or broiled), or any one of two fish dishes. Baked or french fried potatoes and a choice of three vegetables complement the main course. Red or white wine or water are the only beverages served. However, the owner is fussy, and he will serve red wine or water only with meat dishes, and white wine or water only with the fish dishes. How many meals can be ordered?

Section 2.2

7. (a) How many ways are there to arrange six people in a circle? Two arrangements are to be considered the same if everyone has the same right-hand neighbor and the same left-hand neighbor regardless of the exact seat each person occupies.

(b) How many ways are there to arrange six people in a circle if person p_1 cannot sit next to person p_2?

8. There are five roads from city A to city B and six roads from city B to city C. There are no direct routes from A to C.

(a) How many different ways are there from city A to C?

(b) How many different ways are there from A to C and back to A?

(c) What is the answer to part b if each road is to be used exactly once?

Section 2.3

9. (a) A contest is entered by ten people. There will be four different prizes awarded among the ten people. No person will receive more than one prize. In how many ways can the prizes be distributed?

(b) Suppose that instead of awarding four different prizes to the ten people it is decided that there will be four \$10 prizes, three \$7 prizes, and three \$5 prizes. Suppose that each person will win a prize. In how many ways can the prizes be distributed?

10. A real estate developer has finished constructing twelve houses and must paint them. He has purchased quantities of white and blue paint so that five of the houses will be blue and the remainder will be white. How many ways can he decide to paint the houses?

11. Ten persons apply for three identical jobs and all are qualified for the positions. Two of these persons will work in New York and the other one will work in San Diego. How many ways can the positions be filled?

Section 2.4

12. Let $A = \{1,\ 2,\ 3,\ \ldots,\ 10\}$.

(a) Determine the cardinality of $\mathcal{P}(A)$.
(b) How many subsets of A contain exactly four elements?
(c) How many subsets of A contain at least four elements?

13. Among eleven senators, how many ways are there to select (a) a committee of five members; (b) a committee of five members so that a particular senator, Senator A, is always included; (c) a committee of five so that either Senator A or Senator B will be included?

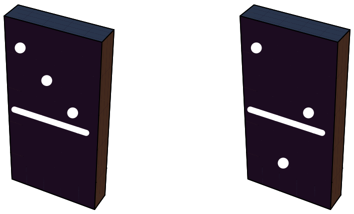
14. Use the combination formula to prove that $\binom{n}{1} = \binom{n}{n-1} = n$.

15. (a) How many ways can three people be seated in a car with four seats? Assume that someone must drive.
(b) What is your answer if only two of the three people have a driver's license?

16. (a) Let $T = \{1, 2, 3, 4, 5\}$. How many subsets of T have less than four elements?

(b) How many *proper* subsets of $\{1, 2, 3, 4, 5\}$ contain the numbers 1 and 5? How many of them also *do not* contain the number 2?

chapter 3



LOGIC

GOALS

In this chapter, we will introduce some of the basic concepts of mathematical logic. In order to fully understand some of the later concepts in this book, you must be able to recognize valid logical arguments. Although these arguments will usually be applied to mathematics, they employ the same techniques that are used by a lawyer in a courtroom or a physician examining a patient. An added reason for the importance of this chapter is that the circuits that make up digital computers are designed using the same algebra of propositions that we will be discussing.

3.1 Propositions and Logical Operators

PROPOSITIONS

Definition: Proposition. A proposition is a sentence to which one and only one of the terms true or false can be meaningfully applied.

Example 3.1.1. "Four is even," "$4 \in \{1, 3, 5\}$," and "$43 > 21$" are propositions.

In traditional logic, a declarative statement with a definite truth value is considered a proposition. Although our ultimate aim is to discuss mathematical logic, we won't separate ourselves completely from the traditional setting. This is natural because the basic assumptions, or postulates, of mathematical logic are modeled after the logic we use in everyday speech. Since compound sentences are frequently used in everyday speech, we expect that logical propositions contain connectives like the word and. The statement "Europa supports life or Mars supports life" is a proposition and, hence, must have a definite truth value. Whatever that truth value is, it should be the same as the truth value of "Mars supports life or Europa supports life."

LOGICAL OPERATORS

There are several ways in which we commonly combine simple statements into compound ones. The words/phrases *and*, *or*, *not*, *if… then*, and *if and only if* can be added to one or more propositions to create a new proposition. To avoid any confusion, we will precisely define each one's meaning and introduce its standard symbol. With the exception of negation (not), all of the operators act on pairs of propositions. Since each proposition has two possible truth values, there are four ways that truth can be assigned to two propositions. In defining the effect that a logical operator has on two propositions, the result must be specified for all four cases. The most convenient way of doing this is with a truth table, which we will illustrate by defining the word *and*.

Conjunction

***Definition*: Conjunction** *(And). If p and q are propositions, their conjunction, p and q (denoted $p \land q$), is defined by the truth table in Table 3.1.1.*

p	q	$p \land q$
0	0	0
0	1	0
1	0	0
1	1	1

Table 3.1.1. Truth Table for *And*

Notes:

(a) To read this truth table, you must realize that any one line represents a case: one possible set of values for p and q.

(b) The numbers 0 and 1 are used to denote false and true, respectively. This is consistent with the way that many programming languages treat logical, or Boolean, variables since a single bit, 0 or 1, can represent a truth value. Although *Mathematica*'s logical expressions have a value of True or False, there is a built in function called `Boole` which converts the value to 1 or 0, if desired.

```
{Boole[False], Boole[True]}
```

```
{0, 1}
```

(c) For each case, the symbol under p represents the truth value of p. The same is true for q. The symbol under $p \land q$ represents the truth value of $p \land q$ for that case. For example, the second row of the truth table represents the case in which p is false, q is true, and the resulting truth value for $p \land q$ is false. As in everyday speech, $p \land q$ is true only when both propositions are true.

(d) Just as the letters x, y, and z are frequently used in algebra to represent numeric variables, p, q, and r seem to be the most commonly used symbols for logical variables. When we say that p is a logical variable, we mean that any proposition can take the place of p.

(e) One final comment: The order in which we list the cases in a truth table is standardized in this book. If the truth table involves two simple propositions, the numbers under the simple propositions can be inter preted as the two-digit binary integers in increasing order, 00, 01, 10, and 11, for 0, 1, 2, and 3.

Disjunction

***Definition:* Disjunction** *(Or). If p and q are propositions, their disjunction is p or q, denoted $p \lor q$, and is defined by the truth table in Table 3.1.2.*

p	q	$p \lor q$
0	0	0
0	1	1
1	0	1
1	1	1

Table 3.1.2. Truth Table for *Or*

Note; The only case in which disjunction is false is when both propositions are false. This interpretation of the word or is called the nonexclusive *or*. The exclusive or will be discussed when we consider logical design in Chapter 13.

Negation

Definition: Negation *(Not). If p is a proposition, its negation, not p, is denoted ¬p and is defined by the truth table in Table 3.1.3.*

p	$\neg p$
0	1
1	0

Table 3.1.3 Truth Table for *Not*

Note: Negation is the only standard operator that acts on a single proposition; hence only two cases are needed.

The Conditional Operator (*If . . . then*).

Consider the following propositions from everyday speech:

(a) I'm going to quit if I don't get a raise.

(b) If I pass the final, then I'll graduate.

(c) I'll be going to the movies provided that my car starts.

All three propositions are conditional, they can all be restated to fit into the form if *Condition*, then *Conclusion*. For example, statement (a) can be rewritten as "If I don't get a raise, then I'm going to quit."

A conditional statement is meant to be interpreted as a guarantee; if the condition is true, then the conclusion is expected to be true. It says no more and no less.

Definition: Conditional Operator*. The conditional statement if p then q, denoted p → q, is defined by the truth table in Table 3.1.4.*

p	q	$p \to q$
0	0	1
0	1	1
1	0	0
1	1	1

Table 3.1.4 Truth Table for *If... then*

Example 3.1.2. Assume your instructor told you "If you receive a grade of 95 or better in the final examination, then you will receive an A in this course." Your instructor has made a promise to you (placed a condition with you). If you fulfill his condition you expect the conclusion (getting an A) to be forthcoming. Your graded final has been returned to you. Has your instructor told the truth (kept the promise) or is your instructor guilty of a falsehood?

Case I: Your final exam score was less than 95 (the condition is false) and you did not receive an A (the conclusion is false). The instructor told the truth.

Case II: Your final exam score was less than 95, yet you received an A for the course. The instructor told the truth. (Perhaps your overall course average was excellent.)

Case III: Your final exam score was greater than 95, but you did not receive an A. The instructor lied.

Case IV: Your final exam score was greater than 95, and you received an A. The instructor told the truth.

To sum up, the only case in which a conditional proposition is false is when the condition is true and the conclusion is false.

The order of the condition and conclusion in a conditional proposition is important. If the condition and conclusion are exchanged, a different proposition is produced.

Definition: Converse*. The converse of the proposition p→ q is the proposition q → p.*

The converse of "If you receive a grade of 95 or better in the final exam, then you will receive an A in this course," is "If you receive an A in this course, then you received a grade of 95 or better in the final exam." It should be clear that these two statements say different things.

Definition: Biconditional Operator *(...if and only if...). If p and q are propositions, the biconditional statement "p if and only if q," denoted p↔ q, is defined by the truth table in Table 3.1.5.*

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Table 3.1.5 Truth table for "*... if and only if...*"

Note that $p \leftrightarrow q$ is true when p and q have the same truth values. It is common to abbreviate "*if and only if*" to "*iff*."

Although "*if . . . then*" and "*if and only if*" are frequently used in everyday speech, there are several alternate forms that you should be aware of. They are summarized in the following list:

Conditional

If p then q.

p implies q.

q follows from q.

p, only if q.

q, if p.

p is sufficient for q.

q is necessary for p.

Biconditional

p if and only if q.

p is necessary and sufficient for q.

p is equivalent to q.

If p, then q, and if q, then p.

If p, then q and conversely.

EXERCISES FOR SECTION 3.1

A Exercises

1. Let d = "I like discrete structures" c = "I will pass this course" s = "I will do my assignments" Express each of the following propositions in symbolic form:

(a) I like discrete structures and I will pass this course.

(b) I will do my assignments or I will not pass this course.

(c) It is not true that I like discrete structures and I will do my assignments.

(d) I will not do my assignment and I will not pass this course.

2. For each of the following propositions, identify simple propositions, express the compound proposition in symbolic form, and determine whether it is true or false:

(a) The world is flat or zero is an even integer.

(b) If 432,802 is a multiple of 4, then 432,802 is even.

(c) 5 is a prime number and 6 is not divisible by 4.

(d) $3 \in \mathbb{Z}$ and $3 \in \mathbb{Q}$.

(e) $2/3 \in \mathbb{Z}$ and $2/3 \in \mathbb{Q}$.

(f) The sum of two even integers is even and the sum of two odd integers is odd.

3. Let p = "$2 < 5$," q = "8 is an even integer," and r = "11 is a prime number." Express the following as a statement in English and determine whether the statement is true or false:

(a) $\neg\, p \lor q$

(b) $p \to q$

(c) $(p \land q) \to r$

(d) $p \to q \lor (\neg r)$

(e) $p \to (\neg q) \lor (\neg r)$

(f) $\neg q \to \neg p$

4. Rewrite each of the following statements using the other conditional forms:

(a) If an integer is a multiple of 4, then it is even.

(b) The fact that a polygon is a square is a sufficient condition that it is a rectangle.

(c) If $x = 5$, then $x^2 = 25$.

(d) If $x^2 - 5x + 6 = 0$, then $x = 2$ or $x = 3$.

(e) $x^2 = y^2$ is a necessary condition for $x = y$.

5. Write the converse of the propositions in exercise 4. Compare the truth of each proposition and its converse.

3.2 Truth Tables and Propositions Generated by a Set

Consider the compound proposition $c = (p \wedge q) \vee (\neg q \wedge r)$, where p, q, and r are propositions. This is an example of a proposition generated by p, q, and r. We will define this terminology later in the section. Since each of the three simple propositions has two possible truth values, it follows that there are eight different combinations of truth values that determine a value for c. These values can be obtained from a truth table for c. To construct the truth table, we build c from p, q, and r and from the logical operators. The result is Table 3.2.1. Strictly speaking, the first three columns and the last column make up the truth table for c. The other columns are work space needed to build up to c.

p	q	r	$p \wedge q$	$\neg q$	$\neg q \wedge r$	$(p \wedge q) \vee (\neg q \wedge r)$
0	0	0	0	1	0	0
0	0	1	0	1	1	1
0	1	0	0	0	0	0
0	1	1	0	0	0	0
1	0	0	0	1	0	0
1	0	1	0	1	1	1
1	1	0	1	0	0	1
1	1	1	1	0	0	1

Table 3.2.1 Truth Table for $c = (p \wedge q) \vee (\neg q \wedge r)$

Note that the first three columns of the truth table are an enumeration of the eight three-digit binary integers. This standardizes the order in which the cases are listed. In general, if c is generated by n simple propositions, then the truth table for c will have 2^n rows with the first n columns being an enumeration of the n digit binary integers. In our example, we can see at a glance that for exactly four of the eight cases, c will be true. For example, if p and r are true and q is false (the sixth case), then c is true.

Let S be any set of propositions. We will give two definitions of a proposition generated by S. The first is a bit imprecise, but should be clear. The second definition is called a *recursive definition*. If you find it confusing, use the first definition and return to the second later.

Definition: Proposition Generated by S.

(1) A proposition generated by S is any valid combination of propositions in S with conjunction, disjunction, and negation.

(2) (a) If $p \in S$, then p is a proposition generated by S.

(b) If x and y are propositions generated by S, then so are (x), $\neg x$, $x \vee y$, and $x \wedge y$.

Note: We have not included the conditional and biconditional in the definition because they can both be obtained from conjunction, disjunction, and negation, as we will see later.

If S is a finite set, then we may use slightly different terminology. For example, if $S = \{p, q, r\}$, we might say that a proposition is generated by p, q, and r instead of $\{p, q, r\}$.

Hierarchy of Logical Operations

It is customary to use the following hierarchy for interpreting propositions, with parentheses overriding this order:

First: Negation

Second: Conjunction

Third: Disjunction

Within any level of the hierarchy, work from left to right. Using these rules, $p \wedge q \vee r$ is taken to mean $(p \wedge q) \vee r$. These precedence rules are universal, and are exactly those used by computer languages to interpret logical expressions.

Example 3.2.1. A few shortened expressions and their fully parenthesized versions:

(a) $p \wedge q \wedge r$ is $(p \wedge q) \wedge r$.

(b) $\neg p \vee \neg r$ is $(\neg p) \vee (\neg r)$.

(c) $\neg \neg p$ is $\neg (\neg p)$.

A proposition generated by a set S need not include each element of S in its expression. For example, $\neg q \wedge r$ is a proposition generated by p, q, and r.

EXERCISES FOR SECTION 3.2

A Exercises

1. Construct the truth tables of:

(a) $p \vee p$

(b) $p \wedge (\neg p)$

(c) $p \vee (\neg p)$

(d) $p \wedge p$

2. Construct the truth tables of:

(a) $\neg (p \wedge q)$

(b) $p \wedge (\neg q)$

(c) $(p \wedge q) \wedge r$

(d) $(p \wedge q) \vee (q \wedge r) \vee (r \wedge p)$

(e) $\neg p \vee \neg q$

(f) $p \vee q \vee r \vee s$

3. Rewrite the following with as few extraneous parentheses as possible:

(a) $(\neg ((p) \wedge (r))) \vee (s)$

(b) $((p) \vee (q)) \wedge ((r) \vee (q))$

4. In what order are the operations in the following propositions performed?

(a) $p \vee \neg q \vee r \wedge \neg p$

(b) $p \wedge \neg q \wedge r \wedge \neg p$

5. Determine the number of rows in the truth table of a proposition containing four variables p, q, r, and s.

6. If there are 45 lines on a sheet of paper, and you want to reserve one line for each line in a truth table, how large could $| S |$ be if you can write truth tables of propositions generated by S on a sheet of paper?

3.3 Equivalence and Implication

Tautologies & Contradictions

Consider two propositions generated by p and q: $\neg (p \land q)$ and $\neg p \lor \neg q$. At first glance, they are different propositions. In form, they are different, but they have the same meaning. One way to see this is to substitute actual propositions for p and q; such as:

p: I've been to Toronto; and q: I've been to Chicago.

Then $\neg (p \land q)$ translates to "I haven't been to both Toronto and Chicago," while $\neg p \lor \neg q$. is "I haven't been to Toronto or I haven't been to Chicago." Determine the truth values of these propositions. Naturally, they will be true for some people and false for others. What is important is that no matter what truth values they have, $\neg (p \land q)$ and $\neg p \lor \neg q$. will have the same truth value. The easiest way to see this is by examining the truth tables of these propositions ().

p	q	$\neg (p \land q)$	$\neg p \lor \neg q$
0	0	1	1
0	1	1	1
1	0	1	1
1	1	0	0

Table 3.3.1 Truth tables of $\neg (p \land q)$ and $\neg p \lor \neg q$.

In all four cases, $\neg (p \land q)$ and $\neg p \lor \neg q$. have the same truth value. Then when the biconditional operator is applied to them, the result is a value of true in all cases.

Definition: Tautology. *An expression involving logical variables that is true in all cases is called a tautology.*

Example 3.3.1. All of the following are tautologies because their truth tables consist of a column of 1's.

(a) $(\neg (p \land q)) \leftrightarrow (\neg p \lor \neg q)$.

(b) $p \lor \neg p$

(c) $(p \land q) \rightarrow p$

(d) $q \rightarrow (p \lor q)$

(e) $(p \lor q) \leftrightarrow (q \lor p)$

Definition: Contradiction. *An expression involving logical variables that is false for all cases is called a contradiction.*

Example 3.3.2. $p \land \neg p$ and $(p \lor q) \land (\neg p) \land (\neg q)$ are contradictions.

Equivalence

Definition: Equivalence. *Let S be a set of propositions and let r and s be propositions generated by S. r and s are equivalent if and only if $r \leftrightarrow s$ is a tautology. The equivalence of r and s is denoted $r \Leftrightarrow s$.*

Example 3.3.3. The following are all equivalences:

(a) $(p \land q) \lor (\neg p \land q) \Leftrightarrow q$.

(b) $p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$

(c) $p \lor q \Leftrightarrow q \lor p$.

All tautologies are equivalent to one another. We will use the number 1 to symbolize a tautology.

Example 3.3.4. $p \lor \neg p \Leftrightarrow l$.

All contradictions are equivalent to one another. We will use the number 0 to symbolize a contradiction.

Example 3.3.5. $p \land \neg p \Leftrightarrow 0$.

Equivalence is to logic what equality is to algebra. Just as there are many ways of writing an algebraic expression, the same logical meaning can be expressed in many different ways.

IMPLICATION

Example 3.3.6. Consider the two propositions:

x: The money is behind Door A; and

y: The money is behind Door A or Door B.

Imagine that you were told that there is a large sum of money behind one of two doors marked A and B, and that one of the two propositions x and y is true and the other is false. Which door would you choose? All that you need to realize is that if x is true, then y will also be true. Since we know that this can't be the case, y must be the true proposition and the money is behind Door B.

This is an example of a situation in which the truth of one proposition leads to the truth of another. Certainly, y can be true when x is false; but x can't be true when y is false. In this case, we say that x implies y.

Look at the truth table of $p \rightarrow q$ in Table 3.1.4 (copied below). If p implies q, then the third case can be ruled out, since it is the case that makes a conditional proposition false.

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Definition: Implication. *Let S be a set of propositions and let r and s be propositions generated by S. We say that r implies s if $r \rightarrow s$ is a tautology. We write $r \Rightarrow s$ to indicate this implication.*

Example 3.3.7. A commonly used implication is that p implies $p \vee q$, which is verified by the truth table in Table 3.3.2.

p	q	$p \vee q$	$p \rightarrow p \vee q$
0	0	0	1
0	1	1	1
1	0	1	1
1	1	1	1

Table 3.3.2 Truth Table for $p \rightarrow (p \vee q)$

If we let p represent "The money is behind Door A" and q represent "The money is behind Door B," $p \Rightarrow (p \vee q)$ is a formalized version of the reasoning used in Example 3.3.6. A common name for this implication is disjunctive addition. In the next section we will consider some of the most commonly used implications and equivalences.

When we defined what we mean by a proposition generated by a set in Section 3.2, we didn't include the conditional and biconditional operators. This was because of the two equivalences $p \rightarrow q \Leftrightarrow \neg p \vee q$ and $p \leftrightarrow q \Leftrightarrow (p \wedge q) \vee (\neg p \wedge \neg q)$. Therefore, any proposition that includes the conditional or biconditional operators can be written in an equivalent way using only conjunction, disjunction, and negation. We could even dispense with disjunction since $p \vee q$ is equivalent to a proposition that uses only conjunction and negation.

EXERCISES FOR SECTION 3.3

A Exercises

1. Given the following propositions generated by p, q, and r, which are equivalent to one another?

(a) $(p \wedge r) \vee q$

(b) $p \vee (r \vee q)$

(c) $r \wedge p$

(d) $\neg r \vee p$

(e) $(p \vee q) \wedge (r \vee q)$

(f) $r \rightarrow p$

(g) $r \vee \neg p$

(h) $p \rightarrow r$

2. (a) Construct the truth table for $x = (p \wedge \neg q) \vee (r \wedge p)$.

(b) Give an example other than x itself of a proposition generated by p, q, and r that is equivalent to x.

(c) Give an example of a proposition other than x that implies x.

(d) Give an example of a proposition other than x that is implied by x.

3. Is an implication equivalent to its converse? Verify your answer using a truth table.

4. Suppose that x is a proposition generated by p, q, and r that is equivalent to $p \vee \neg q$. Write out the truth table for x.

B Exercises

5. How large is the largest set of propositions generated by p and q with the property that no two elements are equivalent?

6. Find a proposition that is equivalent to $p \lor q$ and uses only conjunction and negation.

7. Explain why a contradiction implies any proposition and any proposition implies a tautology.

3.4 The Laws of Logic

In this section, we will list the most basic equivalences and implications of logic. Most of the equivalences listed in Table 3.4.1 should be obvious to the reader. Remember, 0 stands for contradiction, 1 for tautology. Many logical laws are similar to algebraic laws. For example, there is a logical law corresponding to the associative law of addition, $a + (b + c) = (a + b) + c$. In fact, associativity of both conjunction and disjunction are among the laws of logic. Notice that with one exception, the laws are paired in such a way that exchanging the symbols $\wedge$, $\vee$, 1 and 0 for $\vee$, $\wedge$, 0, and 1, respectively, in any law gives you a second law. For example, $p \vee 0 \Leftrightarrow p$ results in $p \wedge 1 \Leftrightarrow p$. This called a *duality principle*. For now, think of it as a way of remembering two laws for the price of one. We will leave it to the reader to verify a few of these laws with truth tables. However, the reader should be careful in applying duality to the conditional operator and implication since the dual involves taking the converse. For example, the dual of $p \wedge q \Rightarrow p$ is $p \vee q \Leftarrow p$, which is usually written $p \Rightarrow p \vee q$

Example 3.4.1. The identity law:

p	1	$p \wedge 1$	$(p \wedge 1) \leftrightarrow p$
0	1	0	1
1	1	1	1

therefore, $(p \wedge l) \Leftrightarrow p$.

Some of the logical laws in Table 3.4.2 might be less obvious to you. For any that you are not comfortable with, substitute actual propositions for the logical variables. For example, if p is "John owns a pet store" and q is "John likes pets," the detachment law should make sense.

TABLE 3.4.1 Basic Logical Laws

Commutative Laws	$p \vee q \Leftrightarrow q \vee p$	$p \wedge q \Leftrightarrow q \wedge p$
Associative Laws	$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$	$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$
Distributive Laws	$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
Identity Laws	$p \vee 0 \Leftrightarrow p$	$p \wedge 1 \Leftrightarrow p$
Negation Laws	$p \wedge \neg p \Leftrightarrow 0$	$p \vee \neg P \Leftrightarrow 1$
Idempotent Laws	$p \vee p \Leftrightarrow p$	$p \wedge p \Leftrightarrow p$
Null Laws	$p \wedge 0 \Leftrightarrow 0$	$p \vee 1 < \Leftrightarrow 1$
Absorption Laws	$p \wedge \{p \vee q) \Leftrightarrow p$	$p \vee (p \wedge q) \Leftrightarrow p$
DeMorgan's Laws	$\neg (p \vee q) \Leftrightarrow (\neg p) \wedge (\neg q)$	$\neg (p \wedge q) \Leftrightarrow (\neg p) \vee (\neg q)$
Involution Law	$\neg (\neg p) \Leftrightarrow p$	

TABLE 3.4.2 Common Implications and Equivalences

Detachment	$(p \to q) \land p \Rightarrow q$
Indirect Reasoning	$(p \to q) \land \neg q \Rightarrow \neg p$
Disjunctive Addition	$p \Rightarrow (p \lor q)$
Conjunctive Simplification	$(p \land q) \Rightarrow p$ and $(p \land q) \Rightarrow q$
Disjunctive Simplification	$(p \lor q) \land \neg p \Rightarrow q$ and $(p \lor q) \land \neg q \Rightarrow p$
Chain Rule	$(p \to q) \land (q \to r) \Rightarrow (p \to r)$
Conditional Equivalence	$p \to q \Leftrightarrow \neg p \lor q$
Biconditional Equivalences	$(p \leftrightarrow q) \Leftrightarrow (p \to q) \land (q \to p) \Leftrightarrow (p \land q) \lor (\neg p \land \neg q)$
Contrapositive	$(p \to q) \Leftrightarrow (\neg q \to \neg p)$

EXERCISES FOR SECTION 3.4

A Exercises

1. Write the following in symbolic notation and determine whether it is a tautology: "If I study then I will learn. I will not learn. Therefore, I do not study."

2. Show that the common fallacy $(p \to q) \land \neg p \Rightarrow \neg q$ is not a law of logic.

3. Describe in general how duality can be applied to implications if we introduce the symbol $\Leftarrow$, read "is implied by."

4. Write the dual of the following statements:

(a) $(p \land q) \Rightarrow p$

(b) $(p \lor q) \land \neg q \Rightarrow p$

3.5 Mathematical Systems

In this section, we present an overview of what a mathematical system is and how logic plays an important role in one. The axiomatic method that we will use here will not be duplicated with as much formality anywhere else in the book, but we hope an emphasis on how mathematical facts are developed and organized will help to unify the concepts we will present. The system of propositions and logical operators we have developed will serve as a model for our discussion. Roughly, a mathematical system can be defined as follows:

Definition: Mathematical System. *A mathematical system consists of:*

(1) A set or universe, U.

(2) Definitions — sentences that explain the meaning of concepts that relate to the universe. Any term used in describing the universe itself is said to be undefined. All definitions are given in terms of these undefined concepts of objects.

(3) Axioms — assertions about the properties of the universe and rules for creating and justifying more assertions. These rules always include the system of logic that we have developed to this point.

(4) Theorems — the additional assertions mentioned above.

Example 3.5.1. In Euclidean geometry the universe consists of points and lines (two undefined terms). Among the definitions is a definition of parallel lines and among the axioms is the axiom that two distinct parallel lines never meet.

Example 3.5.2. Propositional calculus is a formal name for the logical system that we've been discussing. The universe consists of propositions. The axioms are the truth tables for the logical operators and the key definitions are those of equivalence and implication. We use propositions to describe any other mathematical system; therefore, this is the minimum amount of structure that a mathematical system can have.

Definition: Theorem. *A true proposition derived from axioms of mathematical system is called a theorem.*

Theorems are normally expressed in terms of a finite number of propositions, $p_1, p_2, \ldots, p_n$, called the *premises*, and a proposition, C, called the *conclusion*. These theorems take the form

$$p_1 \land p_2 \land \cdots \land p_n \Rightarrow C$$

or more informally,

$$p_1, p_2, \ldots, \text{ and } p_n \text{ imply } C$$

For a theorem of this type, we say that the premises imply the conclusion. When a theorem is stated, it is assumed that the axioms of the system are true. In addition, any previously proven theorem can be considered an extension of the axioms and can be used in demonstrating that the new theorem is true. When the proof is complete, the new theorem can be used to prove subsequent theorems. A mathematical system can be visualized as an inverted pyramid with the axioms at the base and the theorems expanding out in various directions (Figure 3.5.1).

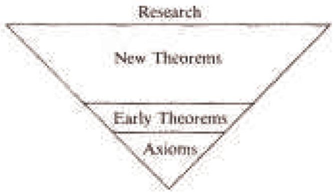


FIGURE 3.5.1 The body of knowledge In a mathematical system

PROOF

Definition: Proof. *A proof of a theorem is a finite sequence of logically valid steps that demonstrate that the premises of a theorem imply the conclusion.*

Exactly what constitutes a proof is not always clear. For example, a research mathematician might require only a few steps to prove a theorem to a colleague, but might take an hour to give an effective proof to a class of students. Therefore, what constitutes a proof often depends on the audience. But the audience is not the only factor. One of the most famous theorems in graph theory, The Four Color Theorem, was finally proven in 1976, after over a century of effort by many mathematicians. Part of the proof consisted of having a computer check many different graphs for a certain property. Without the aid of the computer, this checking would have taken years. In the eyes of some mathematicians, this proof was considered questionable. Shorter proofs have been developed since 1976 and there is no controversy associated with The Four Color Theorem at this time. (The theorem is stated in Chapter 9.)

PROOFS IN PROPOSITIONAL CALCULUS

Theoretically, you can prove anything in propositional calculus with truth tables. In fact, the laws of logic stated in Section 5.4 are all theorems. Propositional calculus is one of the few mathematical systems for which any valid sentence can be determined true or false by mechanical means. A program to write truth tables is not too difficult to write; however, what can be done theoretically is not always practical. For example,

$$a, \; a \to b, \; b \to c, \; \ldots, \; y \to z \Rightarrow z$$

is a theorem in propositional calculus. However, suppose that you wrote such a program and you had it write the truth table for

$$(a \land (a \to b) \land (b \to c) \land \cdots \land (y \to z)) \to z$$

The truth table will have 2^{26} cases. At one million cases per second, it would take approximately one minute to verify the theorem. Now if you decided to check a similar theorem,

$$p_1, p_1 \to p_2, \ldots, p_{99} \to p_{100} \Rightarrow p_{100},$$

you would really have time trouble. There would be $2^{100} \approx 1.26765 \times 10^{30}$ cases to check in the truth table. At one million cases per second it would take approximately 1.46719×10^{19} days to check all cases. For most of the remainder of this section, we will discuss an alternate method for proving theorems in propositional calculus. It is the same method that we will use in a less formal way for proofs in other systems. Formal axiomatic methods would be too unwieldy to actually use in later sections. However, none of the theorems in later chapters would be stated if they couldn't be proven by the axiomatic method.

We will introduce two types of proof here, direct and indirect.

DIRECT PROOFS

*A **direct proof** is a proof in which the truth of the premises of a theorem are shown to directly imply the truth of the theorem's conclusion.*

Example 3.5.3. Theorem: $p \to r,\ q \to s,\ p \lor q \Rightarrow s \lor r$. A direct proof of this theorem is:

Step	Proposition	Justification
(1)	$p \lor q$	Premise
(2)	$\neg p \to q$	(1), conditional rule
(3)	$q \to s$	Premise
(4)	$\neg p \to s$	(2), (3), chain rule
(5)	$\neg s \to p$	(4), contrapositive
(6)	$p \to r$	Premise
(7)	$\neg s \to r$	(5), (6), chain rule
(8)	$s \lor r$	(7), conditional rule ■

Note that ■ marks the end of a proof.

Rules for Formal Proofs. Example 3.5.3 illustrates the usual method of formal proof in a formal mathematical system. The rules governing these proofs are:

(1) A proof must end in a finite number of steps.

(2) Each step must be either a premise or a proposition that is implied from previous steps using any valid equivalence or implication.

(3) For a direct proof , the last step must be the conclusion of the theorem. For an indirect proof (see below), the last step must be a contradiction.

(4) Justification Column. The column labeled "justification" is analogous to the comments that appear in most good computer programs. They simply make the proof more readable.

Example 3.5.4. Here are two direct proofs of $\neg p \lor q,\ s \lor p,\ \neg q \Rightarrow s$:

(1)	$\neg p \lor q$	Premise
(2)	$\neg q$	Premise
(3)	$\neg p$	Disjunctive simplification, (1), (2)
(4)	$s \lor p$	Premise
(5)	s	Disjunctive simplification, (3), (4). ■

You are invited to justify the steps in this second proof:

(1) $\neg p \vee q$

(2) $\neg q \to \neg p$

(3) $s \vee p$

(4) $p \vee s$

(5) $\neg p \to s$

(6) $\neg q \to s$

(7) $\neg q$

(8) s ■

CONDITIONAL CONCLUSIONS

The conclusion of a theorem is often a conditional proposition. The condition of the conclusion can be included as a premise in the proof of the theorem. The object of the proof is then to prove the consequence of the conclusion. This rule is justified by the logical law

$$p \to (h \to c) \Leftrightarrow (p \wedge h) \to c.$$

Example 3.5.5. The following proof of $p \to (q \to s), \neg r \vee p, q \Rightarrow r \to s$ includes r as a fourth premise. The truth of s concludes the proof.

(1)	$\neg r \vee p$	Premise
(2)	r	Added premise
(3)	p	(1), (2), disjunction simplification
(4)	$p \to (q \to s)$	Premise
(5)	$q \to s$	(3), (4), detachment
(6)	q	Premise
(7)	s	(5), (6), detachment. ■

INDIRECT PROOFS / PROOF BY CONTRADICTION

Consider a theorem $P \Rightarrow C$, where P represents $p_1, p_2, \ldots,$ and p_n, the premises. The method of indirect proof is based on the equivalence $P \to C \Leftrightarrow \neg (P \wedge \neg C)$.
In words, this logical law states that if $P \Rightarrow C$, then $P \wedge \neg C$ is always false; that is, $P \wedge \neg C$ is a contradiction. This means that a valid method of proof is to negate the conclusion of a theorem and add this negation to the premises. If a contradiction can be implied from this set of propositions, the proof is complete. For the proofs in this section, a contradiction will often take the form $t \wedge \neg t$. For proofs involving numbers, a contradiction might be $1 = 0$ or $0 < 0$. Indirect proofs involving sets might conclude with $x \in \emptyset$ or ($x \in A$ and $x \in A^c$). Indirect proofs are often more convenient than direct proofs in certain situations. *Indirect proofs are often called* ***proofs by contradiction***.

Example 3.5.6. Here is an example of an indirect proof of the theorem in Example 3.5.3:

(1)	$\neg (s \vee r)$	Negated conclusion
(2)	$\neg s \wedge \neg r$	DeMorgan's Law, (1)
(3)	$\neg s$	Conjunctive simplification, (2)
(4)	$q \to s$	Premise
(5)	$\neg q$	Indirect reasoning, (3), (4)
(6)	$\neg r$	Conjunctive simplification, (2)
(7)	$p \to r$	Premise
(8)	$\neg p$	Indirect reasoning, (6), (7)
(9)	$(\neg p) \wedge (\neg q)$	Conjunctive, (5), (8)
(10)	$\neg (p \vee q)$	DeMorgan's Law, (9)
(11)	$p \vee q$	Premise
(12)	0	(10), (11) ■

PROOF STYLE

The rules allow you to list the premises of a theorem immediately; however, a proof is much easier to follow if the premises are only listed when they are needed.

Example 3.5.7. Here is an indirect proof of $a \to b,\ \neg(b \lor c) \Rightarrow \neg a$.

(1)	a	Negation of the conclusion
(2)	$a \to b$	Premise
(3)	b	(1), (2), detachment
(4)	$b \lor c$	(3), disjunctive addition
(5)	$\neg(b \lor c)$	Premise
(6)	0	(4), (5) ■

As we mentioned at the outset of this section, we are only presenting an overview of what a mathematical system is. For greater detail on axiomatic theories, see Stoll (1961). An excellent description of how propositional calculus plays a part in artificial intelligence is contained in Hofstadter (1980). If you enjoy the challenge of constructing proofs in propositional calculus, you should enjoy the game WFF'N PROOF (1962), by L.E. Allen.

EXERCISES FOR SECTION 3.5

A Exercises

1. Prove with truth tables:

(a) $p \lor q,\ \neg q \Rightarrow p$

(b) $p \to q,\ \neg q \Rightarrow \neg p$

2. Prove with truth tables:

(a) $q,\ \neg q \Rightarrow p$

(b) $p \to q \Rightarrow \neg p \lor q$

B Exercises

3. Give direct and indirect proofs of:

(a) $a \to b,\ c \to b,\ d \to (a \lor c),\ d \Rightarrow b.$

(b) $(p \to q) \land (r \to s),\ (q \to t) \land (s \to u),\ \neg(t \land u),\ p \to r \Rightarrow \neg p.$

(c) $p \to (q \to s),\ \neg s \lor p,\ q \Rightarrow s \to r.$

(d) $p \to q,\ q \to r,\ \neg(p \land r),\ p \lor r \Rightarrow r.$

(e) $\neg q,\ p \to q,\ p \lor t \Rightarrow t$

4. Give direct and indirect proofs of:

(a) $p \to q,\ \neg r \to \neg q,\ \neg r \Rightarrow \neg p.$

(b) $p \to \neg q,\ \neg r \to q,\ p \Rightarrow r.$

(c) $a \lor b,\ c \land d,\ a \to \neg c \Rightarrow b.$

5. Are the following arguments valid? If they are valid, construct formal proofs; if they aren't valid, explain why not.

(a) If wages increase, then there will be inflation. The cost of living will not increase if there is no inflation. Wages will increase. Therefore, the cost of living will increase.

(b) If the races are fixed or the casinos are crooked, then the tourist trade will decline. If the tourist trade decreases, then the police will be happy. The police force is never happy. Therefore, the races are not fixed.

6. Determine the validity of the following argument: For students to do well in a discrete mathematics course, it is necessary that they study hard. Students who do well in courses do not skip classes. Students who study hard do well in courses. Therefore students who do well in a discrete mathematics course do not skip class.

7. Describe how $p_1,\ p_1 \to p_2,\ \ldots,\ p_{99} \to p_{100} \Rightarrow p_{100}$ could be proven in 199 steps.

3.6 Propositions over a Universe

Example 3.6.1. Consider the sentence "He was a member of the Boston Red Sox." There is no way that we can assign a truth value to this sentence unless "he" is specified. For that reason, we would not consider it a proposition. However, "he" can be considered a variable that holds a place for any name. We might want to restrict the value of "he" to all names in the major-league baseball record books. If that is the case, we say that the sentence is a proposition over the set of major-league baseball players, past and present.

Definition: Proposition over a Universe. Let U be a nonempty set. A proposition over U is a sentence that contains a variable that can take on any value in U and that has a definite truth value as a result of any such substitution.

Example 3.6.2.

(a) A few propositions over the integers are $4x^2 - 3x = 0$, $0 \leq n \leq 5$, and "k is a multiple of 3."

(b) A few propositions over the rational numbers are $4x^2 - 3x = 0$, $y^2 = 2$, and $(s - 1)(s + 1) = s^2 - 1$.

(c) A few propositions over the subsets of $\mathbb{P}$ are $(A = \emptyset) \vee (A = \mathbb{P})$, $3 \in A$, and $A \cap \{1, 2, 3\} \neq \emptyset$.

All of the laws of logic that we listed in Section 3.4 are valid for propositions over a universe. For example, if p and q are propositions over the integers, we can be certain that $p \wedge q \Rightarrow p$, because $(p \wedge q) \to p$ is a tautology and is true no matter what values the variables in p and q are given. If we specify p and q to be $p(n) : n < 4$ and $q(n) : n < 8$, we can also say that p implies $p \wedge q$. This is not a usual implication, but for the propositions under discussion, it is true. One way of describing this situation in general is with truth sets.

TRUTH SETS

Definition: Truth Set. *If p is a proposition over U, the truth set of p is* $T_p = \{a \in U \mid p(a) \text{ is true}\}$.

Example 3.6.3. The truth set of the proposition $\{1, 2\} \cap A = \emptyset$ taken as a proposition over the power set of $\{1, 2, 3, 4\}$ is $\{\emptyset, \{3\}, \{4\}, \{3, 4\}\}$.

Example 3.6.4. In the universe $\mathbb{Z}$ (the integers), the truth set of $4x^2 - 3x = 0$ is $\{0\}$. If the universe is expanded to the rational numbers, the truth set becomes $\{0, 3/4\}$. The term solution set is often used for the truth set of an equation such as the one in this example.

Definition*: Tautology and Contradiction. A proposition over U is a tautology if its truth set is U. It is a contradiction if its truth set is empty.*

Example 3.6.5. $(s - 1)(s + 1) = s^2 - 1$ is a tautology over the rational numbers. $x^2 - 2 = 0$ is a contradiction over the rationals.

The truth sets of compound propositions can be expressed in terms of the truth sets of simple propositions. For example, if $a \in T_{p \wedge q}$, then a makes $p \wedge q$ true. Therefore, a makes both p and q true, which means that $a \in T_p \cap T_q$. This explains why the truth set of the conjunction of two propositions equals the intersection of the truth sets of the two propositions. The following list summarizes the connection between compound and simple truth sets:

$$T_{p \wedge q} = T_p \cap T_q$$

$$T_{p \vee q} = T_p \cup T_q$$

$$T_{\neg p} = {T_p}^c$$

$$T_{p \leftrightarrow q} = \left(T_p \cap T_q\right) \cup \left({T_p}^c \cap {T_q}^c\right)$$

$$T_{p \to q} = {T_p}^c \cup T_q$$

Definition*: Equivalence. Two propositions are equivalent if* $p \leftrightarrow q$ *is a tautology. In terms of truth sets, this means that p and q are equivalent if* $T_p = T_q$.

Example 3.6.6.

(a) $n + 4 = 9$ and $n = 5$ are equivalent propositions over the integers.

(b) $A \cap \{4\} \neq \emptyset$ and $4 \in A$ are equivalent propositions over the power set of the natural numbers.

Definition*: Implication. If p and q are propositions over U, p implies q if* $p \to q$ *is a tautology.*

Since the truth set of $p \to q$ is ${T_p}^c \cup T_q$, the Venn diagram for $T_{p \to q}$ in Figure 3.6.1 shows that $p \Rightarrow q$ when $T_p \subseteq T_q$.

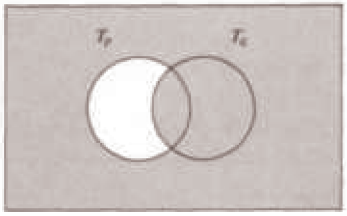


FIGURE 3.6.1 Venn diagram for $T_{p\to q}$

Example 3.6.7.

(a) Over the natural numbers: $n < 4 \Rightarrow n < 8$ since $\{0, 1, 2, 3, 4\} \subseteq \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$.

(b) Over the power set of the integers: $\left|A^c\right| = 1$ implies $A \cap \{0, 1\} \neq \emptyset$.

(c) $A \subseteq$ even integers $\Rightarrow A \cap$ odd integers $= \emptyset$.

EXERCISES FOR SECTION 3.6

A Exercises

1. If $U = \mathcal{P}(\{1, 2, 3, 4\})$, what are the truth sets of the following propositions?

(a) $A \cap \{2, 4\} = \emptyset$.

(b) $3 \in A$ and $1 \notin A$.

(c) $A \cup \{1\} = A$.

(d) A is a proper subset of $\{2, 3, 4\}$.

(e) $|A| = \left|A^c\right|$.

2. Over the universe of positive integers, define

$p(n)$: n is prime and $n < 32$.

$q(n)$: n is a power of 3.

$r(n)$: n is a divisor of 27.

(a) What are the truth sets of these propositions?

(b) Which of the three propositions implies one of the others?

3. If $U = \{0, 1, 2\}$, how many propositions over U could you list without listing two that are equivalent?

4. Given the propositions over the natural numbers:

$p : n < A$

$q : 2n > 17$

r : n is a divisor of 18

what are the truth sets of:

(a) q

(b) $p \wedge q$

(c) r

(d) $q \to r$

5. Suppose that s is a proposition over $\{1, \ldots, 8\}$. If $T_s = \{1, 3, 5, 7\}$, give two examples of propositions that are equivalent to s.

6. (a) Determine the truth sets of the following propositions over the

positive integers:

$p(n)$: n is a perfect square and $n < 100$.

$q(n) : n = |\mathcal{P}(A)|$ for some set A

(b) Determine $T_{p \wedge q}$ for p and q above.

7. Let the universe be $\mathbb{Z}$, the set of integers. Which of the following propositions are equivalent over $\mathbb{Z}$?

a: $0 < n^2 < 9$.

b: $0 < n^3 < 27$.

c: $0 < n < 3$.

3.7 Mathematical Induction

In this section, we will examine mathematical induction, a technique for proving propositions over the positive integers. Mathematical (or finite) induction reduces the proof that all of the positive integers belong to a truth set to a finite number of steps.

Mathematical Induction is sometimes called finite induction.

Example 3.7.1. Consider the following proposition over the positive integers, which we will label $p(n)$: The sum of the positive integers from 1 to n is $\frac{n(n+1)}{2}$. This is a well-known formula that is quite simple to verify for a given value of n. For example, $p(5)$ is: The sum of the positive integers from 1 to 5 is $\frac{5(5+1)}{2}$. Indeed, $1 + 2 + 3 + 4 + 5 = 15 = \frac{5(5+1)}{2}$. Unfortunately, this doesn't serve as a proof that $p(n)$ is a tautology. All that we've established is that 5 is in the truth set of p. Since the positive integers are infinite, we certainly can't use this approach to prove the formula.

An Analogy: Mathematical induction is often useful in overcoming a problem such as this one. A proof by mathematical induction is similar to knocking over a row of closely spaced dominos that are standing on end. To
knock over the five dominos in Figure 3.7.1, all you need to do is push Domino 1 to the right. To be assured that they all will be knocked over, some work must be done ahead of time. The dominos must be positioned so that if any domino is pushed to the right, it will push the next domino in the line.

FIGURE 3.7.1 Illustration of example 3.7.1

Now imagine the propositions $p(1)$, $p(2)$, $p(3)$, … to be an infinite line of dominos. Let's see if these propositions are in the same formation as the dominos were. First, we will focus on one specific point of the line: $p(99)$ and $p(100)$. We are not going to prove that either of these propositions is true, just that the truth of $p(99)$ implies the truth of $p(100)$. In terms of our analogy, if $p(99)$ is knocked over, it will knock over $p(100)$.

In proving $p(99) \Rightarrow p(l00)$, we will use $p(99)$ as our premise. We must prove: The sum of the positive integers from 1 to 100 is $\frac{100(100+1)}{2}$. We start by observing that the sum of the positive integers from 1 to 100 is $(1 + 2 + \cdots + 99) + 100$. That is, the sum of the positive integers from 1 to 100 equals the sum of the first ninety-nine plus the final number, 100. We can now apply our premise, $p(99)$, to the sum $1 + 2 + \cdots + 99$. After rearranging our numbers, we obtain the desired expression for $1 + 2 + \cdots + 100$:

$$\begin{aligned}1 + 2 + \cdots + 99 + 100 &= (1 + 2 + \cdots + 99) + 100\\ &= \frac{99(99+1)}{2} + 100\\ &= \frac{99 \times 100}{2} + \frac{2 \times 100}{2}\\ &= \frac{100 \times 101}{2}\\ &= \frac{100(100+1)}{2}\end{aligned}$$

What we've just done is analogous to checking two dominos in a line and finding that they are properly positioned. Since we are dealing with an infinite line, we must check all pairs at once. This is accomplished by proving that $p(n) \Rightarrow p(n + 1)$ for all n ≥ 1:

$$\begin{aligned}1 + 2 + \cdots + n + (n + 1) &= (1 + 2 + \cdots + n) + (n + 1)\\ &= \frac{n(n+1)}{2} + (n + 1) \qquad \text{by } p(n)\\ &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2}\\ &= \frac{(n+1)(n+2)}{2}\\ &= \frac{(n+1)((n+1)+1)}{2}\end{aligned}$$

They are all lined up! Now look at $p(1)$: The sum of the positive integers from 1 to l is $\frac{1+1}{2}$. Clearly, $p(1)$ is true. This sets off a chain reaction. Since $p(1) \Rightarrow p(2)$, $p(2)$ is true. Since $p(2) \Rightarrow p(3)$, $p(3)$ is true; and so on. ■

The Principle of Mathematical Induction. *Let p(n) be a proposition over the positive integers, then p(n) is a tautology if*
(1) p(1) is true, and
(2) for all n ≥ 1, $p(n) \Rightarrow p(n + 1)$.

Note: The truth of $p(1)$ is called the basis for the induction proof. The premise that p(n) is true in Statement (b) is called the induction hypothesis. The proof that $p(n)$ implies $p(n + 1)$ is called the induction step of the proof. Despite our analogy, the basis is usually done first in an induction proof. The order doesn't really matter.

Example 3.7.2. Consider the implication over the positive integers

$p(n):\ q_0 \to q_1,\ q_1 \to q_2,\ \ldots,\ q_{n-1} \to q_n,\ q_0 \Rightarrow\ q_n$

A proof that $p(n)$ is a tautology follows.

Basis: $p(1)$ is $q_0 \to q_1,\ q_0 \Rightarrow q_1$. This is the logical law of detachment which we know is true. If you haven't done so yet, write out the truth table of $((q_0 \to q_1) \wedge q_0) \to q_1$ to verify this step.

Induction: Assume that $p(n)$ is true for some $n \geq 1$. We want to prove that $p(n+1)$ must be true. That is:

$$q_0 \to q_1,\ q_1 \to q_2,\ \ldots,\ q_{n-1} \to q_n,\ q_n \to q_{n+1},\ q_0 \Rightarrow\ q_{n+1}$$

Here is a direct proof of $p(n+1)$:

Steps	Proposition(s)	Justification
$(1) - (n+1)$	$q_0 \to q_1,\ q_1 \to q_2,\ \ldots,\ q_{n-1} \to q_n,\ q_0$	Premises
$(n+2)$	q_n	$(1) - (n+1)$, $p(n)$
$(n+3)$	$q_n \to q_{n+1}$	Premise
$(n+4)$	q_{n+1}	$(n+2)$, $(n+3)$, detachment ■

Example 3.7.3. For all $n \geq 1$, $n^3 + 2n$ is a multiple of 3. An inductive proof follows:

Basis: $1^3 + 2(1) = 3$ is a multiple of 3.

The basis is almost always this easy!

Induction: Assume that $n \geq 1$ and $n^3 + 2n$ is a multiple of 3. Consider $(n+1)^3 + 2(n+1)$. Is it a multiple of 3?

$$\begin{aligned}(n+1)^3 + 2(n+1) &= (n^3 + 3n^2 + 3n + 1) + (2n + 2) & .\\ &= n^3 + 2n + 3n^2 + 3n + 3 & \text{Rearrange the terms}\\ &= (n^3 + 2n) + 3(n^2 + n + 1)\end{aligned}$$

Yes, $(n+1)^3 + 2(n+1)$ is the sum of two multiples of 3; therefore, it is also a multiple of 3. ■

Variations of Induction

Now we will discuss some of the variations of the principle of mathematical induction. The first simply allows for universes that are similar to $\mathbb{P}$, like $\{-2, -1, 0, 1, \ldots\}$ or $\{5, 6, 7, 8, \ldots\}$.

Principle of Mathematical Induction (Generalized). If $p(n)$ is a proposition over $\{k_0,\ k_0 + 1,\ k_0 + 2,\ \ldots\}$, where k_0 is any integer, then $p(n)$ is a tautology if
(1) $p(k_0)$ is true, and
(2) for all $n \geq k_0$, $p(n) \Rightarrow p(n+1)$.

Example 3.7.4. In Chapter 2, we stated that the number of different permutations of k elements taken from an n element set, $P(n;\ k)$, can be computed with the formula $\frac{n!}{(n-k)!}$. We can prove this statement by induction on n. For $n \geq 0$, let $q(n)$ be the proposition

$$P(n;\ k) = \frac{n!}{(n-k)!} \text{ for all } k \text{ from 0 to } n.$$

Basis: $q(0)$ states that

$P(0;\ 0) =$ the number of ways that 0 elements can be
selected from the empty set and arranged in order
$= 0!/0! = 1$.

This is true — a general law in combinatorics is that there is exactly one way of doing nothing.

Induction: Assume that $q(n)$ is true for some natural number n. It is left for us to prove that this assumption implies that $q(n+1)$ is true. Suppose that we have a set of cardinality $n+1$ and want to select and arrange k of its elements. There are two cases to consider, the first of which is easy. If k = 0, then there is one way of selecting zero elements from the set; hence

$$P(n+1;\ 0) = 1 = \frac{(n+1)!}{(n+1+0)!}$$

and the formula works in this case.

The more challenging case is to verify the formula when k is positive and less than or equal to $n+1$. Here we count the value of $P(n+1;\ k)$ by counting the number of ways that the first element in the arrangement can be filled and then counting the number of ways that the remaining $k-1$ elements can be filled in using the induction hypothesis.

There are $n+1$ possible choices for the first element. Since that leaves n elements to fill in the remaining $k-1$ positions, there are $P(n;\ k-1)$ ways of completing the arrangement. By the rule of products,

$$\begin{aligned}P(n+1;k) &= (n+1)\,P(n;k-1)\\ &= (n+1)\,\frac{n!}{(n-(k-1))!}\\ &= \frac{(n+1)\,n!}{(n-k+1)!}\\ &= \frac{(n+1)!}{((n+1)-k)!} \quad \blacksquare\end{aligned}$$

A second variation allows for the expansion of the induction hypothesis. The course-of-values principle includes the previous generalization. It is also sometimes called *strong induction*.

The Course-of-Values Principle of Mathematical Induction. If $p(n)$ is a proposition over $\{k_0,\ k_0+1, k_0+2, \ldots\}$, where k_0 is any integer, then $p(n)$ is a tautology if
(1) p(k_0) is true, and
(2) for all $n \geq k_0$, $p(k_0),\ p(k_0+1),\ \ldots,\ p(n) \Rightarrow p(n+1)$.

Example 3.7.5. A prime number is defined as a positive integer that has exactly two positive divisors, 1 and itself. There are an infinite number of primes. The list of primes starts with 2, 3, 5, 7, 11,... . The proposition over $\{2,\ 3,\ 4,\ \ldots\}$ that we will prove here is $p(n)$: n can be written as the product of one or more primes. In most texts, the assertion that $p(n)$ is a tautology would appear as:

Theorem. *Every positive integer greater than or equal to 2 has a prime decomposition.*

If you were to encounter this theorem outside the context of a discussion of mathematical induction, it might not be obvious that the proof can be done by induction. Recognizing when an induction proof is appropriate is mostly a matter of experience. Now on to the proof!

Basis: Since 2 is a prime, it is already decomposed into primes (one of them).

Induction: Suppose that for some $k \geq 2$ all of the integers 2, 3, $\ldots$, k have a prime decomposition. Notice the course-of-value hypothesis. Consider $k+1$. Either $k+1$ is prime or it isn't. If $k+1$ is prime, it is already decomposed into primes. If not, then $k+1$ has a divisor, d, other than 1 and $k+1$. Hence, $k+1 = c\,d$ where both c and d are between 2 and k. By the induction hypothesis, c and d have prime decompositions, $c_1\,c_2 \cdots c_m$ and $d_1\,d_2 \cdots d_m$, respectively. Therefore, $k+1$ has the prime decomposition $c_1\,c_2 \cdots c_m\,d_1\,d_2 \cdots d_m$. ■

HISTORICAL NOTE

Mathematical induction originated in the late nineteenth century. Two mathematicians who were prominent in its development were Richard Dedekind and Giuseppe Peano. Dedekind developed a set of axioms that describe the positive integers. Peano refined these axioms and gave a logical interpretation to them. The axioms are usually called the Peano Postulates.

Peano's Postulates. The system of positive integers consists of a nonempty set, P; a least element of P, denoted 1; and a "successor function," s, with the properties
(1) If $k \in \mathbb{P}$, then there is an element of $\mathbb{P}$ called the successor of k, denoted $s(k)$.
(2) No two elements of $\mathbb{P}$ have the same successor.
(3) No element of $\mathbb{P}$ has 1 as its successor.
(4) If $S \subseteq \mathbb{P}$, $1 \in$ S, and k $\in$ S $\Rightarrow s(k) \in S$, then $S = \mathbb{P}$.

Richard Dedekind

Giuseppe Peano

Notes:

(a) You might recognize $s(k)$ as simply being $k+1$.

(b) Axiom 4, mentioned above, is the one that makes mathematical induction possible. In an induction proof, we simply apply that axiom to the truth set of a proposition.

Exercises for Section 3.7

A Exercises

1. Prove that the sum of the first n odd integers equals n^2 .

2. Prove that if $n \geq 1$, then $1\,(1\,!) + 2\,(2\,!) + \cdots + n\,(n!) = (n + 1)! - 1$.

3. Prove that for $n \geq 1$: $\sum_{k=1}^{n} k^2 = \frac{1}{6}\, n(n+1)\,(2\,n+1)$.

4. Prove that for n ≥ 1: $\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$.

5. Use mathematical induction to show that for $n \geq 1$,

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

6. Prove that if $n \geq 2$, the generalized DeMorgan's Law is true:

$$\neg\,(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \Leftrightarrow (\neg\, p_1) \vee (\neg\, p_2) \vee \cdots \vee (\neg\, p_n)$$

B Exercises

7. The number of strings of n zeros and ones that contain an even number of ones is 2^{n-1}. Prove this fact by induction for $n \geq 1$.

8. Let $p\,(n)$ be $8^n - 3^n$ is a multiple of 5. Prove that $p\,(n)$ is a tautology over $\mathbb{N}$.

9. Suppose that there are n people in a room, $n \geq 1$, and that they all shake hands with one another. Prove that $\frac{n(n-1)}{2}$ handshakes will have occurred.

10. Prove that it is possible to make up any postage of eight cents or more using only three- and five-cent stamps.

C Exercises

11. Generalized associativity. It is well known that if a_1, a_2, and a_3 are numbers, then no matter what order the sums in the expression $a_1 + a_2 + a_3$ are taken in, the result is always the same. Call this fact $p(3)$ and assume it is true. Prove using course-of-values induction that if $a_1, a_2, \ldots$, and a_n are numbers, then no matter what order the sums in the expression $a_1 + a_2 + \cdots + a_n$ are taken in, the result is always the same.

12. Let S be the set of all numbers that can be produced by applying any of the rules below in any order a finite number of times.

Rule 1: $\frac{1}{2} \in S$

Rule 2: $1 \in S$

Rule 3: If a and b have been produced by the rules, then $a\,b \in S$.

Rule 4: If a and b have been produced by the rules, then $\frac{a+b}{2} \in S$.

Prove by course-of-values induction that $a \in S \Rightarrow 0 < a \leq 1$. Hint: The number of times the rules are applied should be the integer that you do the induction on.

13. A recursive definition is similar to an inductive proof. It consists of a basis, usually the simple part of the definition, and the recursion, which defines complex objects in terms of simpler ones. For example, if x is a real number and n is a positive integer, we can define x^n as follows:

Basis: $x^1 = x$.

Recursion: if $n \geq 2, x^n = x^{n-1}\,x$.

For example, $x^3 = x^2\,x = (x^1\,x)\,x = (x\,x)\,x$. Proofs involving objects that are defined recursively are often inductive. Prove that if $n, m \in \mathbb{P}$, $x^{m+n} = x^m\,x^n$. Hint: Let $p\,(m)$ be the proposition that $x^{m+n} = x^m\,x^n$ for all $n \geq 1$. There is much more on recursion in Chapter 8.

14. Let S be a finite set and let P_n,, be defined recursively by $P_1 = S$ and $P_n = S \times P_{n-1}$ for $n \geq 2$.

(a) List the elements of P_3 for the case S = {a, b}.

(b) Determine the formula for $|\,P_n\,|$, given that $|\,S\,| = k$, and prove your formula by induction.

3.8 Quantifiers

As we saw in Section 3.6, if $p(n)$ is a proposition over a universe U, its truth set T_p is equal to a subset of U. In many cases, such as when $p(n)$ is an equation, we are most concerned with whether T_p is empty or not. In other cases, we might be interested in whether $T_p = U$; that is, whether $p(n)$ is a tautology. Since the conditions $T_p \neq \emptyset$ and $T_p = U$ are so often an issue, we have a special system of notation for them.

THE EXISTENTIAL QUANTIFIER

If $p(n)$ is a proposition over U with $T_p \neq \emptyset$, we commonly say "There exists an n in U such that $p(n)$ (is true)." We abbreviate this with the symbols $(\exists\, n)_U\, (p(n))$. The symbol $\exists$ is called the existential quantifier. If the context is clear, the mention of U is dropped: $(\exists\, n)\, (p(n))$.

Example 3.8.1.

(a) $(\exists\, k)_{\mathbb{Z}} \left(k^2 - k - 12 = 0\right)$ is another way of saying that there is an integer that solves the equation k 2 - k - 12 = 0. The fact that two such integers exist doesn't affect the truth of this proposition in any way.

(b) $(\exists\, k)_{\mathbb{Z}}\, (3\, k = 102)$ simply states that 102 is a multiple of 3, which is true. On the other hand, $(\exists\, k)_{\mathbb{Z}}\, (3\, k = 100)$ states that 100 is a multiple of 3, which is false.

(c) $(\exists\, x)_{\mathbb{R}}\, (x^2 + 1 = 0)$ is false since the solution set of the equation $x^2 + 1 = 0$ in the real numbers is empty. It is common to write $(\nexists\, x)_{\mathbb{R}}\, (x^2 + 1 = 0)$ in this case.

There are a wide variety of ways that you can write a proposition with an existential quantifier. Table 3.8.1 contains a list of different variations that could be used for both the existential and universal quantifiers.

THE UNIVERSAL QUANTIFIER

If $p(n)$ is a proposition over U with $T_p = U$, we commonly say "For all n in U, $p(n)$ (is true)." We abbreviate this with the symbols $(\forall\, n)_U\, (p(n))$. The symbol $\forall$ is called the universal quantifier. If the context is clear, the mention of U is dropped: $(\forall\, n)\, (p(n))$.

Example 3.8.2.

(a) We can say that the square of every real number is non-negative symbolically with a universal quantifier: $(\forall\, x)_{\mathbb{R}}\, (x^2 \geq 0)$.

(b) $(\forall\, n)_{\mathbb{Z}}\, (n + 0 = 0 + n = n)$ says that the sum of zero and any integer n is n. This fact is called the identity property of zero for addition.

Table 3.8.1 Notational Variations for Existential and Universal Quantifiers

Universal Quantifier	Existential Quantifier
$(\forall\, n)_U\, (p(n))$	$(\exists\, n)_U\, (p(n))$
$(\forall\, n \in U)\, (p(n))$	$(\exists\, n \in U)\, (p(n))$
$\forall\, n \in U,\ p(n)$	$\exists\, n \in U$ such that $p(n)$
$p(n),\ \forall\, n \in U$	$p(n)$ is true for some $n \in U$
$p(n)$ is true for all $n \in U$	

THE NEGATION OF QUANTIFIED PROPOSITIONS

When you negate a quantified proposition, the existential and universal quantifiers complement one another.

Example 3.8.3. Over the universe of animals, define F(x) : x is a fish and W(x) : x lives in the water. We know that the proposition W(x) → F(x) is not always true. In other words, (∀x)(W(x) → F(x)) is false. Another way of stating this fact is that there exists an animal that lives in the water and is not a fish; that is,

$$\begin{aligned} \neg\, (\forall\, x)\, (W(x) \rightarrow F(x)) &\Leftrightarrow (\exists\, x)\, (\neg\, (W(x) \rightarrow F(x))) . \\ &\Leftrightarrow (\exists\, x)\, (W(x) \wedge \neg\, F(x)) \end{aligned}$$

Note that the negation of a universally quantified proposition is an existentially quantified proposition. In addition, when you negate an existentially quantified proposition, you obtain a universally quantified proposition.   Symbolically,

$\neg\, ((\forall\, n)_U\, (p(n))) \Leftrightarrow (\exists\, n)_U\, (\neg\, p(n)))$, and

$\neg\, ((\exists\, n)_U\, (p(n))) \Leftrightarrow (\forall\, n)_U\, (\neg\, p(n)))$

Example 3.8.4.

(a) The ancient Greeks first discovered that $\sqrt{2}$ is an irrational number; that is, $\sqrt{2}$ is not a rational number. $\neg((\exists\, r)_{\mathbb{Q}}\,(r^2 = 2))$ and $(\forall\, r)_{\mathbb{Q}}\,(r^2 \neq 2)$ both state this fact symbolically.

(b) $\neg((\forall\, n)_{\mathbb{P}}\,(n^2 - n + 41 \text{ is prime}))$ is equivalent to $(\exists\, n)_{\mathbb{P}}\,(n^2 - n + 41 \text{ is composite})$. They are both either true or false.

MULTIPLE QUANTIFIERS

If a proposition has more than one variable, then you can quantify it more than once. For example, if $p(x, y): x^2 - y^2 = (x + y)(x - y)$ is a tautology over the set of all pairs of real numbers because it is true for each pair (x, y) in $\mathbb{R} \times \mathbb{R}$. Another way to look at this proposition is as a proposition with two variables. The assertion that $p(x, y)$ is a tautology could be quantified as $(\forall\, x)_{\mathbb{R}}\,((\forall\, y)_{\mathbb{R}}\,(p(x, y)))$ or $(\forall\, y)_{\mathbb{R}}\,((\forall\, x)_{\mathbb{R}}\,(p(x, y)))$

In general, multiple universal quantifiers can be arranged in any order without logically changing the meaning of the resulting proposition. The same is true for multiple existential quantifiers. For example, $p(x, y) : x + y = 4 \text{ and } x - y - 2$ is a proposition over $\mathbb{R} \times \mathbb{R}$. $(\exists\, x)_{\mathbb{R}}\,((\exists\, y)_{\mathbb{R}}\,(x + y = 4 \text{ and } x - y = 2))$ and $(\exists\, y)_{\mathbb{R}}\,((\exists\, x)_{\mathbb{R}}\,(x + y = 4 \text{ and } x - y = 2))$ are equivalent. A proposition with multiple existential quantifiers such as this one says that there are simultaneous values for the quantified variables that make the proposition true. A similar example is $q(x, y) : 2x - y - 2 \text{ and } 4x - 2y = 5$, which is always false; and the following are all equivalent

$$\begin{aligned}
\neg((\exists\, x)_{\mathbb{R}}\,((\exists\, y)_{\mathbb{R}}\,(q(x, y)))) &\Leftrightarrow \neg(\exists\, y)_{\mathbb{R}}\,((\exists\, x)_{\mathbb{R}}\,(q(x, y)))) \\
&\Leftrightarrow (\forall\, y)_{\mathbb{R}}\,(\neg((\exists\, x)_{\mathbb{R}}\,(q(x, y))) \\
&\Leftrightarrow ((\forall\, y)_{\mathbb{R}}\,((\forall\, x)_{\mathbb{R}}\,(\neg q(x, y)))) \\
&\Leftrightarrow ((\forall\, x)_{\mathbb{R}}\,((\forall\, y)_{\mathbb{R}}\,(\neg q(x, y))))
\end{aligned}$$

When existential and universal quantifiers are mixed, the order cannot be exchanged without possibly changing the meaning of the proposition. For example, let $\mathbb{R}^+$ be the positive real numbers, $x : (\forall\, a)_{\mathbb{R}^+}\,((\exists\, b)_{\mathbb{R}^+}\,(a b = 1))$ and $y : (\exists\, b)_{\mathbb{R}^+}\,((\forall\, a)_{\mathbb{R}^+}\,(a b = 1))$ have different meanings; x is true, while y is false.

TIPS ON READING MULTIPLY QUANTIFIED PROPOSITIONS

It is understandable that you would find propositions such as x difficult to read. The trick to deciphering these expressions is to "peel" one quantifier off the proposition just as you would peel off the layers of an onion (but quantifiers shouldn't make you cry). Since the outermost quantifier in x is universal, x says that $z(a) : (\exists\, b)_{\mathbb{R}^+}\,(a b = 1)$ is true for each value that a can take on. Now take the time to select a value for a, like 6. For the value that we selected, we get $z(6) : (\exists\, b)_{\mathbb{R}^+}\,(6 b = 1)$, which is obviously true since $6 b = 1$ has a solution in the positive real numbers. We will get that same truth value no matter which positive real number we choose for a; therefore, $z(a)$ is a tautology over $\mathbb{R}^+$ and we are justified in saying that x is true. The key to understanding propositions like x on your own is to experiment with actual values for the outermost variables as we did above.

Now consider y. To see that y is false, we peel off the outer quantifier. Since it is an existential quantifier, all that y says is that some positive real number makes $w(b) : (\forall\, a)_{\mathbb{R}^+}\,(a b = 1)$ true. Choose a few values of b to see if you can find one that makes $w(b)$ true. For example, if we pick $b = 2$, we get $(\forall\, a)_{\mathbb{R}^+}\,(2 a = 1)$, which is false, since $2a$ is almost always different from 1. You should be able to convince yourself that no value of b will make $w(b)$ true. Therefore, y is false.

Another way of convincing yourself that y is false is to convince yourself that $\neg y$ is true:

$$\begin{aligned}
\neg((\exists\, b)_{\mathbb{R}^+}\,((\forall\, a)_{\mathbb{R}^+}\,(a b = 1))) &\Leftrightarrow (\forall\, b)_{\mathbb{R}^+}\,\neg\,((\forall\, a)_{\mathbb{R}^+}\,(a b = 1)) \\
&\Leftrightarrow (\forall\, b)_{\mathbb{R}^+}\,((\exists\, a)_{\mathbb{R}^+}\,(a b \neq 1))
\end{aligned}$$

In words, for each value of b, a value for a that makes $a b \neq 1$. One such value is $a = \frac{1}{b} + 1$. Therefore, $\neg y$ is true.

EXERCISES FOR SECTION 3.8

A Exercises

1. Let $C(x)$ be "x is cold-blooded," let $F(x)$ be "x is a fish," and let $S(x)$ be "x lives in the sea."

(a) Translate into a formula: Every fish is cold-blooded.

(b) Translate into English: $(\exists\, x)\,(S(x) \wedge \neg F(x))$

and $(\forall\, x)\,(F(x) \rightarrow S(x))$.

2. Let $M(x)$ be "x is a mammal," let $A(x)$ be "x is an animal," and let $W(x)$ be "x is warm-blooded."

(a) Translate into a formula: Every mammal is warm-blooded.

(b) Translate into English: $(\exists\, x)\,(A(x) \wedge (\neg M(x)))$.

3. Over the universe of books, define the propositions $B(x)$: x has a blue cover, $M(x)$: x is a mathematics book, $C(x)$: x is published in the United States, and $R(x, y)$: The bibliography of x includes y. Translate into words:

(a) $(\exists\, x)\,(\neg B(x))$.

(b) $(\forall x)(M(x) \wedge U(x) \rightarrow B(x))$.

(c) $(\exists x)(M(x) \wedge \neg B(x))$.

(d) $(\exists y)((\forall x)(M(x) \rightarrow R(x, y)))$.

Express using quantifiers:

(e) Every book with a blue cover is a mathematics book.

(f) There are mathematics books that are published outside the United States.

(g) Not all books have bibliographies.

revised

4. Let the universe of discourse, U, be the set of all people, and let $M(x, y)$ be "x is the mother of y."

(a) Which of the following is a true statement? Translate it into English.

(i) $(\exists x)_U((\forall y)_U(M(x, y)))$

(ii) $(\forall y)_U((\exists x)_U(M(x, y)))$

(b) Translate the following statement into logical notation using quantifiers and the proposition $M(x, y)$ over U: "Everyone has a grandmother,"

5. Translate into your own words and indicate whether it is true or false that $(\exists u)_{\mathbb{Z}}(4u^2 - 9 = 0)$.

6. Use quantifiers to say that $\sqrt{3}$ is an irrational number.

7. What do the following propositions say, where U is the power set of $\{1, 2, \ldots, 9\}$? Which of these propositions are true?

(a) $(\forall A)_U(|A| \neq |A^c|)$.

(b) $(\exists A)_U(\exists B)_U(|A| = 5,\ |B| = 5,\ \text{and } A \cap B = \emptyset)$

(c) $(\forall A)_U(\forall B)_U(A - B = B^c - A^c)$

8. Use quantifiers to state that for every positive integer, there is a larger positive integer.

9. Use quantifiers to state that the sum of any two rational numbers is rational.

10. Over the universe of real numbers, use quantifiers to say that the equation $a + x = b$ has a solution for all values of a and b. Hint: You will need three quantifiers.

11. Let n be a positive integer. Describe using quantifiers:

(a) $x \in \bigcup_{k=1}^{n} A_k$

(b) $x \in \bigcap_{k=1}^{n} A_k$

12. Prove that $(\exists x)(\forall y)(p(x, y)) \Rightarrow (\forall y)(\exists x)(p(x, y))$, but the converse is not true.

3.9 A Review of Methods of Proof

One of the major goals of this chapter is to acquaint the reader with the key concepts in the nature of proof in logic, which of course carries over into all areas of mathematics and its applications. In this section we will stop, reflect, and "smell the roses," so that these key ideas are not lost in the many concepts covered in logic. In Chapter 4 we will use set theory as a vehicle for further practice and insights into methods of proof.

KEY CONCEPTS IN PROOF

1. All theorems in mathematics can be expressed in "If P then C" ($P \Rightarrow C$) format, or in "C_1 if and only if C_2" ($P \Leftrightarrow C$) format. The latter is equivalent to "If C_1 then C_2, and if C_2 then C_1." Alternate ways of expressing conditional propositions are found in Section 3.1.

2. In "If P then C," P is the premise (or hypothesis) and C is the conclusion. It is important to realize that a theorem makes a statement that is dependent on the premise being true.

3. There are two basic methods for proving $P \Rightarrow C$:

(a) **Direct:** Assume P is true and prove C is true; and

(b) **Indirect (proof by contradiction):** Assume P is true and C is false and prove that this leads to a contradiction of some premise, theorem, or basic concept.

4. The method of proof for "**If and only if**" (iff) theorems is found in the law $(P \leftrightarrow C) \Leftrightarrow ((P \to C) \land (C \to P))$. Hence to prove an "If and only if" statement one must prove an "if . . . then ..." statement and its converse.

The initial response of most people when confronted with the task of being told they must be able to read and do proofs is:

(a) Why? or,

(b) I cannot do proofs.

To answer the first question, problem solving, even on the most trivial level, involves being able to read statements. First we must understand the problem and know the hypothesis; second, we must realize when we are done and we must understand the conclusion. To apply theorems or algorithms we must be able to read theorems and their proofs intelligently.

To be able to do the actual proofs of theorems we are forced to learn:

(1) the actual meaning of the theorems, and

(2) the basic definitions and concepts of the topic discussed.

For example, when we discuss rational numbers and refer to a number x as being rational, this means we can substitute a fraction $\frac{p}{q}$ in place of x, with the understanding that p and q are integers and $q \neq 0$. Therefore, to prove a theorem about rational numbers it is absolutely necessary that you know what a rational number "looks like."

It's easy to comment on the response, "I cannot do proofs." Have you tried? As elementary school students we were in awe of anyone who could handle algebraic expressions, especially complicated ones. We learned by trying and applying ourselves. Maybe we cannot solve all problems in algebra or calculus, but we are comfortable enough with these subjects to know that we can solve many and can express ourselves intelligently in these areas. The same remarks hold true for proofs.

THE ART OF PROVING $P \Rightarrow C$

First one must completely realize what is given, the hypothesis. The importance of this is usually overlooked by beginners. It makes sense, whenever you begin any task, to spend considerable time thinking about the tools at your disposal. Write down the premise in precise language. Similarly, you have to know when the task is finished. Write down the conclusion in precise language. Then you usually start with P and attempt to show that C follows logically. How do you begin? Basically you attack the proof the same way you solve a complicated equation in elementary algebra. You may not know exactly what each and every step is but you must try something. If we are lucky, C follows naturally; if it doesn't, try something else. Often what is helpful is to work backward from C. Finally, we have all learned, possibly the hard way, that mathematics is a participating sport, not a spectator sport. One learns proofs by doing them, not by watching others do them. We give several illustrations of how to set up the proofs of several examples. Our aim here is not to prove the statements given, but to concentrate on the logical procedure.

Example 3.9.1. We will outline a proof that the sum of any two odd integers is even. Our first step will be to write the theorem in the familiar conditional form: If j and k are odd integers, then $j + k$ is even. The premise and conclusion of this theorem should be clear now. Notice that if j and k are not both odd, then the conclusion may or may not be true. Our only objective is to show that the truth of the premise forces the conclusion to be true. Therefore, we can express the integers j and k in the form that all integers take; that is:

$$n \in \mathbb{Z} \text{ is odd implies } (\exists\, m \in \mathbb{Z})\,(n = 2m + 1).$$

This observation allows us to examine the sum y + k and to verify that it must be even.

Example 3.9.2. Let $n \in \mathbb{Z}$. We will outline a proof that n^2 is even if and only if n is even.

Outline of a proof: Since this is an "If and only if theorem we must prove two facts (see key concept number 4 above):

I. (⇒) If n^2 is even, then n is even. To do this directly, assume that n^2 is even and prove that n is even. To do this indirectly, assume n^2 is even and that n is odd, and reach a contradiction. It turns out that the latter of the two approaches is easiest here.

II. (⇐) If n is even, then n^2 is even. To do this directly, assume that n is even and prove that n^2 is even.

Now that we have broken the theorem down into two parts and know what to prove, we proceed to prove the two implications. The final ingredient that we need is a convenient way of describing even integers. When we refer to an integer n (or m, or k,. . .) as even, we can always replace it with a product of the form $2\,q$, where q is an integer (more precisely, $(\exists\, q)_{\mathbb{Z}}\,(n = 2\,q)$). In other words, for an integer to be even it must have a factor of two in its prime decomposition.

Example 3.9.3. Our final example will be an outline of the proof that the square root of 2 is irrational (not an element of $\mathbb{Q}$). This is an example of the theorem that does not appear to be in the standard $P \Rightarrow C$ form. One way to rephrase the theorem is: If x is a rational number, then $x^2 \neq 2$. A direct proof of this theorem would require that we verify that the square of every rational number is not equal to 2. There is no convenient way of doing this, so we must turn to the indirect method of proof. In such a proof, we assume that x is a rational number and that $x^2 = 2$ (i.e., $\sqrt{2}$ is a rational number). This will lead to a contradiction. In order to reach this contradiction, we need to use the following facts:

(a) A rational number is a quotient of two integers.

(b) Every fraction can be reduced to lowest terms, so that the numerator and denominator have no common factor greater than 1.

(c) If n is an integer, n^2 is even if and only if n is even.

EXERCISES FOR SECTION 3.9

B Exercises

1. Prove that the sum of two odd positive integers is even.

2. Write out a complete proof that if n is an integer, n^2 is even if and only if n is even.

3. Write out a complete proof that $\sqrt{2}$ is irrational.

4. Prove that $\sqrt[3]{2}$ is an irrational number.

5. Prove that if x and y are real numbers such that $x + y \leq 1$, then either $x \leq \frac{1}{2}$ or $y \leq \frac{1}{2}$.

6. Use the following definition of absolute value to prove the given statements: If x is a real number, then the absolute value of x, $|x|$, is defined by:

$$\left|x\right| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

(a) For any real number x, $|x| \geq 0$. Moreover, $|x| = 0$ implies $x = 0$.

(b) For any two real numbers x and y, $|x| \cdot |y| = |x\,y|$.

(c) For any two real numbers x and y, $|x + y| \leq |x| + |y|$.

SUPPLEMENTARY EXERCISES FOR CHAPTER 3

Section 3.1

1. Construct the truth tables of

(a) $p \lor p$

(b) $p \land (\neg p)$

(c) $p \lor (\neg p)$

(d) $p \land p$

2. Express each of the following in symbolic form and determine whether they are true or false:

(a) If $a,\ b \in \mathbb{Z}$, and if $a = 0$ or $b = 0$, then $a \cdot b = 0$.

(b) If $a,\ b \in \mathbb{Z}$, and if $a \cdot b = 0$, then $a = 0$ or $b = 0$.

(c) Let $a,\ b \in \mathbb{Z}$. $a \cdot b = 0$ if and only if $a = 0$ or $b = 0$.

(d) If $\{5\} \subseteq \mathbb{Z}$, then $2 + 3 = 8$.

(e) If $2 + 3 = 8$, then the world is flat.

(f) 5 is an odd integer if and only if 8 is an even integer.

Section 3.2

3. Write the truth table for the expression $p \lor q \land \neg p$.

4. Insert parentheses in the following statements to indicate the order in which the operations are performed:

(a) $p \lor q \land r \lor \neg q$

(b) $p \land \neg q \lor \neg p \land q$

(c) $p \lor q \land r$

(d) $p \land q \lor p \land r \lor q \land r$

Section 3.3

5. Use truth tables to verify that $((p \to \neg q) \land (q \lor r) \land (\neg r)) \Rightarrow \neg p$ is a tautology.

6. Is an implication equivalent to its converse? Verify your answer using a truth table.

7. Prove that an implication is always equivalent to its contrapositive.

8. (a) Construct truth tables for the following propositions generated by p, q, and r.

(i) $r \land (p \land q)$ (ii) $r \lor (p \lor q)$ (iii) $r \land q$

(b) Which of the propositions i, ii, and iii in part (a) imply proposition i? Explain.

9. Suppose that x is a proposition generated by p and q, and x is equivalent to $p \to p \land q$. What is the truth table for x?

10. The Scheffer Stroke is the logical operator defined by the following truth table:

p	q	p|q
0	0	1
0	1	1
1	0	1
1	1	0

Truth Table for the Sheffer Stroke

(a) Prove that $p \mid q$ is equivalent to $\neg (p \land q)$.

The significance of the Sheffer Stroke is that it is a "universal" operator. All other operators can be built from it.

(b) Prove that $\neg p \Leftrightarrow p \mid p$.

(c) Build $\land$ using only the Sheffer Stroke.

(d) Build $\vee$ using only the Sheffer Stroke.

Section 3.4

11. Write the negation of each of the following statements:

    (a) 3 is a prime number and it is even.

    (b) 4 is a prime number or it is odd.

    (c) If I can exhibit an example of a statement then I have proven it true.

    (d) If $x^2 - 11x + 12 = 0$, then $x = 3$ or $x = 8$.

12. Prove that all $\overline{\wedge}$ defined by has the same property as the Sheffere Stroke (see problem 10) in that is is a "universal" operator.

p	q	$p \overline{\wedge} q$
0	0	1
0	1	1
1	0	1
1	1	0

Truth Table for $p\overline{\wedge}q$

13. The following are frequently used and very important tautologies in logic. Use truth tables to prove them.

    (a) $(p \rightarrow q) \Leftrightarrow (\neg q \rightarrow \neg p)$

    (b) $(p \leftrightarrow q) \Leftrightarrow ((p \rightarrow q) \wedge (q \rightarrow p))$

14. Write the following in symbolic notation and prove it is a tautology: "The statement p if and only if q is equivalent to saying if p then q and if q then p."

15. Write the following in symbolic notation and determine whether it is a valid argument: "If I quit my job, then I will starve. If I don't do my work, then I must quit my job. I did my work, therefore I will eat."

16. Write the dual of each of the following statements:

    (a) $(\neg p \vee 0) \Rightarrow 1$

    (b) $(p \vee q) \wedge (\neg p \vee r) \Rightarrow (r \vee q)$

Section 3.5

17. Write the following in symbolic form and then determine its validity. "If this car is made in England then parts are difficult to obtain. This car is expensive, or it is not difficult to obtain parts. But this car is not expensive. Hence it was not made in England."

18. In order to attach the Mark 13 printer to the Lemon III computer, you must set eight "dip switches" in the computer according to the following rules. The switches are labeled a through h and are set to be either ON or OFF.

    (1) Neither a nor c is set the same as d.

    (2) b and g are different if and only if e and g are in the same positions.

    (3) g is OFF if d is OFF, but g is ON if b is OFF.

    (4) d is ON, unless e is the same as/.

    (5) h is not the same as a if either b or e is OFF.

    (6) g is OFF only if e is not the same as h.

    (7) b,f, and g are not all the same.

    How should the switches be set?

19. Consider the following argument:

    If person X does not live in France, then X does not speak French.

    X does not drive a Chevrolet.

    If X lives in France, then he rides a bicycle.

    Either X speaks French or he drives a Chevrolet.

Therefore, X rides a bicycle.

Let p = "X lives in France."

q = "X speaks French."

r = "X drives a Chevrolet."

s = "X rides a bicycle."

Translate the argument into logical notation using these propositions, and prove it by any method except a truth table.

20. Determine the validity of the following argument: "I will miss class only if I sleep late. I will not sleep late. Therefore, I will not miss class."

21. Mayoral candidate Ms. Perpetual Candidate made the following promise to the voters: "If I am elected, I will bring industry to the town. If I bring industry to the town, your taxes will decrease. If your taxes decrease, you will be wealthier. Therefore, if I am elected, you will be wealthier." Express this argument in symbolic notation and determine whether the mayoral candidate is telling the truth.

22. Professor Smoothtalker made the following promise to his class. "If you receive an A in this course, you are happy. You will do all your assignments or you are not happy. If you concentrate too hard, you will not do all your assignments. Therefore, if you are happy, do not concentrate too hard." Is Professor Smoothtalker's argument valid?

23. Determine whether the following argument is valid: Taxes will increase or government spending decreases. Government spending increases or more people have jobs. More people do not have jobs or people are rich. Therefore, if taxes decrease, people are rich.

Section 3.6

24. Let $p(n)$ be $n < 2$ and let $q(n)$ be $n^2 < 5$.

(a) Over the universe of integers, $\mathbb{Z}$, are p and q equivalent? Does one imply the other?

(b) Over the universe of natural numbers, $\mathbb{N}$, are p and q equivalent? Does one imply the other?

25. Prove that: $T_{p\wedge q} = T_p \cap T_q$.

26. Prove that: $T_{p\to q} = T_p{}^c \cup T_q$.

Section 3.7

27. Express 60 and 120 as a product of primes.

28. Prove that for $n \geq 1$

$$\sum_{i=1}^{n} i^3 = \frac{1}{4} n^2 (n+1)^2 = \left(\frac{1}{2} n (n+1)\right)^2$$

29. (a) Prove that $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$ for $k > 1$ and $n \geq k + 1$.

(b) Use mathematical induction to prove the binomial theorem:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \text{ for } n \geq 0.$$

30. Use mathematical induction to prove for all $n \geq 1$ and for all real numbers c, a_i, and b_i, $i = 1, 2, \ldots, n$:

(a) $\sum_{i=1}^{n} (a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i$

(b) $\sum_{i=1}^{n} c\, a_i = c \sum_{i=1}^{n} a_i$

Section 3.8

31. Write the negation of: "Some sailing is dangerous and all fishing is tedious" in graceful English.

32. Prove: $\neg ((\exists u)(\forall v)(p)) \Leftrightarrow (\forall u)((\exists v)(\neg p))$

33. Translate the following sentences into expressions using quantifiers:

(a) All fish except sharks are kind to children.

(b) Either every wine-drinker is very communicative, or some pawn broker is honest and doesn't drink wine.

(c) If all clever philosophers are cynics, and only women are clever philosophers, then, if there are any clever philosophers, some women are cynics.

34. First write each of the following in logical notation using quantifiers, then write the negative of each logical expression using symbols and complete English sentences. If possible, determine which of the statements are true.

(a) All people in this classroom are over six feet tall.

(b) Some of the people in this classroom are over six feet tall and are bald.

(c) Let $U = \{2, 3, 4, 5\}$ and let $p(n)$ denote the statement "n is a prime number." Apply the above directions to the statement: Every number in U is a prime number.

(d) All prime numbers are odd.

(e) You will all pass the course Discrete Structures or you will all fail.

(f) You can fool some of the people some of the time.

35. Use quantifiers to state that for every positive integer, there is a larger positive integer.

36. Over the universe of students in your class, let $N(x, y)$ be "x knows y's name." Interpret in English:

(a) $(\exists x)((\forall y)(N(x, y)))$

(b) $(\forall y)((\exists x)(N(x, y)$ and $x \neq y))$

(c) How would you symbolically say that everyone knows everyone's name?

(d) How would you symbolically say that everyone knows your name?

(e) How would you symbolically say that someone in the class has amnesia?

Section 3.9

37. For any nonzero real number x,

$$x^2 = 1 \quad \Leftrightarrow \quad x = 1 \text{ or } x = -1$$

(a) Outline the logical procedure you would use to prove this statement.

(b) Fill in the proof.

38. Let $a, b, c \in \mathbb{P}$ and read $a \mid b$ as "a divides evenly into b." Consider the statements

(i) $b \mid a$ and $a \mid b$ implies $a = b$.

(ii) If p is prime and $p \mid a^2$, then $p \mid a$.

(a) Are these statements true? Explain your answers.

(b) Is the converse of each of these statements true? Explain your answers.

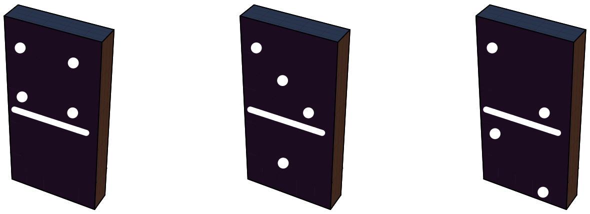
(c) Is the contrapositive of each of these statements true? Explain your answers.

39. Let $a, b \in \mathbb{R}$. A necessary and sufficient condition for $a \cdot b = 0$ is that $a = 0$ or $b = 0$.

(a) Is this statement true? Explain your answer.

(b) Outline the logical procedure you would use to prove this statement.

Chapter 4



MORE ON SETS

GOALS

In this chapter we shall look more closely at some basic facts about sets. One question we could ask ourselves is: Can we manipulate sets similarly to the way we manipulated expressions in basic algebra, or to the way we manipulated propositions in logic? In basic algebra we are aware that $a \cdot (b + c) = a \cdot b + a \cdot c$ for all real numbers a, b, and c. In logic we verified an analogue of this statement, namely, $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r))$, where p, q, and r were arbitrary propositions. If A, B, and C are arbitrary sets, is $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$? How do we convince ourselves of its truth or falsity? Let us consider some approaches to this problem, look at their pros and cons, and determine their validity. Many of the ideas expressed are true, in general, in mathematics. Partitions of sets and min sets will be introduced.

4.1 Methods of Proof for Sets

There are a variety of ways that we could attempt to prove that the distributive law for intersection over union is true; that is, that for any three sets, A, B, and C, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. We start with a common "non-proof" and then work toward more acceptable methods.

EXAMPLES AND COUNTEREXAMPLES

We could, for example, let $A = \{1, 2\}$, $B = \{5, 8, 10\}$, and $C = \{3, 2, 5\}$, and determine whether the distributive law is true. Obviously, in doing this we will have only determined that the distributive law is true for this one example. It does not prove the distributive law for all possible sets A, B, and C and hence is an invalid method of proof. However, trying a few examples has considerable merit insofar as it makes us more comfortable with the statement in question, and indeed if the statement is not true for the example, we have disproved the statement.

***Definition*: *Counterexample*.** *An example that disproves a statement is called a counterexample.*

Example 4.1.1. From basic algebra we learned that multiplication is distributive over addition. Is addition distributive over multiplication; that is, is $a + (b \cdot c) = (a + b) \cdot (a + c)$? If we choose the values $a = 3$, $b = 4$, and $c = 1$, we find that $3 + (4 \cdot 1) \neq (3 + 4) \cdot (3 + 1)$. Therefore, this set of values serves as a counterexample to a distributive law of addition over multiplication.

PROOF USING VENN DIAGRAMS

In this method, we illustrate both sides of the statement via a Venn diagram and determine whether both Venn diagrams give us the same "picture," For example, the left side of the distributive law is developed in Figure 4.1.1 and the right side in Figure 4.1.2. Note that the final results give you the same shaded area.

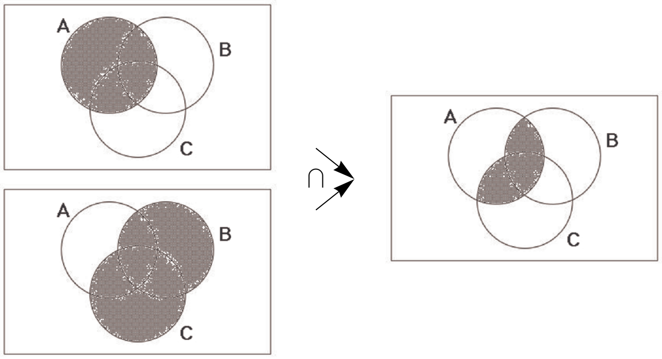


Figure 4.1.1 Left side of distributive law developed

The advantage of this method is that it is relatively quick and mechanical. The disadvantage is that it is workable only if there are a small number of sets under consideration. In addition, it doesn't work very well in a static environment like a book or test paper. Venn diagrams tend to work well if you have a potentially dynamic environment like a blackboard or video.

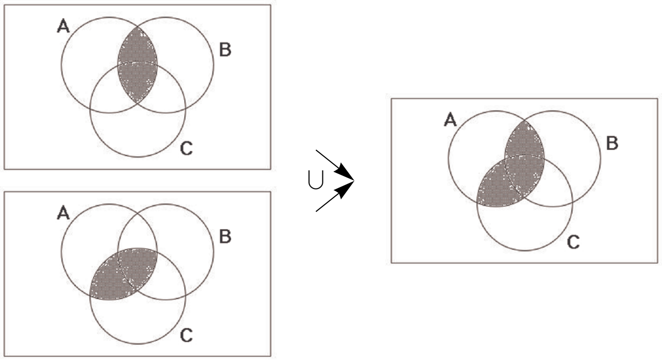


Figure 4.1.2 Right side of distributive law developed

PROOF USING SET-MEMBERSHIP TABLES

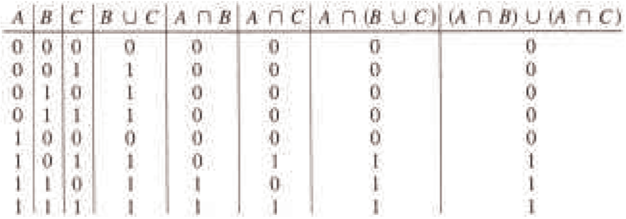
Let A be a subset of a universal set U and let $u \in U$. To use this method we note that exactly one of the following is true: $u \in A$ or $u \notin A$. Denote the situation where $u \in A$ by 1 and that where $u \notin A$ by 0. Working with two sets, A and B, and if $u \in U$, there are four possible outcomes of "where u can be." What are they? The set-membership table for $A \cup B$ is :

A	B	A⋃B
0	0	0
0	1	1
1	0	1
1	1	1

This table illustrates that $u \in A \cup B$ if and only if $a \in A$ or $u \in B$.

In order to prove the distributive law via a set-membership table, write out the table for each side of the set statement to be proved and note that if S and T are two columns in a table, then the set statement S is equal to the set statement T if and only if corresponding entries in each row are the same.

To prove $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, first note that the statement involves three sets, A, B, and C, So there are $2^3 = 8$ possibilities for the membership of an element in the sets.



A	B	C	$B \cup C$	$A \cap B$	$A \cap C$	$A \cap (B \cup C)$	$(A \cap B) \cup (A \cap C)$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	0	1	1	1
1	1	0	1	1	0	1	1
1	1	1	1	1	1	1	1

Since each entry in Column 7 is the same as the corresponding entry in Column 8, we have shown that $A \cup (B \cup C) = (A \cap B) \cup (A \cap C)$ for any sets A, B, and C. The main advantage of this method is that it is mechanical. The main disadvantage is that it is reasonable to use only for a relatively small number of sets. If we are trying to prove a statement involving five sets, there are $2^5 = 32$ rows, which would test anyone's patience doing the work by hand.

PROOF USING DEFINITIONS

This method involves using definitions and basic concepts to prove the given statement. This procedure forces one to learn, relearn, and understand basic definitions and concepts. It helps individuals to focus their attention on the main ideas of each topic and therefore is the most useful method of proof. One does not learn a topic by memorizing or occasionally glancing at core topics, but by using them in a variety of contexts. The word proof panics most people; however, everyone can become comfortable with proofs. Do not expect to prove every statement immediately. In fact, it is not our purpose to prove every theorem or fact encountered, only those that illustrate methods and/or basic concepts. Throughout the text we will focus in on main techniques of proofs. Let's illustrate by proving the distributive law.

Proof Technique 1. *State or restate the theorem so you understand what is given (the hypothesis) and what you are trying to prove (the conclusion).*

Theorem 4.1.1. *If A, B, and C are sets, then* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Assume: A, B, and C are sets.

Prove: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Commentary: What am I trying to prove? What types of objects am I working with: sets? real numbers? propositions? The answer is sets: sets of elements that can be anything you care to imagine. The universe from which we draw our elements plays no part in the proof of this theorem.

We need to show that the two sets are equal. Let's call them the left-hand set ($L.H.S.$) and the right-hand set ($R.H.S.$) To prove that $L.H.S. = R.H.S.$, we must prove two things: (a) $L.H.S. \subseteq R.H.S.$ and (b) $R.H.S. \subseteq L.H.S.$

To prove part a and, similarly, part b, we must show that each element of L.H.S. is an element of R.H.S. Once we have diagnosed the problem we are ready to begin.

Proof of Theorem 4.1.1: We must prove:

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

Let $x \in A \cap (B \cup C)$ to show $x \in (A \cap B) \cup (A \cap C)$.

$x \in A \cap (B \cup C)$

Definition of $\cup$, $\cap$	$\Rightarrow x \in A$ and ($x \in B$ or $x \in C$)
Distributive Law of Logic	$\Rightarrow$ ($x \in A$ and $x \in B$) or ($x \in A$ and $x \in C$)
Definition of $\cap$	$\Rightarrow$ ($x \in A \cap B$) or($x \in A \cap C$)
Definition of $\cup$	$\Rightarrow x \in (A \cap B) \cup (A \cap C)$

and (b) $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$

$x \in (A \cap B) \cup (A \cap C)$

Why?	$\Rightarrow$ ($x \in A \cap B$) or ($x \in A \cap C$)
Why?	$\Rightarrow$ ($x \in A$ and $x \in B$) or ($x \in A$ and $x \in C$)
Why?	$\Rightarrow x \in A$ and ($x \in B$ or $x \in C$)
Why?	$\Rightarrow x \in A \cap (B \cup C)$ ■

Proof Technique 2.

(1) To prove that $A \subseteq B$, *we must show that if* $x \in A$, *then* $x \in B$.

(2) To prove that $A = B$, *we must show:*
(a) $A \subseteq B$, *and*
(b) $B \subseteq A$.

To further illustrate the Proof-by-Definition technique, let's prove the following:

Theorem 4.1.2. Let A, B, and C be sets, then
$A \times (B \bigcap C) = (A \times B) \bigcap (A \times C)$.

Commentary; We again ask ourselves: What are we trying to prove? What types of objects are we dealing with? We realize that we wish to prove two facts: (a) $L.H.S. \subseteq R.H.S.$ and (b) $R.H.S. \subseteq L.H.S.$

To prove part a, and similarly part b, we'll begin the same way. Let

___ $\in L.H.S.$ to show ___ $\in R.H.S.$ What should ___ be?

What does a typical object in the $L.H.S.$ look like?

Proof of Theorem 4.1.2: We must prove:

(a) $A\times(B \bigcap C) \subseteq (A\times B) \bigcap (A\times C)$.

Let $(x, y) \in A\times(B \bigcap C)$ to prove $(x, y) \in (A\times B) \bigcap (A\times C)$.

$(x, y) \in A\times(B \bigcap C)$.
Why? $\Rightarrow$ $x \in A$ and $y \in (B \bigcap C)$.
Why? $\Rightarrow$ $x \in A$ and $(y \in B$ and $y \in C)$.
Why? $\Rightarrow$ $(x \in A$ and $y \in B)$ and $(x \in A$ and $y \in C)$.
Why? $\Rightarrow$ $(x, y) \in (A\times B)$ and $(x, y) \in (A\times C)$.
Why? $\Rightarrow$ $(x, y) \in (A\times B) \bigcap (A\times C)$.

and (b) $(A\times B) \bigcap (A\times C) \subseteq A\times(B \bigcap C)$.

Let $(x, y) \in (A\times B) \bigcap (A\times C)$ to prove $(x, y) \in A \bigcap (B\times C)$.

$(x, y) \in (A\times B) \bigcap (A\times C)$.
Why? $\Rightarrow$ $(x, y) \in A\times B$ and $(x, y) \in A\times C$.
Why? $\Rightarrow$ $(x \in A$ and $y \in B)$ and $(x \in A$ and $y \in C)$.
Why? $\Rightarrow$ $x \in A$ and $(y \in B$ and $y \in C)$.
Why? $\Rightarrow$ $x \in A$ and $y \in (B \bigcap C)$.
Why? $\Rightarrow$ $(x, y) \in A\times(B \bigcap C)$ ■

EXERCISES FOR SECTION 4.1

A Exercises

1. Prove the following:

(a) Let A, B, and C be sets. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

(b) Let A and B be sets. Then $A - B = A \bigcap B^c$.

(c) Let A, B, and C be sets. If $(A \subseteq B$ and $A \subseteq C)$ then $A \subseteq B \bigcap C$.

(d) Let A and B be sets. $A \subseteq B$ If and only if $B^c \subseteq A^c$.

(e) Let A, B, and C be sets. If $A \subseteq B$ then $A\times C \subseteq B\times C$.

2. Write the converse of parts (a), (c), and (e) of Exercise 1 and prove or disprove them.

3. Disprove the following, assuming A, B, and C are sets;

(a) $A - B = B - A$.

(b) $A\times B = B\times A$.

(c) A $\bigcap$ B = A $\bigcap$ C implies $B = C$.

4. Let A, B, and C be sets. Write the following in "if . . . then . . ." language and prove:

(a) $x \in B$ is a sufficient condition for $x \in A \bigcup B$.

(b) $A \bigcap B \bigcap C = \emptyset$ is a necessary condition for $A \bigcap B = \emptyset$.

(c) $A \bigcup B = B$ is a necessary and sufficient condition for $A \subseteq B$.

B Exercises

5. Prove by induction that if $A, B_1\ B_2, \ldots, B_n$, are sets, $n \geq 2$, then

$$A \bigcap (B_1 \bigcup B_2 \bigcup \cdots \bigcup B_n) = (A \bigcap B_1) \bigcup (A \bigcap B_2) \bigcup \cdots \bigcup (A \bigcap B_n)$$

4.2 Laws of Set Theory

The following basic set laws can be derived using either the Basic Definition or the Set-Membership approach and can be illustrated by Venn diagrams.

Commutative Laws

(1) $A \bigcup B = B \bigcup A$ (1') $A \bigcap B = B \bigcap A$

Associative Laws

(2) $A \bigcup (B \bigcup C) = (A \bigcup B) \bigcup C$ (2') $\mathrm{A} \bigcap (\mathrm{B} \bigcap \mathrm{C}) = (\mathrm{A} \bigcap \mathrm{B}) \bigcap \mathrm{C}$

Distributive Laws

(3) $A \bigcap (B \bigcup C) = (A \bigcap B) \bigcup (A \bigcap C)$ (3') $\mathrm{A} \bigcup (\mathrm{B} \bigcap \mathrm{C}) = (\mathrm{A} \bigcup \mathrm{B}) \bigcap (\mathrm{A} \bigcup \mathrm{C})$

Identity Laws

(4) $A \bigcup \emptyset = \emptyset \bigcup A = A.$ (4') $A \bigcap U = U \bigcap A = A$

Complement Laws

(5) $A \bigcup A^c = U$ (5') $A \bigcap A^c = \emptyset$

Idem potent Laws

(6) $A \bigcup A = A$ (6') $A \bigcap A = A$

Null Laws

(7) $A \bigcup U = U$ (7') $A \bigcap \emptyset = \emptyset$

Absorption Laws

(8) $A \bigcup (A \bigcap B) = A.$ (8') $A \bigcap (A \bigcup B) = A.$

DeMorgan's Laws

(9) $(A \bigcup B)^c = A^c \bigcap B^c$. (9') $(A \bigcap B)^c = A^c \bigcup B^c$

Involution Law

(10) $(A^c)^c = A.$

It is quite clear that most of these laws resemble or, in fact, are analogues of laws in basic algebra and the algebra of propositions.

PROOF USING PREVIOUSLY PROVEN THEOREMS

Once a few basic laws or theorems have been established, we frequently use them to prove additional theorems. This method of proof is sometimes more efficient than that of Proof by Definition. To illustrate, let us prove the following:

Theorem 4.2.1. *Let A and B be sets. Then* $(A \bigcap B) \bigcup (A \bigcap B^c) = A.$

Proof : $(A \bigcap B) \bigcup (A \bigcap B^c) = A \bigcap (B \bigcup B^c)$ Why?
$= A \bigcap U$ Why?
$= A$ Why? ■

PROOF USING THE INDIRECT METHOD/ CONTRADICTION

The procedure one most frequently uses to prove a theorem in mathematics is the Direct Method, as illustrated in Theorems 4.1.1 and 4.1.2. Occasionally there are situations where this method is not applicable. Consider the following:

Theorem 4.2.2. *Let* A, B, C *be sets. If* $A \subseteq B$ *and* $B \bigcap C = \emptyset$*, then* $A \bigcap C = \emptyset$.

Commentary: The usual and first approach would be to assume $A \subseteq B$ and $B \bigcap C = \emptyset$ is true and to attempt to prove $A \bigcap C = \emptyset$ is true. To do this you would need to show that nothing is contained in the set $A \bigcap C$. Think about how you would show that something doesn't exist. It is very difficult to do directly.

The Indirect Method is much easier: If we assume the conclusion is false and we obtain a contradiction—then the theorem must be true. This approach is on sound logical footing since it is exactly the same method of indirect proof that we discussed in Section 3.5.

Proof of Theorem 4.2.2; Assume $A \subseteq B$ and $B \cap C = \emptyset$, and $A \cap C \neq \emptyset$. To prove that this cannot occur, let $x \in A \cap C$.

Why? $\Rightarrow$ $x \in A$ and $x \in C$,

Why? $\Rightarrow$ $x \in B$ and $x \in C$.

Why? $\Rightarrow$ $x \in B \cap C$.

But this contradicts the second premise. Hence, the theorem is proven. ■

EXERCISES FOR SECTION 4.2

In the exercises that follow it is most important that you outline the logical procedures or methods you use.

A Exercises

1. (a) Prove the associative law for intersection (Law 2') with a Venn diagram.

   (b) Prove DeMorgan's Law (Law 9) with a membership table.

   (c) Prove the Idempotent Law (Law 6) using basic definitions.

2. (a) Prove the Absorption Law (Law 8') with a Venn diagram.

   (b) Prove the Identity Law (Law 4) with a membership table.

   (c) Prove the Involution Law (Law 10) using basic definitions.

3. Prove, using the set theory laws, as well as any other theorems proved so far;

   (a) $A \cup (B - A) = A \cup B$

   (b) $A - B = B^c - A^c$.

   (c) $A \subseteq B,\ A \cap C \neq \emptyset \Rightarrow B \cap C \neq \emptyset$

   (d) $A \cap (B - C) = (A \cap B) - (A \cap C)$.

   (e) $A - (B \cup C) = (A - B) \cap (A - C)$

4. Use previously proven theorems to prove:

   (a) $A \cap (B \cap C)^c = (A \cap B^c) \cup (A \cap C^c)$

   (b) $A \cap (B \cap (A \cap B)^c) = \emptyset$

   (c) $(A \cap B) \cup B^c = A \cup B^c$

   (d) $A \cup (B - C) = (A \cup B) - (C - A)$.

5. Hierarchy of Set Operations. The rules that determine the order of evaluation in a set expression that involves more than one operation are similar to the rules for logic. In the absence of parentheses, complementations are done first, intersections second, and unions third. Parentheses are used to override this order. If the same operation appears two or more consecutive times, evaluate from left to right. In what order are the following expressions performed?

(a) $A \cup B^c \cap C$.

(b) $A \cap B \cup C \cap B$.

(c) $A \cup B \cup C^c$.

C Exercise

6. There are several ways that can be used to format the proofs in this chapter. One that should be familiar to you from Chapter 3 is illustrated with the following proof. Alternate proof of part (a) in Theorem 4.1.1:

(1)	$x \in A \cap (B \cup C)$	Premise
(2)	$(x \in A) \wedge (x \in B \cup C)$	(1), definition of intersection
(3)	$(x \in A) \wedge ((x \in B) \vee (x \in C))$	(2), definition of union

(4) $(x \in A) \bigwedge (x \in B) \bigvee (x \in A) \bigwedge (x \in C)$ (3), distribute $\wedge$ over $\vee$

(5) $(x \in A \bigcap B)\, V\, (x \in A \bigcap C)$ (4), definition of intersection

(6) $x \in (A \bigcap B) \bigcup (A \bigcap C)$ (5), definition of union

4.3 Minsets

Let B_1 and B_2 be subsets of a set A. Notice that the Venn diagram of Figure 4.3.1 is naturally partitioned into the subsets A_1, A_2, A_3, and A_4. Further we observe that A_1, A_2, A_3, and A_4 can be described in terms of B_1 and B_2 as follows:

$A_1 = B_1 \bigcup B_2{}^c$

$A_2 = B_1 \bigcap B_2$

$A_3 = B_1{}^c \bigcap B_2$

$A_4 = B_1{}^c \bigcap B_2{}^c$

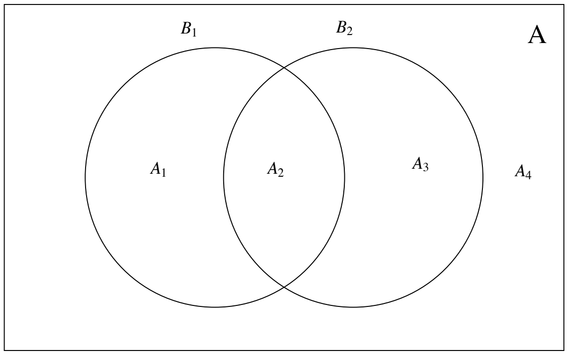


Figure 4.3.1

Each A_i is called a minset generated by B_1 and B_2 . We note that each minset is formed by taking the intersection of two sets where each may be either B_k or its complement $B_k{}^c$ Note also, given two sets, there are $2^2 = 4$ minsets.

Minsets are occasionally called *minterms*.

The reader should note that if we apply all possible combinations of the operations intersection, union, and complementation to the sets B_1 and B_2 of Figure 4.3.1, the smallest sets generated will be exactly the minsets, the minimum sets. Hence the derivation of the term minset.

Next consider the Venn diagram containing three sets, B_1, B_2, and B_3. What are the minsets generated by B_1, B_2, and B_3? How many are there? Following the procedures outlined above, we note that

$B_1 \bigcap B_2 \bigcap B_3^c$

$B_1 \bigcap B_2^c \bigcap B_3$

$B_1 \bigcap B_2^c \bigcap B_3^c$

are three of the $2^3 = 8$ minsets. See Exercise 1 of this section.

Definition: Minset. *Let $\{B_1, B_2, \ldots ,B_n\}$ be a set of subsets of a set A. Sets of the form $D_1 \bigcap D_2 \bigcap \cdots \bigcap D_n$, where each D_i, may be either B_i or B_i^c is called a minset generated by $B_1, B_2, \ldots ,B_n$.*

Example 4.3.1. For another view, consider the following: Let $A = \{1, 2, 3, 4, 5, 6\}$ with subsets $B_1 = \{1, 3, 5\}$ and $B_2 = \{1, 2, 3\}$. How can we, using set operations applied to B_1 and B_2 , produce a list of sets that contain elements of A efficiently without duplication? As a first attempt, we note that:

$B_1 \bigcap B_2 = \{1, 3\}$,

$B_1^c = \{2, 4, 6\}$, and

$B_2^c = \{4, 5, 6\}$.

We have produced all elements of A but we have 4 and 6 repeated in two sets. In place of B_1^c and B_2^c , let us try $B_1^c \bigcap B_2$ and $B_1 \bigcap B_2^c$, respectively:

$B_1^c \bigcap B_2 = \{2\}$ and

$B_1 \bigcap B_2^c = \{5\}$.

We have now produced the elements 1, 2, 3, and 5 using $B_1 \bigcap B_2$, $B_1^c \bigcap B_2$ and $B_1 \bigcap B_2^c$ yet we have not listed the elements 4 and 6. Most ways that we could combine B_1 and B_2 such as $B_1 \bigcup B_2$ or $B_1 \bigcup B_2^c$ will produce duplications of listed elements and will not produce both 4 and 6. However we note that $B_1^c \bigcap B_2^c = \{4, 6\}$, exactly the elements we need. Each element of A appears exactly once in one of the four minsets $B_1 \bigcap B_2$, $B_1^c \bigcap B_2$, $B_1 \bigcap B_2^c$ and $B_1^c \bigcap B_2^c$. Hence, we have a partition of A.

Theorem 4.3.1. *Let A be a set and let $B_1, B_2 \ldots , B_n$ be subsets of A. The set of nonempty minsets generated by $B_1, B_2 \ldots , B_n$ is a partition of A.*

The proof of this theorem is left to the reader. The most significant fact about minsets is that any subset of A that can be obtained from B_1, B_2 … , B_n, using the standard set operations can be obtained in a standard form by taking the union of selected minsets.

Definition: Minset Normal Form. *A set is said to be in minset normal form when it is expressed as the union of zero or more distinct nonempty minsets.*

Notes:

(a) The union of zero sets is the empty set, $\emptyset$.

(b) Minset normal form is also called *canonical form*.

Example 4.3.2. Let $U = \{-2, -1, 0, 1, 2\}$, $B_1 = \{0, 1, 2\}$, and $B_2 = \{0, 2\}$. Then

$$B_1 \cap B_2 = \{0, 2\}$$

$$B_1^c \cap B_2 = \emptyset$$

$$B_1 \cap B_2^c = \{1\}$$

$$B_1^c \cap B_2^c = \{-2, -1\}$$

In this case, there are only three nonempty minsets, producing the partition $\{\{0, 2\}, \{1\}, \{-2, -1\}\}$. An example of a set that could not be produced from just B_1 and B_2 is the set of even elements of U, $\{-2, 0, 2\}$. This is because -2 and -1 cannot be separated — they are in the same minset and any union of minsets needs either include or exclude them both. In general, there are $2^3 = 8$ different minset normal forms because there are three nonempty minsets. This means that only 8 of the $2^5 = 32$ subsets of U can be generated from B_1 and B_2.

EXERCISES FOR SECTION 4.3

A Exercises

1. Consider the subsets $A = \{1, 7, 8\}$, $B = \{1, 6, 9, 10\}$, and $C = \{1, 9, 10\}$, where $U = \{1, 2, \ldots, 10\}$.

(a) List the nonempty minsets generated by A, B, and C.

(b) How many elements of the power set of U can be generated by A, B, and C? Compare this number with $| \mathcal{P}(U) |$. Give an example of one subset that cannot be generated by A, B, and C.

2. (a) Partition $\{1, 2, ... 9\}$ into the minsets generated by $B_1 = \{5, 6, 7\}$, $B_2 = \{2, 4, 5, 9\}$, and $B_3 = \{3, 4, 5, 6, 8, 9\}$.

(b) How many different subsets of $\{1, 2, \ldots, 9\}$ can you create using B_1, B_2, and B_3 with the standard set operations?

(c) Do there exist subsets C_1, C_2, C_3 whose minsets will generate every subset of $\{1, 2, \ldots, 9\}$?

3. Partition the set of strings of 0's and 1's of length two or less, using the minsets generated by $B_1 = \{s \mid s \text{ has length } 2\}$, and $B_2 = \{s \mid s \text{ starts with a } 0\}$.

4. Let B_1, B_2, and B_3 be subsets of a universal set U,

(a) Find all minsets generated by B_1, B_2, and B_3.

(b) Illustrate with a Venn diagram all minsets obtained in part (a).

(c) Express the following sets in minset normal form: B_1^c, $B_1 \cap B_2$, $B_1 \cup B_2^c$.

5. (a) Partition $A = \{0, 1, 2, 3, 4, 5\}$ with the minsets generated by $B_1 = \{0, 2, 4\}$ and $B_2 = \{1, 5\}$.

(b) How many different subsets of A can you generate from B_1 and B_2?

B Exercises

6. If $\{B_1, B_2, \ldots, B_n\}$ is a partition of A, how many minsets are generated by $B_1, B_2, \ldots, B_n$?

7. Prove Theorem 4.3.1.

C Exercise

8. Let S be a finite set of n elements. Let B_i ,, i = 1, 2, … , k be nonempty subsets of S. There are 2^{2^k} minset normal forms generated by the k subsets. The number of subsets of S is 2^n. Since we can make $2^{2^k} > 2^n$ by choosing $k \geq \log_2 n$, it is clear that two distinct minset normal-form expressions do not always equal distinct subsets of S. Even for $k < \log_2 n$, it may happen that two distinct minset normal-form expressions equal the same subset of S. Determine necessary and sufficient conditions for distinct normal-form expressions to equal distinct subsets of S.

4.4 The Duality Principle

In Section 4.2 we observed that each of the set laws labeled 1 through 9 had an analogue 1' through 9'. We notice that each of the laws in one column 2 can be obtained from the corresponding law in the other column by replacing $\bigcup$ by $\bigcap$, ($\bigcap$ by $\bigcup$, $\emptyset$ by U, U by $\emptyset$, and leaving the complement unchanged.

Definition: Duality Principle for Sets. *Let S be any identity involving sets and the operations complement, intersection and union, . If S* is obtained from S by making the substitutions $\bigcup \to \bigcap$, $\bigcap \to \bigcup$, $\emptyset \to U$, and $U \to \emptyset$, then the Statement S* is also true and it is called the dual of the Statement S.*

Example 4.4.1. The dual of $(A \bigcap B) \bigcup (A \bigcap B^c) = A$ is $(A \bigcup B) \bigcap (A \bigcup B^c) = A$

One should not underestimate the importance of this concept. It gives us a whole second set of identities, theorems, and concepts. For example, we can consider the dual of *minsets* and *minset normal form* to obtain what is called *maxsets* and *maxset normal form*.

EXERCISES FOR SECTION 4.4

A Exercises

1. State the dual of:

(a) $A \bigcup (B \bigcap A) = A$.

(b) $A \bigcup ((B^c \bigcup A) \bigcap B)^c = U$,

(c) $(A \bigcup B^c)^c \bigcap B = A^c \bigcap B$

2. Consider Table 3.4.1 and then write a description of the principle of duality for logic.

3. Write the dual of:

(a) $p \bigvee \neg ((\neg q \bigvee p) \bigwedge q) \Leftrightarrow 1$

(b) $(\neg (p \bigwedge (\neg q)) \bigvee q \Leftrightarrow (\neg p \bigvee q)$.

B Exercises

4. Use the principle of duality and the definition of minset to write the definition of maxset. {Hint, just replace$\bigcap$by $\bigcup$.)

5. Let $A = \{1, 2, 3, 4, 5, 6\}$ and let $B_1 = \{1, 3, 5\}$ and $B_2 = \{1, 2, 3\}$. Find the maxsets generated by B_1 and B_2. Note the set of maxsets does not constitute a partition of A. Can you explain why?

(a) Write out the definition of maxset normal form.

(b) Repeat Problem 4 of Section 4.3 for maxsets.

6. Is the dual of Exercise 5 of Section 4.1 true?

SUPPLEMENTARY EXERCISES FOR CHAPTER 4

Section 4.1

1. Let A and B be subsets of a universal set U. Use basic definitions to prove each statement. Be sure to outline carefully the logical structure of the proof.

(a) $A \subseteq S$ if and only if $A \cap (U - B) = \emptyset$.

(b) If $U = A \cup B$ and $A \cap B = \emptyset$, then $A = U - B$.

(c) A and B are disjoint if and only if $A \subseteq U — B$.

2. Let A and B be subsets of a universal set U. Verify the statements using a Venn diagram.

(a) $A \subseteq B$ if and only if $A \cap B = A$.

(b) $A \subseteq B$ if and only if $A \cup B = B$.

(c) $A \cap B \subseteq A \cup B$.

3. (a) Prove that if A, B, and C are sets, then $(A \cup B) \times C$ is a subset

of $(A \times C) \cup (B \times C)$.

(b) Explain how you would proceed following part a if you wanted to prove that $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

4. Simplify the following:

(a) $(A \cap B^c \cap C) \cup B \cup (B \cap C) \cup (A^c \cap C)$.

(b) $(A \cup (B \cap C^c)) \cap ((A^c \cap B^c) \cup C)$.

Section 4.2

5. Prove with an *indirect proof* that if A, B, and C are subsets of universe U, A is a subset of B, and B is a subset of C, then C^c is a subset of A^c.

6. Basic laws and theorems in different algebraic structures can be recalled easily by thinking in terms of analogous situations in elementary algebra.

(a) Complete the following table:

	Algebra of Sets	Algebra of Logic	Elementary Algebra
Objects Used	Sets		Real Numbers
Basic Operations	$\cup$	$\wedge$	$\cdot$
		$\neg$	$+$
			$-$ (or multiplicative inverse
Other Connectives	$\subseteq$	$\Leftrightarrow$	$\leqslant$
			$=$

(b) Write analogous statements in the algebras of sets and logic.

Which are true?

(i) If x, y, and z are real numbers and if $x \leq y$ and $y \leqslant z$, then $x \leqslant z$.

(ii) $-(-x) = x$ for any real number x.

(iii) If x, y, and z are real numbers and $x + y = x + z$, then $y = z$.

(iv) Let $x,\ y \in \mathbb{R}. x = y$ if and only if $x \leqslant y$ and $y \leqslant x$.

(v) For $x \in \mathbb{R}$, $x + 0 = 0 + x = x$ and $x \cdot 1 = 1 \cdot x = x$.

7. Prove or disprove:

(a) Let A, B, and C be sets. If $A \cup C \neq B \cup C$, then $A \neq B$.

(b) If $A \neq B$, then $A^c \neq B^c$.

8. Let $\{A_1, A_2, \ldots \mathrm{A}_n\}$ be a partition of set A, and let B be any nonempty subset of A, Prove that $\{A_i \cap B \mid A_i \cap B \neq \emptyset\}$ is a partition of $A \cap B$.

Section 4.3

9. Let $U = \{1, 2, 3, 4, 5, 6\}, B_1 = \{1, 3\}$, and $B_2 = \{2, 3, 5\}$.

(a) List the minsets generated by B_1 and B_2.

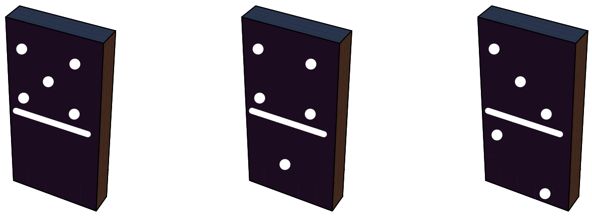
(b) Show that the set of minsets form a partition of U.

Section 4.4

10. State the dual of each statement in Exercise 3, Section 4.2.

11. Show that the dual of each of the basic set laws 1 through 9 are the corresponding laws 1' through 9'.

chapter 5



INTRODUCTION TO MATRIX ALGEBRA

GOALS

The purpose of this chapter is to introduce you to matrix algebra, which has many applications. You are already familiar with several algebras: elementary algebra, the algebra of logic, the algebra of sets. We hope that as you studied the algebra of logic and the algebra of sets, you compared them with elementary algebra and noted that the basic laws of each are similar. We will see that matrix algebra is also similar. As in previous discussions, we begin by defining the objects in question and the basic operations.

5.1 Basic Definitions

Definition: Matrix. *A matrix is a rectangular array of elements of the form*

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{pmatrix}$$

A convenient way of describing a matrix in general is to designate each entry via its position in the array. That is, the entry a_{34} is the entry in the third row and fourth column of the matrix A. Depending on the situation, we will decide in advance to which set the entries in a matrix will belong. For example, we might assume that each entry a_{ij} $(1 \leq i \leq m, 1 \leq j \leq n)$ is a real number. In that case we would use $M_{m\times n}(\mathbb{R})$ to stand for the set of all m by n matrices whose entries are real numbers. If we decide that the entries in a matrix must come from a set S, we use $M_{m\times n}(S)$ to denote all such matrices.

Definition: Order of a Matrix. *The matrix A that has m rows and n columns is called an $m \times n$ (read "m by n") matrix, and is said to have order $m \times n$.*

Since it is rather cumbersome to write out the large rectangular array above each time we wish to discuss the generalized form of a matrix, it is common practice to replace the above by $A = [a_{\text{ij}}]$. In general, matrices are often given names that are capital letters and the corresponding lower case letter is used for individual entries. For example the entry in the third row, second column of a matrix called C would be c_{32}.

Example 5.1.1.

$$A = \begin{pmatrix} 2 & 3 \\ 0 & -5 \end{pmatrix}, B = \begin{pmatrix} 0 \\ \frac{1}{2} \\ 15 \end{pmatrix}, \text{and } D = \begin{pmatrix} 1 & 2 & 5 \\ 6 & -2 & 3 \\ 4 & 2 & 8 \end{pmatrix}$$

are 2×2, 3×1, and 3×3 matrices, respectively

Since we now understand what a matrix looks like, we are in a position to investigate the operations of matrix algebra for which users have found the most applications.

Example 5.1.2. First we ask ourselves: Is the matrix $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ equal to the matrix $B = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$? No, they are not because the corresponding entries in the second row, second column of the two matrices are not equal. Next, is $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ equal to $B = \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix}$? No, although the corresponding entries in the first two columns are identical, B doesn't have a third column to compart to that of A. We formalize these observations in the following definition.

Definition; Equality of Matrices. *A matrix A is said to be equal to matrix B (written $A = B$) if and only if:*

(1) A and B have the same order, and

(2) all corresponding entries are equal: that is, $a_{ij} = b_{ij}$ for all appropriate i and j.

5.2 Addition and Scalar Multiplication

Example 5.2.1. Concerning addition, it seems natural that if

$A = \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}$ and $B = \begin{pmatrix} 3 & 4 \\ -5 & 2 \end{pmatrix}$, then $A + B = \begin{pmatrix} 1+3 & 0+4 \\ 2-5 & -1+2 \end{pmatrix} = \begin{pmatrix} 4 & 4 \\ -3 & 1 \end{pmatrix}$.

However, if $A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \end{pmatrix}$ and $B = \begin{pmatrix} 3 & 0 \\ 2 & 8 \end{pmatrix}$, can we find $A + B$? No, the orders of the two matrices must be identical.

Definition: Matrix Addition. *Let A and B be $m \times n$ matrices. Then $A + B$ is an $m \times n$ matrix where $(A + B)_{ij} = a_{ij} + b_{ij}$ (read "the ith jth entry of the matrix $A + B$ is obtained by adding the ith jth entry of A to the ith jth entry of B"). If the orders of A and B are not identical, $A + B$ is not defined.*

It should be clear from Example 5.2.1 and the definition of addition that $A + B$ is defined if and only if A and B are of the same order.

Another frequently used operation is that of multiplying a matrix by a number, commonly called a scalar in this context. Scalars normally come from the same set as the entries in a matrix. For example, if $A \in M_{m\times n}(\mathbb{R})$, a scalar can be any real number.

Example 5.2.2. If $c = 3$ and if $A = \begin{pmatrix} 1 & -2 \\ 3 & 5 \end{pmatrix}$ and we wish to find $c A$, it seems natural to multiply each entry of A by 3 so that $3 A = \begin{pmatrix} 3 & -6 \\ 9 & 15 \end{pmatrix}$, and this is precisely the way scalar multiplication is defined.

Definition: Scalar Multiplication. *Let A be an $m \times n$ matrix and c a scalar. Then c A is the $m \times n$ matrix obtained by multiplying c times each entry of A; that is $(cA)_{ij} = c\, a_{ij}$.*

5.3 Multiplication of Matrices

- For a video introduction to this section, go to http://faculty.uml.edu/klevasseur/ads2/videos/matrixmultiplication/

A definition that is more awkward to motivate (and we will not attempt to do so here) is the product of two matrices. In time, the reader will see that the following definition of the product of matrices will be very useful, and will provide an algebraic system that is quite similar to elementary algebra.

Definition: Matrix Multiplication. *Let A be an $m \times n$ matrix and let B be an $n \times p$ matrix. The product of A and B, denoted by AB, is an $m \times p$ matrix whose ith row jth column entry is*

$$\begin{aligned}(A\,B)_{i\,j} &= a_{i\,1}\, b_{1\,j} + a_{i\,2}\, b_{2\,j} + \cdots + a_{i\,n}\, b_{n\,j} \\ &= \sum_{k=1}^{n} a_{i\,k}\, b_{k\,j}\end{aligned}$$

for $1 \le i \le m$ and $1 \le j \le p$.

The mechanics of computing one entry in the product of two matrices is illustrated in Figure 5.3.1.

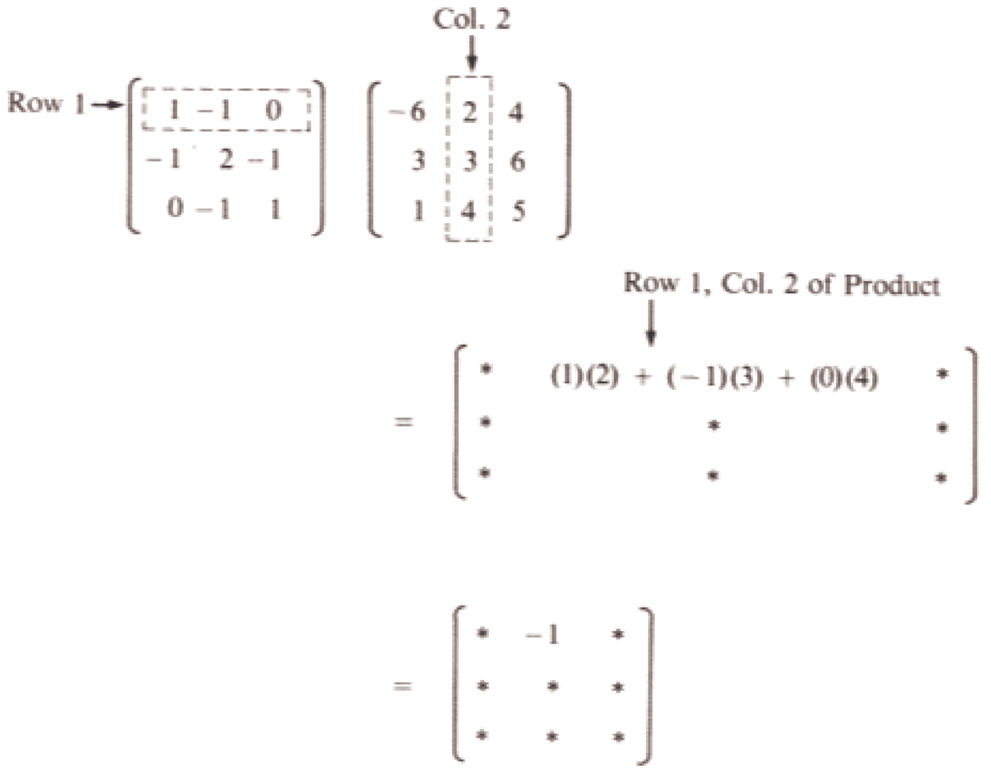


Figure 5.3.1 Computation of one entry in the product of two 3 by 3 matrices

The computation of a product can take a considerable amount of time in comparison to the time required to add two matrices. Suppose that A and B are $n\times n$ matrices; then $(\mathrm{AB})_{ij}$ is determined performing n multiplications and $n-1$ additions. The full product takes n^3 multiplications and $n^3 — n^2$ additions. This compares with n^2 additions for the sum of two $n\times n$ matrices. The product of two 10 by 10 matrices will require 1,000 multiplications and 900 additions, clearly a job that you would assign to a computer. The sum of two matrices requires a more modest 100 additions. This analysis is based on the assumption that matrix multiplication will be done using the formula that is given in the definition. There are more advanced methods that, in theory, reduce operation counts. For example, Strassen's algorithm (http://mathworld.wolfram.com/StrassenFormulas.html) computes the product of two n by n matrices in $7\cdot 7^{\log_2 n} - 6\cdot 4^{\log_2 n} \approx 7\,n^{2.808}$ operations. There are practical issues involved in actually using the algorithm in many situations. For example, round-off error can be more of a problem than with the standard formula.

Example 5.3.1. Let $A = \begin{pmatrix} 1 & 0 \\ 3 & 2 \\ -5 & 1 \end{pmatrix}$, a 3×2 matrix, an let $B = \begin{pmatrix} 6 \\ 1 \end{pmatrix}$, a 2×1 matrix. Then $A\,B$ is a 3×1 matrix:

$$A\,B = \begin{pmatrix} 1 & 0 \\ 3 & 2 \\ -5 & 1 \end{pmatrix}\begin{pmatrix} 6 \\ 1 \end{pmatrix} = \begin{pmatrix} 1\cdot 6 + 0\cdot 1 \\ 2\cdot 1 + 3\cdot 6 \\ -5\cdot 6\, +\, 1\cdot 1 \end{pmatrix} = \begin{pmatrix} 6 \\ 20 \\ -29 \end{pmatrix}$$

Remarks:

(1) The product $A\,B$ is defined only if A is an $m\times n$ matrix and B is an $n\times p$ matrix; that is, the two "inner" numbers must be the equal. Furthermore, the order of the product matrix $A\,B$ is the "outer" numbers, in this case $m\times p$.

(2) It is wise to first determine the order of a product matrix. For example, if A is a 3×2 matrix and B is a 2×2 matrix, then $A\,B$ is a 3×2 matrix of the form

$$A\,B = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \\ c_{31} & c_{32} \end{pmatrix}$$

Then to obtain, for example, C_{31}, we multiply corresponding entries in the third row of A times the first column of B and add the results.

Example 5.3.2.

Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$, and $B = \begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix}$. Then

$$A\,B = \begin{pmatrix} 1\cdot 3 + 0\cdot 2 & 1\cdot 0 + 0\cdot 1 \\ 0\cdot 3 + 3\cdot 2 & 0\cdot 0 + 3\cdot 1 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 6 & 3 \end{pmatrix}$$

Note: $B\,A = \begin{pmatrix} 3 & 0 \\ 2 & 3 \end{pmatrix} \neq A\,B$

Remarks;

(1) An $n \times n$ matrix is called a *square matrix*.

(2) If A is a square matrix, $A\,A$ is defined and is denoted by A^2 , and $A\,A\,A = A^3$, etc.

(3) The $m \times n$ matrices whose entries are all 0 are denoted by $\mathbf{0}_{m\times n}$, or simply $\mathbf{0}$, when no confusion arises regarding the order.

EXERCISES FOR SECTIONS 5.1 THROUGH 5.3

A Exercises

1. Let $A = \begin{pmatrix} 1 & -1 \\ 2 & 3 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ 3 & -5 \end{pmatrix}$, and $C = \begin{pmatrix} 0 & 1 & -1 \\ 3 & -2 & 2 \end{pmatrix}$

(a) Compute $A\,B$ and $B\,A$.

(b) Compute $A + B$ and $B + A$.

(c) If $c = 3$, show that $c(A + B) = c\,A + c\,B$.

(d) Show that $(A\,B)\,C = A\,(B\,C)$.

(e) Compute $A^2\,C$.

(f) Compute $B + \mathbf{0}$

(g) Compute $A\,\mathbf{0}_{2\times 2}$ and $\mathbf{0}_{2\times 2}\,A$, where $\mathbf{0}_{2\times 2}$ is the 2×2 zero matrix,

(h) Compute $0\,A$, where 0 is the real number (scalar) zero.

(i) Let $c = 2$ and $d = 3$. Show that $(c + d)\,A = c\,A + d\,A$.

2. Let $A = \begin{pmatrix} 1 & 0 & 2 \\ 2 & -1 & 5 \\ 3 & 2 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 2 & 3 \\ 1 & 1 & 2 \\ -1 & 3 & -2 \end{pmatrix}$, and $C = \begin{pmatrix} 2 & 1 & 2 & 3 \\ 4 & 0 & 1 & 1 \\ 3 & -1 & 4 & 1 \end{pmatrix}$

Compute, if possible;

(a) $A - B$

(b) $A\,B$

(c) $A\,C - B\,C$

(d) $A\,(B\,C)$

(e) $C\,A - C\,B$

(f) $C \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix}$

3. Let $A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$. Find a matrix B such that $A\,B = I$ and $B\,A = I$, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

4. Find $A\,I$ and $B\,I$ where I is as in Exercise 3, where

$$A = \begin{pmatrix} 1 & 8 \\ 9 & 5 \end{pmatrix} \text{ and } B = \begin{pmatrix} -2 & 3 \\ 5 & -7 \end{pmatrix}.$$

What do you notice?

5. Find A^3 if $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$. What is A^{15} equal to?

B Exercises

6. (a) Determine I^2 and I^3 if $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

(b) What is I^n equal to for any $n \geq 1$?

(c) Prove your answer to part (b) by induction.

7. (a) If $A = \begin{pmatrix} 2 & 1 \\ 1 & -1 \end{pmatrix}$, $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, and $B = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$, show that $A X = B$ is a way of expressing the system $\begin{array}{l} 2x_1 + x_2 = 3 \\ x_1 - x_2 = 1 \end{array}$ using matrices.

(b) Express the following systems of equations using matrices:

(i) $\begin{array}{l} 2x_1 - x_2 = 4 \\ x_1 + x_2 = 0 \end{array}$

(ii) $\begin{array}{l} x_1 + x_2 + 2x_3 = 1 \\ x_1 + 2x_2 - x_3 = -1 \\ x_1 + 3x_2 + x_3 = 5 \end{array}$

(iii) $\begin{array}{lllll} x_1 + x_2 & & & = & 3 \\ & x_2 & & = & 5 \\ x_1 & & + 3x_3 & = & 6 \end{array}$

5.4 Special Types of Matrices

We have already investigated one special type of matrix, namely the zero matrix, and found that it behaves in matrix algebra in an analogous fashion to the real number 0; that is, as the additive identity. We will now investigate the properties of a few other special matrices.

Definition: Diagonal Matrix. *A square matrix D is called a diagonal matrix if* $d_{ij} = 0$ *whenever* $i \neq j$.

Example 5.4.1.

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{pmatrix},\ B = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -5 \end{pmatrix},\ \text{and } I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ are all diagonal matrices.}$$

In Example 5.4.1, the 3×3 diagonal matrix I whose diagonal entries are all 1's has the singular property that for any other 3×3 matrix A we have $A I = I A = A$. For example:

Example 5.4.2. If $A = \begin{pmatrix} 1 & 2 & 5 \\ 6 & 7 & -2 \\ 3 & -3 & 0 \end{pmatrix}$, then

$$A I = \begin{pmatrix} 1 & 2 & 5 \\ 6 & 7 & -2 \\ 3 & -3 & 0 \end{pmatrix} \text{ and}$$

$$I A = \begin{pmatrix} 1 & 2 & 5 \\ 6 & 7 & -2 \\ 3 & -3 & 0 \end{pmatrix}.$$

In other words, the matrix I behaves in matrix algebra like the real number 1; that is, as a multiplicative identity. In matrix algebra the matrix I is called simply the identity matrix. Convince yourself that if A is any $n\times n$ matrix $A I = I A = A$.

Definition: Identity Matrix. *The $n\times n$ diagonal matrix whose diagonal components are all 1's is called the identity matrix and is denoted by I or I_n .*

In the set of real numbers we realize that, given a nonzero real number x, there exists a real number y such that $x y = y x = 1$. We know that real numbers commute under multiplication so that the two equations can be summarized as $x y = 1$. Further we know that $y = x^{-1} = \frac{1}{x}$. Do we have an analogous situation in $M_{n\times n}(\mathbb{R})$? Can we define the multiplicative inverse of an $n\times n$ matrix A? It seems natural to imitate the definition of multiplicative inverse in the real numbers.

Definition: Matrix Inverse. *Let A be an $n\times n$ matrix. If there exists an $n\times n$ matrix B such that $A B = B A = I$, then B is the multiplicative inverse of A (called simply the inverse of A) and is denoted by A^{-1} (read "A inverse").*

When we are doing computations involving matrices, it would be helpful to know that when we find A^{-1}, the answer we obtain is the only inverse of the given matrix.

Remark: Those unfamiliar with the laws of matrices should go over the proof of Theorem 5.4.1 after they have familiarized themselves with the Laws of Matrix Algebra in Section 5.5.

Theorem 5.4.1. *The inverse of an $n\times n$ matrix A, when it exists, is unique.*

Proof: Let A be an $n\times n$ matrix. Assume to the contrary, that A has two (different) inverses, say B and C. Then

$$\begin{aligned} B &= B I && \text{Identity property of } I \\ &= B(A C) && \text{Assumption that } C \text{ is an inverse of } A \\ &= (B A) C && \text{Associativity of matrix multiplication} \\ &= I C && \text{Assumption that } B \text{ is an inverse of } A \\ &= C && \text{Identity property of } I \quad \blacksquare \end{aligned}$$

Example 5.4.3. Let $A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$. What is A^{-1} ? Without too much difficulty, by trial and error, we determine that $A^{-1} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{3} \end{pmatrix}$. This might lead us to guess that the inverse is found by taking the reciprocal of all nonzero entries of a matrix. Alas, it isn't that easy! If $A = \begin{pmatrix} 1 & 2 \\ -3 & 5 \end{pmatrix}$, the "reciprocal rule" would tell us that the inverse of A is $B = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{-1}{3} & \frac{1}{5} \end{pmatrix}$. Try computing $A B$ and you will see that you don't get the identity matrix. So, what *is* A^{-1}? In order to understand more completely the notion of the inverse of a matrix, it would be beneficial to have a formula that would enable us to compute the inverse of at least a 2×2 matrix. To do this, we need to recall the definition of the determinant of a 2×2 matrix. Appendix A gives a more complete description of the determinant of a 2×2 and higher-order matrices.

Definition: Determinant of a 2×2 Matrix. *Let* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. *The determinant of A is the number* $\det A = a d - b c$.

In addition to det A, common notation for the determinant of matrix A is $|A|$. This is particularly common when writing out the whole matrix, which case we would write $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$ for the determinant of the general 2×2 matrix.

Example 5.4.4.

If $A = \begin{pmatrix} 1 & 2 \\ -3 & 5 \end{pmatrix}$ then $\det A = 1 \cdot 5 - 2 \cdot (-3) = 11$.

If $B = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ then $\det B = 1 \cdot 4 - 2 \cdot 2 = 0$

Theorem 5.4.2. *Let* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. *If* $\det A \neq 0$, *then* $A^{-1} = \frac{1}{\det A}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Proof: See Exercise 4 at the end of this section.

Example 5.4.5. Can we find the inverses of the matrices in Example 5.4.4?

If $A = \begin{pmatrix} 1 & 2 \\ -3 & 5 \end{pmatrix}$ then $A^{-1} = \frac{1}{11}\begin{pmatrix} 5 & -2 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} \frac{5}{11} & -\frac{2}{11} \\ \frac{3}{11} & \frac{1}{11} \end{pmatrix}$

The reader should verify that $A A^{-1} = A^{-1} A = I$.

The second matrix, B has a determinant equal to zero. We we tried to apply the formula in Theorem 5.4.2, we would be dividing by zero. For this reason, the formula can't be applied and in fact B^{-1} does not exist.

Remarks:

(1) In general, if A is a 2×2 matrix and if $\det A = 0$, then A^{-1} does not exist.

(2) A formula for the inverse of $n \times n$ matrices $n \geq 3$ can be derived that also involves det A, Hence, in general, if the determinant of a matrix is zero, the matrix does not have an inverse. However the formula for even a 3×3 matrix is very long and is not the most efficient way to compute the inverse of a matrix.

(3) In Chapter 12 we will develop a technique to compute the inverse of a higher-order matrix, if it exists.

(4) Matrix inversion comes first in the hierarchy of matrix operations; therefore, $A B^{-1}$ is $A(B^{-1})$.

EXERCISES FOR SECTION 5.4

A Exercises

1. For the given matrices A find A^{-1} if it exists and verify that $A A^{-1} = A^{-1} A = I$ If A^{-1} does not exist explain why.

(a) $A = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}$

(b) $A = \begin{pmatrix} 6 & -3 \\ 8 & -4 \end{pmatrix}$

(c) $A = \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix}$

(d) $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

(e) Use the definition of the inverse of a matrix to find A^{-1}:

$$A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & -5 \end{pmatrix}$$

2. For the given matrices A find A^{-1} if it exists and verify that $A A^{-1} = A^{-1} A = I$ If A^{-1} does not exist explain why.

(a) $A = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$

(b) $A = \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix}$

(c) $A = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$

(d) $A = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$, were $a > b > 0$.

3. (a) Let $A = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}$ and $B = \begin{pmatrix} 3 & -3 \\ 2 & 1 \end{pmatrix}$. Verify that $(A B)^{-1} = B^{-1} A^{-1}$.

(b) Let A and B be $n \times n$ invertible matrices. Prove that $(A B)^{-1} = B^{-1} A^{-1}$. Why is the right side of the above statement written "backwards"? Is this necessary? Hint: Use Theorem 5.4.1.

B Exercises

4. Let Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Derive the formula for A^{-1}.

5. (a) Let A and B be as in problem 3 above. Show that $\det(A B) = (\det A)(\det B)$.

(b) It can be shown that the statement in part (a) is true for all $n \times n$ matrices. Let A be any invertible $n \times n$ matrix. Prove that $\det(A^{-1}) = (\det A)^{-1}$. Note: The determinant of the identity matrix I_n is 1 for all n, see Appendix A for details.

(c) Verify that the equation in part (b) is true for the matrix in exercise l(a) of this section.

6. Prove by induction that for $n \geq 1$, $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^n = \begin{pmatrix} a^n & 0 \\ 0 & b^n \end{pmatrix}$.

7. Use the assumptions in exercise 5 to prove by induction that if n ≥ 1, $\det(A^n) = (\det A)^n$.

8. Prove: If the determinant of a matrix A is zero, then A does not have an inverse. Hint: Use the indirect method of proof and exercise 5.

C Exercise

9. (a) Let A, B, and D be $n \times n$ matrices. Assume that B is invertible. If $A = B D B^{-1}$, prove by induction that $A^m = B D^m B^{-1}$ is true for $m \geq 1$.

(b) Given that $A = \begin{pmatrix} -8 & 15 \\ -6 & 11 \end{pmatrix} = B \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} B^{-1}$ where $B = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}$ what is A^{10} ?

5.5 Laws of Matrix Algebra

The following is a summary of the basic laws of matrix operations. Assume that the indicated operations are defined; that is, that the orders of the matrices *A*, *B*, and *C* are such that the operations make sense.

(1) $A + B = B + A$

(2) $A + (B + C) = (A + B) + C$

(3) $c(A + B) = cA + cB$, where $c \in \mathbb{R}$.

(4) $(c_1 + c_2)A = c_1 A + c_2 A$, where $c_1, c_2 \in \mathbb{R}$.

(5) $c_1(c_2 A) = (c_1 \cdot c_2)A$, where $c_1, c_2 \in \mathbb{R}$.

(6) $\mathbf{0}A = \mathbf{0}$, where $\mathbf{0}$ is the zero matrix.

(7) $0A = \mathbf{0}$, where 0 on the left is the number 0.

(8) $A + 0 = A$.

(9) $A + (-1)A = \mathbf{0}$.

(10) $A(B + C) = AB + AC$.

(11) $(B + C)A = BA + CA$.

(12) $A(BC) = (AB)C$.

(13) $IA = A$ and $AI = A$.

(14) If A^{-1} exists, $(A^{-1})^{-1} = A$.

(15) If A^{-1} and B^{-1} exist, $(AB)^{-1} = B^{-1}A^{-1}$

Example 5.5.1. If we wished to write out each of the above laws more completely, we would specify the orders of the matrices. For example, Law 10 should read:

(10) Let *A*, *B*, and *C* be $m\times n$, $n\times p$, and $n\times p$ matrices, respectively, then $A(B + C) = AB + AC$

Remarks:

(1) Notice the absence of the "law" $AB = BA$. Why?

(2) Is it really necessary to have both a right (No. 11) and a left (No. 10) distributive law? Why?

(3) What does Law 8 define? What does Law 9 define?

EXERCISES FOR SECTION 5.5

A Exercises

1. Rewrite the above laws specifying as in Example 5.5.1 the orders of the matrices.

2. Verify each of the Laws of Matrix Algebra using examples.

3. Let $A = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$, $B = \begin{pmatrix} 3 & 7 & 6 \\ 2 & -1 & 5 \end{pmatrix}$, and $C = \begin{pmatrix} 0 & -2 & 4 \\ 7 & 1 & 1 \end{pmatrix}$. Compute the following as efficiently as possible by using any of the Laws of Matrix Algebra:

(a) $AB + AC$

(b) A^{-1}

(c) $A(B + C)$

(d) $(A^2)^{-1}$

(e) $(C + B)^{-1} A^{-1}$

4. Let $A = \begin{pmatrix} 7 & 4 \\ 2 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 3 & 5 \\ 2 & 4 \end{pmatrix}$. Compute the following as efficiently as possible by using any of the Laws of Matrix Algebra:

(a) $A B$

(b) $A + B$

(c) $A^2 + A B + B A + B^2$

(d) $B^{-1} A^{-1}$

(e) $A^2 + A B$

5. Let A and B be $n \times n$ matrices of real numbers. Is $A^2 - B^2 = (A - B)(A + B)$? Explain

5.6 Matrix Oddities

We have seen that matrix algebra is similar in many ways to elementary algebra. Indeed, if we want to solve the matrix equation $A X = B$ for the unknown X, we imitate the procedure used in elementary algebra for solving the equation $a x = b$. Notice how exactly the same properties are used in the following detailed solutions of both equations.

Solution of $a x = b$		**Solution of $A X = B$**	
$a x = b$		$A X = B$	
$a^{-1}(a x) = a^{-1} b$	if $a \neq 0$	$A^{-1}(A X) = A^{-1} B$	if A^{-1} exists
$(a^{-1} a) x = a^{-1} b$	associative law	$(A^{-1} A) X = A^{-1} B$	associative law
$1 x = a^{-1} b$	definition of inverse	$I X = A^{-1} B$	definition of inverse
$x = a^{-1} b$	identity property of 1	$X = A^{-1} B$	identity property of I

Certainly the solution process for $A X = B$ is the same as that of $a x = b$.

The solution of $x a = b$ is $x = b a^{-1} = a^{-1} b$. In fact, we usually write the solution of both equations as $x = \frac{b}{a}$. In matrix algebra, the solution of $X A = B$ is $X = B A^{-1}$, which is not necessarily equal to $A^{-1} B$. So in matrix algebra, since the commutative law (under multiplication) is not true, we have to be more careful in the methods we use to solve equations.

It is clear from the above that if we wrote the solution of $A X = B$ as $X = \frac{B}{A}$, we would not know how to interpret the answer $\frac{B}{A}$. Does it mean $A^{-1} B$ or $B A^{-1}$? Because of this, A^{-1} is never written as $\frac{1}{A}$.

Some of the main dissimilarities between matrix algebra and elementary algebra are that in matrix algebra:

(1) $A B$ may be different from $B A$.

(2) There exist matrices A and B such that $A B = \mathbf{0}$, and yet $A \neq \mathbf{0}$ and $B \neq \mathbf{0}$.

(3) There exist matrices A where $A \neq \mathbf{0}$, and yet $A^2 = \mathbf{0}$.

(4) There exist matrices A where $A^2 - A$ with $A \neq I$ and $A \neq \mathbf{0}$

(5) There exist matrices A where $A^2 = I$, where $A \neq I$ and $A \neq -I$

EXERCISES FOR SECTION 5.6

A Exercises

1. Discuss each of the above "oddities" with respect to elementary algebra.

2. Determine 2×2 matrices which show each of the above "oddities" are true.

B Exercises

3. Prove the following implications, if possible:

(a) $A^2 = A$ and $\det A \neq 0 \Rightarrow A = I$

(b) $A^2 = I$ and $\det A \neq 0 \Rightarrow A = I$ or $A = -I$.

4. Let $M_{n\times n}(\mathbb{R})$ be the set of real $n\times n$ matrices. Let $P \subseteq M_{n\times n}(\mathbb{R})$ be the subset of matrices defined by $A \in P$ if and only if $A^2 = A$. Let $Q \subseteq P$ be defined by $A \in Q$ if and only if $\det A \neq 0$.

(a) Determine the cardinality of Q.

(b) Consider the special case $n = 2$ and prove that a sufficient condition for $A \in P \subseteq M_{2\times 2}(\mathbb{R})$ is that A has a zero determinant (i.e., A is singular) and $\operatorname{tr}(A) = 1$ where $\operatorname{tr}(A) = a_{11} + a_{22}$ is the sum of the main diagonal elements of A.

(c) Is the condition of part b a necessary condition?

C Exercises

5. Write each of the following systems in the form $A X = B$, and then solve the systems using matrices.

(a) $2 x_1 + x_2 = 3$
$x_1 - x_2 = 1$

(b) $2 x_1 - x_2 = 4$
$x_1 - x_2 = 0$

(c) $2 x_1 + x_2 = 1$
$x_1 - x_2 = 1$

(d) $2 x_1 + x_2 = 1$
$x_1 - x_2 = -1$

(e) $3 x_1 + 2 x_2 = 1$
$6 x_1 + 4 x_2 = -1$

6. Recall that $p(x) = x^2 - 5x + 6$ is called a polynomial, or more specifically, a polynomial over $\mathbb{R}$, where the coefficients are elements of $\mathbb{R}$ and $x \in \mathbb{R}$. Also, think of the method of solving, and solutions of, $x^2 - 5x + 6 = 0$. We would like to define the analogous situation for 2×2 matrices. First define where A is a 2×2 matrix $p(A) = A^2 - 5A + 6I$. Discuss the method of solving and the solutions of $A^2 - 5A + 6I = \mathbf{0}$.

7. (For those who know calculus)

(a) Write the series expansion for e^a centered around $a = 0$.

(b) Use the idea of exercise 6 to write what would be a plausible definion of e^A where A is an $n \times n$ matrix.

(c) If $A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}$, use the series in part (b) to show that $e^A = \begin{pmatrix} e & e-1 \\ 0 & 1 \end{pmatrix}$ and $e^B = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$.

(d) Show that $e^A e^B \neq e^B e^A$

(e) Show that $e^{A+B} = \begin{pmatrix} e & 0 \\ 0 & 1 \end{pmatrix}$

(f) Is $e^A e^B = e^{A+B}$?

SUPPLEMENTARY EXERCISES FOR CHAPTER 5

Sections 5.1 through 5.3

1. Determine x and y in the following:

$$\begin{pmatrix} x+y & 5 \\ -2 & x-y \end{pmatrix} = \begin{pmatrix} 3 & 5 \\ -2 & 4 \end{pmatrix}$$

2. Let $A = \begin{pmatrix} 1 & 0 & -1 \\ 2 & 1 & 5 \\ 3 & -4 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 & 2 \\ 3 & -1 & 1 \\ 1 & 2 & -1 \end{pmatrix}$, $C = \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix}$. Compute:

(a) $2A - 3B$
(b) $2A - 5A$
(c) $AC + BC$

3. Let A and B be two $m \times m$ matrices with $AB = BA$. Prove by induction on n that $AB^n = B^n A$ for n greater than or equal to 1.

4. Prove by induction that if n is a positive integer, and

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \text{then } A^n = \begin{pmatrix} 1 & n & n(n-1)/2 \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}$$

Section 5.4

5. Determine $A^{-1} A^3$ if $A = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}$

6. Let $A = \begin{pmatrix} 4 & -2 \\ -2 & 5 \end{pmatrix}$ and $B = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}$

Compute $A + B$, $A^2 + AB + BA + B^2$, and $B^{-1} A^{-1}$. You may save some time by thinking before plunging into the computations.

7. For what real number c will the matrix D have no inverse? Explain your answer.

$D = \begin{pmatrix} 3 & 15 \\ 4 & c \end{pmatrix}$

8. Let $P = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{R}) \,\middle|\, ad \neq bc \right\}$.

Fact: The inverse of a diagonal matrix belonging to P can be found simply by reciprocating the diagonal elements of the matrix.

(a) Determine $\begin{pmatrix} 3 & 0 \\ 0 & 6 \end{pmatrix}^{-1}$.

(b) Suppose $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in P$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1/a & b \\ c & 1/d \end{pmatrix}$. In general, is $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ a diagonal matrix? If yes, explain why; if no, give the most general form of such a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Section 5.5

9. (a) Let A and B be $n \times n$ matrices. Expand $(A + B)^2$.

(b) Is $(A + B)^2$ ever equal to $A^2 + 2AB + B^2$? Explain.

10. Solve the following matrix equation for X. Be careful to explain under which conditions each step is possible.

$$AX + C = BX$$

Section 5.6

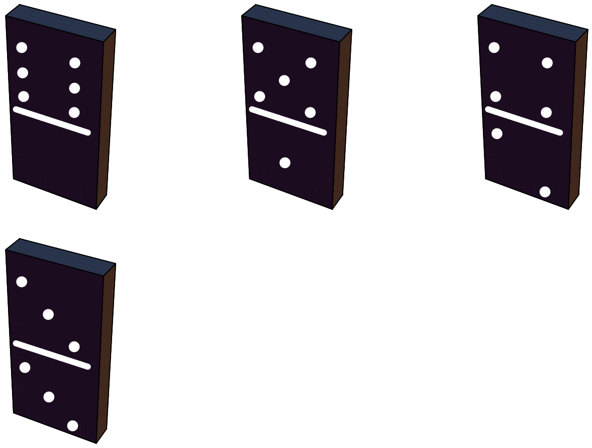
11. Prove or disprove: $A^{-1} = A$ and $B^{-1} = B \Rightarrow (AB)^{-1} = AB$.

12. The following is true for all real numbers a and b: $a \cdot b = 0$ if and only if $a = 0$ or $b = 0$. Is any part of this statement true for $n \times n$ matrices A and B? Explain. Give an example and proof.

13. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where $a, b, c, d \in \mathbb{R}$. Show that the matrices of the form $A = \pm\begin{pmatrix} 1 & 0 \\ c & -1 \end{pmatrix}$, and $A = \pm\begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix}$ are also solutions to the equation $A^2 = I$, confirming that a quadratic matrix equation can have an infinite number of solutions. Are there any others?

chapter 6

RELATIONS AND GRAPHS



GOALS

One understands a set of objects completely only if the structure of that set is made clear by the interrelationships between its elements. For example, the individuals in a crowd can be compared by height, by age, or through any number of other criteria. In mathematics, such comparisons are called relations. The goal of this chapter is to develop the language, tools, and concepts of relations.

6.1 Basic Definitions

In Chapter 1 we introduced the concept of the Cartesian product of sets. Let's assume that a person owns three shirts and two pairs of slacks. More precisely, let $A = \{\text{blue shirt}, \text{tan shirt}, \text{mint green shirt}\}$ and $B = \{\text{grey slacks}, \text{tan slacks}\}$. Then certainly $\mathrm{A} \times \mathrm{B}$ is the set of all possible combinations (six) of shirts and slacks that the individual can wear. However, the individual may wish to restrict himself or herself to combinations which are color coordinated, or "related." This may not be all possible pairs in $A \times B$ but will certainly be a subset of $A \times B$. For example, one such subset may be $\{(\text{blue shirt}, \text{grey slacks}), (\text{blue shirt}, \text{tan slacks}), (\text{mint green shirt}, \text{tan slacks})\}$.

Definition: Relation. *Let A and B be sets. A relation from A into B is any subset of $A \times B$.*

Example 6.1.1. Let $A = \{1, 2, 3\}$ and $B = \{4, 5\}$. Then $\{(1, 4), (2, 4), (3, 5)\}$ is a relation from A into B. Of course, there are many others we could describe; 64, to be exact.

Example 6.1.2. Let $A = \{2, 3, 5, 6\}$ and define a relation r from A into A by $(a, b) \in r$ if and only if a divides evenly into b. The set of pairs that qualify for membership is $r = \{(2, 2), (3, 3), (5, 5), (6, 6), (2, 6), (3, 6)\}$.

Definition: Relation on a Set. *A relation from a set A into itself is called a relation on A.*

The relation "divides" in Example 6.1.2 is will appear throughout the book. Here is a general definition on the whole set of integers.

Definition: Divides. *Let $a, b \in \mathbb{Z}$.*
$a \mid b$ if and only if there exists an integer k such that $a k = b$.

Be very careful in writing about “divides.” The vertical line symbol use for this relation, if written carelessly, can look like division. While $a \mid b$ is either true or false, a / b is a number.

Based on the equation $a k = b$, we can say that $a \mid b$ is equivalent to $k = \frac{b}{a}$, or a divides evenly into b. In fact the "divides" is short for "divides evenly into." You might find the equation $k = \frac{b}{a}$ initially easier to understand, but in the long run we will find the equation $a k = b$ more convenient.

Sometimes it is helpful to illustrate a relation with a graph. Consider Example 6.1.1. A graph of r can be drawn as in Figure 6.1.1. The arrows indicate that 1 is related to 4 under r. Also, 2 is related to 4 under r, and 3 is related to 5, while the upper arrow denotes that r is a relation from the whole set A into the set B.

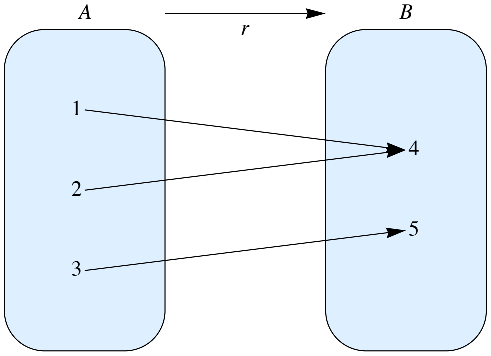


FIGURE 6.1.1 A graph of a relation

A typical element in a relation r is an ordered pair (x, y). In some cases, r can be described by actually listing the pairs which are in r, as in the previous examples. This may not be convenient if r is relatively large. Other notations are used with certain well-known relations. Consider the "less than on equal" relation on the real numbers. We could define it as a set of ordered pairs this way:

$$s = \{(x, y) \mid x \leq y\}.$$

The notation $x \leq y$ is clear and self-explanatory; it is a more natural, and hence preferred, notation to use than $(x, y) \in s$.

Many of the relations we will work with "resemble" the relation ≤, so $x\, s\, y$ is a common way to express the fact that x is related to y through the relation s.

Relation Notion. *Let s be a relation from a set A into a set B. Then the fact that* $(x, y) \in s$ *is frequently written* $x\, s\, y$.

Let $A = \{2, 3, 5, 8\}$, $B = \{4, 6, 16\}$, and $C = \{1, 4, 5, 7\}$; let r be the relation "divides," denoted by |, from A into B; and let s be the relation ≤ from B into C. So $r = \{(2, 4), (2, 6), (2, 16), (3, 6), (8, 16)\}$ and $s = \{(4, 4), (4, 5), (4, 7), (6, 7)\}$.

Notice from Figure 6.1.2 that we can, for certain elements of A, go through elements in B to results in C. That is:

$$2 \mid 4 \text{ and } 4 \leq 4$$

$$2 \mid 4 \text{ and } 4 \leq 5$$

$$2 \mid 4 \text{ and } 4 \leq 7$$

$$2 \mid 6 \text{ and } 6 \leq 7$$

$$3 \mid 6 \text{ and } 6 \leq 7$$

Based on this observation, we can define a new relation, call it rs, from A into C. In order for (a, c) to be in rs, it must be possible to travel along a path in Figure 6.1.2 from a to c. In other words, $(a, c) \in rs$ if and only if $(\exists\, b)_B\, (a\, r\, b$ and $b\, s\, c)$. The name rs was chosen because it reminds us that this new relation was formed by the two previous relations r and s. The complete listing of all elements in rs is $\{(2, 4), (2, 5), (2, 7), (3, 7)\}$. We summarize in a definition.

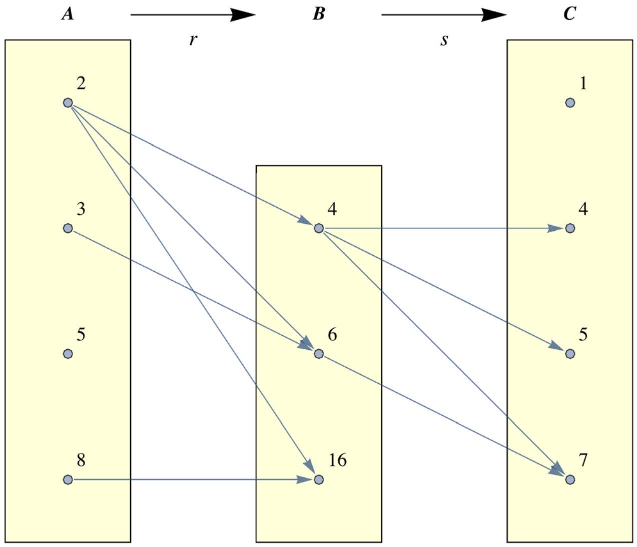


FIGURE 6.1.2 Graphical representation of composition of relations

Definition: Composition of Relations. *Let r be a relation from a set A into a set B, and let s be a relation from B into a set C. The composition of r with s, written rs, is the set of pairs of the form* $(a, c) \in A\times C$*, where* $(a, c) \in rs$ *if and only if there exists* $b \in B$ *such that* $(a, b) \in r$ *and* $(b, c) \in s$*.*

Remark: A word of warning to those readers familiar with composition of functions. (For those who are not, disregard this remark. It will be repeated at an appropriate place in Chapter 7.) As indicated above, the traditional way of describing a composition of two relations is rs where r is the first relation and s the second. However, function composition is traditionally expressed "backwards"; that is, $s\circ r$, where r is the first function and s is the second.

EXERCISES FOR SECTION 6.1

A Exercises

1. For each of the following relations r defined on $\mathbb{P}$, determine which of the given ordered pairs belong to r.

(a) $x\, r\, y$ iff $x \mid y$; $(2, 3), (2, 4), (2, 8), (2, 17)$

(b) $x\, r\, y$ iff $x \leq y$; $(2, 3), (3, 2), (2, 4), (5, 8)$

(c) $x\, r\, y$ iff $y = x^2$; $(1,1), (2, 3), (2, 4), (2, 6)$

2. The following relations are on $\{1, 3, 5\}$. Let r be the relation $x\, r\, y$ iff $y = x + 2$ and s the relation $x\, s\, y$ iff $x \leq y$.

(a) Find rs.

(b) Find sr.

(c) Illustrate rs and sr via a diagram.

(d) Is the relation (set) rs equal to the relation sr? Why?

3. Let $A = \{1, 2, 3, 4, 5\}$ and define r on A by $x\, r\, y$ iff $x + 1 = y$. We

define $r^2 = rr$ and $r^3 = r^2 r$. Find:

(a) r

(b) r^2

(c) r^3

4. Given s and t, relations on $\mathbb{Z}$, $s = \{(1, n) : n \in \mathbb{Z}\}$ and $t = \{(n, 1) : n \in \mathbb{Z}\}$, what are st and ts? Hint: Even when a relation involves infinite sets, you can often get insights into them by drawing partial graphs.

B Exercises

5. Let ρ be the relation on the power set, $\mathcal{P}(S)$, of a finite set S of cardinality n. Define ρ by $(A, B) \in \rho$ iff $A \cap B = \emptyset$.

(a) Consider the specific case $n = 3$, and determine the cardinality of the set ρ.

(b) What is the cardinality of ρ for an arbitrary n? Express your answer in terms of n. (Hint: There are three places that each element of S can go in building an element of ρ.)

6. Let r_1, r_2, and r_3 be relations on any set A. Prove that if $r_1 \subseteq r_2$then $r_1 r_3 \subseteq r_2 r_3$.

6.2 Graphs of Relations on a Set

In this section we introduce directed graphs as a way to visualize relations on a set.

Example 6.2.1, Let $A = \{0, 1, 2, 3\}$, and let

$$r = \{(0, 0), (0, 3), (1, 2), (2, 1), (3, 2), (2, 0)\}.$$

The elements of A are called the vertices of the graph. They are represented by labeled points or occasionally by small circles. We connect vertex a to vertex b with an arrow, called an edge, going from vertex a to vertex b if and only if $a\, r\, b$. This type of graph of a relation r is called a *directed graph* or *digraph*. Figure 6.2.1 is a digraph for r. Notice that since $1\, r\, 2$ and $2\, r\, 1$, we draw a single edge between 1 and 2 with arrows in both directions. Since 0 is related to itself, we draw a "self-loop" at 0.

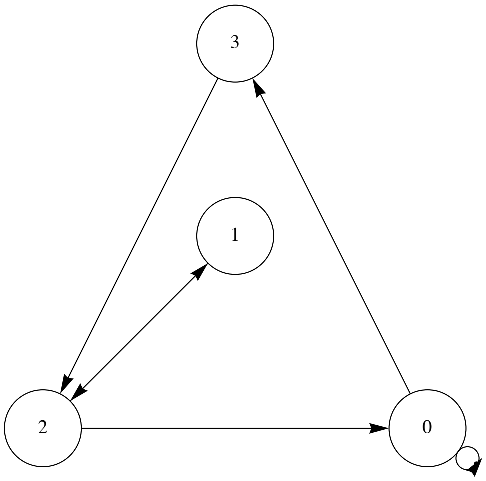


FIGURE 6.2.1

The actual location of the vertices is immaterial. The main idea is to place the vertices in such a way that the graph is easy to read. Obviously, after a rough-draft graph of a relation, we may decide to relocate the vertices so that the final result will be neater. Figure 6.2.1 could also be presented as in Figure 6.2.2.

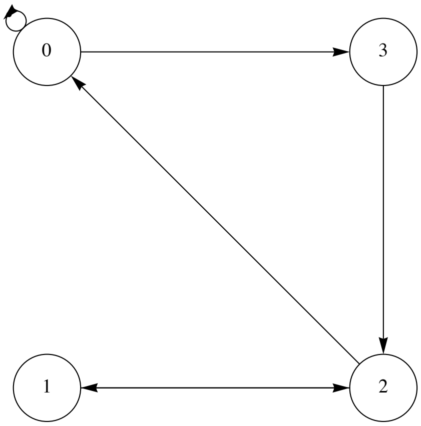


FIGURE 6.2.2

A vertex of a graph is also called a node, point, or a junction. An edge of a graph is also referred to as an arc, a line, or a branch. Do not be concerned if two graphs of a given relation look different.

Example 6.2.2. Consider the relation s whose digraph is Figure 6.2.3. What information does this give us? The graph tells us that s is a relation on $A = \{1, 2, 3\}$ and that

$$s = \{(1, 2), (2, 1), (1, 3), (3, 1), (2, 3), (3, 3)\},$$

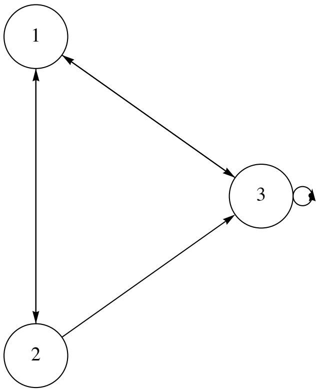


FIGURE 6.2.3

Example 6.2.3. Let $B = \{1, 2\}$, and let $A = \mathcal{P}(B) = \{0, \{1\}, \{2\}, \{1, 2\}\}$. Then $\subseteq$ is a relation on A whose digraph is Figure 6.2.4.

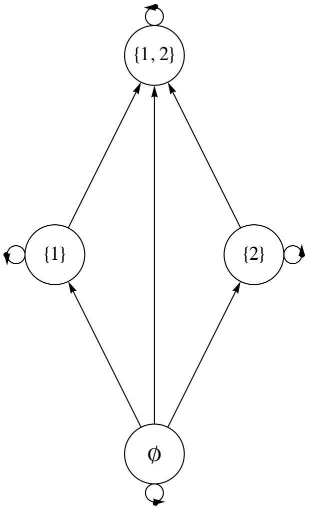


FIGURE 6.2.4

We will see in the next section that since $\subseteq$ has certain structural properties that describe “partial orderings.” We will be able to draw a much simpler type graph than this one, but for now the graph above serves our purposes.

EXERCISES FOR SECTION 6.2

A Exercises

1. Let $A = \{1, 2, 3, 4\}$, and let r be the relation $\leq$ on A. Draw a digraph for r.

2. Let $B = \{1, 2, 3, 4, 6, 8, 12, 24\}$, and let s be the relation "divides," on B. Draw a digraph for s.

3. Let $A = \{1, 2, 3, 4, 5\}$. Define t on A by $a\, t\, b$ if and only if $b - a$ is even. Draw a digraph for t.

4. (a) Let A be the set of strings of 0's and 1's of length 3 or less. Define the relation of d on A by $x\, d\, y$ if x is contained within y. For example, $01\, d\, 101$. Draw a digraph for this relation.

(b) Do the same for the relation p defined by $x\, p\, y$ if x is a prefix of y. For example, $10\, p\, 101$, but $01\, p\, 101$ is false.

B Exercises

5. Recall the relation in Exercise 5 of Section 6.1, ρ defined on the power set, $\mathcal{P}(S)$, of a set S. The definition was $(A, B) \in \rho$ iff $A \cap B = \emptyset$. Draw the digraph for ρ where $S = \{a, b\}$.

6. Let $C = \{1, 2, 3, 4, 6, 8, 12, 24\}$ and define t on C by

$a\, t\, b$ if and only if a and b share a common divisor greater than 1.

Draw a digraph for t.

6.3 Properties of Relations

Consider the set $B = \{1, 2, 3, 4, 6, 12, 36, 48\}$ and the relations "divides" and $\leq$ on B. We notice that these two relations on B have three properties in common:

(1) Every element in B divides itself and is less than or equal to itself. This is called the reflexive property.

(2) If we search for two elements from B where the first divides the second and the second divides the first, then we are forced to choose the the two numbers to be the same. In other words, no two *different* numbers are related in both directions. The reader can verify that a similar fact is true for the relation $\leq$ on B. This is called the antisymmetric property,

(3) Next if we choose three numbers from B such that the first divides the second and the second divides the third, then we always find that the first number to divides the third. Again, the same is true if we replace “divides” with “is less than or equal to.” This is called the transitive property.

Relations that satisfy these properties are of special interest to us. Formal definitions of the properties follow.

Definition: Reflexive Relation. *Let A be a set and let r be a relation on A.*
r is ***reflexive*** *if and only if $a\,r\,a$ for all $a \in A$.*

Definition: Antisymmetric Relation. *Let A be a set and let r be a relation on A.*

r is ***antisymmetric*** *if and only if whenever $a\,r\,b$ and $a \neq b$ then $b\,r\,a$ is false.*

An equivalent condition for antisymmetry is that whenever $a\,r\,b$ and $b\,r\,a$ then $a = b$. You are encouraged to convince yourself that this is the case.

A word of warning about antisymmetry: Students frequently find it difficult to understand this definition. Keep in mind that this term is defined through an "If . .. then . . ." statement. The question that you must ask is: Is it true that whenever there are elements a and b from A where $a\,r\,b$ and $a \neq b$, it follows that b is not related to a? If so, then the relation r is antisymmetric.

Another way to determine whether a relation is antisymmetric is to examine its digraph. The relation is *not* antisymmetric if there exists a pair of vertices that are connected by edges in both directions.

Definition: Transitive Relation. *Let A be a set and let r be a relation on A.*

r is ***transitive*** *if and only if whenever $a\,r\,b$ and $b\,r\,c$ then $a\,r\,c$.*

Partial Orderings

Not all relations have all three of the properties discussed above. Those that do, are a special type of relation.

Definition: Partial Ordering, Poset. *A relation on a set A that is reflexive, antisymmetric, and transitive is called a partial ordering on A. A set on which there is a partial ordering relation defined is called a partially ordered set or poset.*

Example 6.3.1. Let A be a set. Then $\mathcal{P}(A)$ together with the relation $\subseteq$ (set containment) is a poset. To prove this we observe that the three properties hold, as discussed in Chapter 4.

(1) Let $B \in \mathcal{P}(A)$. The fact that $B \subseteq B$ follows from the definition of subset. Hence, set containment is reflexive.

(2) Let $B_1, B_2 \in \mathcal{P}(A)$ and assume that $B_1 \subseteq B_2$ and $B_1 \neq B_2$. Could it be that $B_2 \subseteq B_1$? No. There must be some element $a \in A$ such that $a \notin B_1$, but $a \in B_2$. This is exactly what we need to conclude that B_2 is not contained in B_1. Hence, set containment is antisymmetric

(3) Let $B_1, B_2, B_3 \in \mathcal{P}(A)$ and assume that $B_1 \subseteq B_2$ and $B_2 \subseteq B_3$. Does it follow that $B_1 \subseteq B_3$? Yes, if $a \in B_1$, then $a \in B_2$ because $B_1 \subseteq B_2$. Now that we have $a \in B_2$ and we have assumed $B_2 \subseteq B_3$, we conclude that $a \in B_3$. Therefore, $B_1 \subseteq B_3$ and so set containment is transitive.

Figure 6.3.1 is the graph for the “set containment” relation on $\{1, 2\}$.

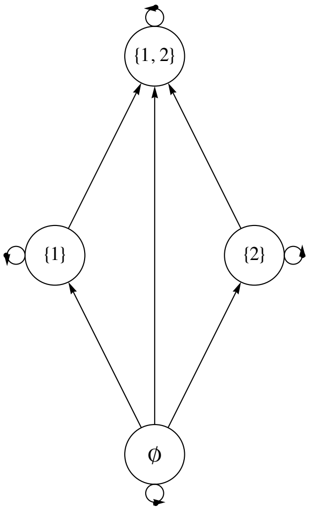


FIGURE 6.3.1

This graph is helpful insofar as it reminds us that each set is a subset of itself (How?) and shows us at a glance the relationship between the various subsets in $\mathcal{P}(\{1, 2\})$. However, when a relation is a partial ordering, we can streamline a graph like this one. The streamlined form of a graph is called a *Hasse diagram* or *ordering diagram*. A Hasse diagram takes into account the following facts.

(1) By the reflexive property, each vertex must be related to itself, so the arrows from a vertex to itself (called "self-loops") are not drawn in a Hasse diagram. They are simply assumed.

(2) By the antisymmetry property, connections between two distinct elements in a directed graph can only go one way, if at all. When there is a connection, we agree to always place the second element above the first (as we do above with the connection from {1} to {1, 2}). For this reason, we can just draw a connection without an arrow, just a line.

(3) By the transitive property, if there are edges connecting one element up to a second element and the second element up to a third element, then there will be a direct connection from the first to the third. We see this in Figure 6.3.1 with $\emptyset$ connected to {1} and then {1} connected to {1, 2}. Notice the edge connecting $\emptyset$ to {1, 2}. Whenever we identify this situation, remove the connection from the first to the third in a Hasse diagram and simply observe that an upward path of any length implies that the lower element is related to the upper one.

Using these observations as a guide, we can draw a Hasse diagram for $\subseteq$ on {1, 2} as in Figure 6.3.2.

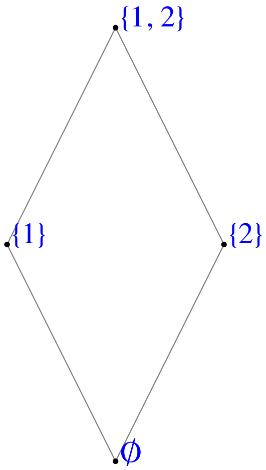


FIGURE 6.3.2

Example 6.3.2. Consider the partial ordering relation s whose Hasse diagram is Figure 6.3.3.

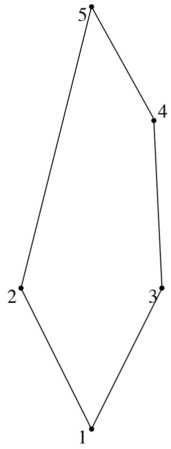


FIGURE 6.3.3

How do we read this diagram? What is A? What is s? What does the digraph of s look like? Certainly $A = \{1, 2, 3, 4, 5\}$ and $1 \, s \, 2$, $3 \, s \, 4$, $1 \, s \, 4$, $1 \, s \, 5$, etc., Notice that $1 \, s \, 5$ is implied by the fact that there is a path of length three upward from 1 to 5. This follows from the edges that are shown and the transitive property that is presumed in a poset. Since $1 \, s \, 3$ and $3 \, s \, 4$, we know that $1 \, s \, 4$. We then combine $1 \, s \, 4$ with $4 \, s \, 5$ to infer $1 \, s \, 5$. Without going into details why, here is a complete list of pairs defined by s.

$$s = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (1, 3), (1, 4), (1, 5), (1, 2), (3, 4), (3, 5), (4, 5), (2, 5)\}$$

A digraph for s is Figure 6.3.4. It is certainly more complicated to read and difficult to draw than the Hasse diagram.

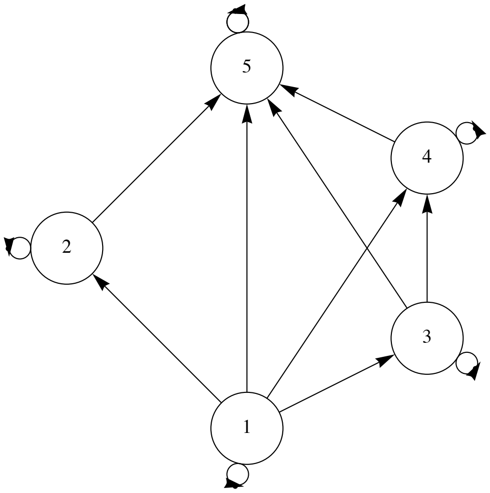


FIGURE 6.3.4 Digraph of Example 6,3.2

A classic example of a partial ordering relation is ≤ on the real numbers, ℝ. Indeed, when graphing partial ordering relations, it is natural to "plot" the elements from the given poset starting with the "least" element to the "greatest" and to use terms like "least," "greatest," etc. Because of this the reader should be forewarned that some texts use the symbol ≤ for arbitrary partial orderings. This can be quite confusing for the novice, so we continue to use generic letters r, s, etc.

Equivalence Relations

Another common property of relations is symmetry.

Definition: Symmetry. *Let r be a relation on a set A. r is* ***symmetric*** *if and only if whenever a r b, it follows that b r a.*

Consider the relation of equality (=) defined on any set A. Certainly $a = b$ implies that $b = a$ so equality is a symmetric relation on A.

Surprisingly, equality is also an antisymmetric relation on A. This is due to the fact that the condition that defines the antisymmetry property, $a = b$ and $a \neq b$, is a contradiction. Remember, a conditional proposition is always true when the condition is false. So a relation can be both symmetric and antisymmetric on a set! Again recall that these terms are *not* negatives of one other. That said, there are very few relations that are both symmetric and antisymmetric.

Definition: Equivalence Relation. *A relation r on a set A is called an equivalence relation if and only if it is reflexive, symmetric, and transitive.*

The classic example of an equivalence relation is equality on a set A. In fact, the term equivalence relation is used because those relations which satisfy the definition behave quite like the equality relation. Here is another important equivalence relation.

Example 6.3.3. Let $\mathbb{Z}^*$ be the set of nonzero integers. One of the most basic equivalence relations in mathematics is the relation q on $\mathbb{Z}\times\mathbb{Z}^*$ defined by $(a, b)\, q\, (c, d)$ if and only if $a d = b c$. We will leave it to the reader to, verify that q is indeed an equivalence relation. Be aware that since the elements of $\mathbb{Z}\times\mathbb{Z}^*$are ordered pairs, proving symmetry involves four numbers and transitivity involves six numbers. Two ordered pairs, (a, b) and (c, d), are related if the fractions $\frac{a}{b}$ and $\frac{c}{d}$ are numerically equal.

FIGURE 6.3.5.

Example 6.3.4. Let m be a positive integer, $m \geq 2$. We define *congruence modulo m* to be the relation $\equiv_m$ defined on the integers by

$$a \equiv_m b \quad \text{if and only if} \quad m \mid (a - b)$$

(1) This relation is reflexive, for if $a \in \mathbb{Z}$, $m \mid (a - a) \Rightarrow a \equiv_m a$.

(2) This relation is symmetric. We can prove this through the following chain of implications.

$$\begin{aligned} a \equiv_m b \quad &\Rightarrow \quad m \mid (a - b) \\ &\Rightarrow a - b = m k \quad \text{for some } k \in \mathbb{Z} \\ &\Rightarrow b - a = m(-k) \\ &\Rightarrow m \mid (b - a) \\ &\Rightarrow b \equiv_m a \end{aligned}$$

(3) Finally, this relation is transitive. We leave it to the reader to prove that if $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$.

On occasion, you will see the equivalent notation $a \equiv b \,(\text{mod } m)$ for this relation.

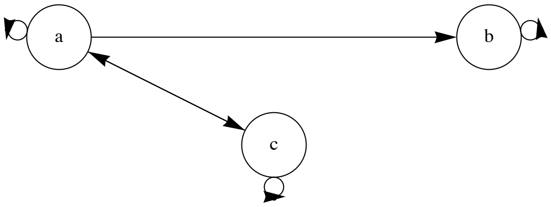
Example 6.3.5. Consider the relation s described by the digraph in Figure 6.3.5.

This relation is reflexive (Why?)

It is not symmetric (Why?)

It is not transitive (Why?)

Is s an equivalence relation or a partial ordering? It is neither, and among the valid reasons why is that s is not transitive.



EXERCISES FOR SECTION 6.3

A Exercises

1. (a) Let $B = \{a, b\}$ and $U = \mathcal{P}(B)$. Draw a Hasse diagram for $\subseteq$ on U.

(b) Let $A = \{1, 2, 3, 6\}$. Show that divides, $|$, is a partial ordering on A.

(c) Draw a Hasse diagram for divides on A.

(d) Compare the graphs of parts a and c.

2. Repeat Exercise 1 with $B = \{a, b, c\}$ and $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$.

3. (a) Consider the relations defined by the digraphs in Figure 6.3.6. Determine whether the given relations are reflexive, symmetric, antisymmetric, or transitive. Try to develop procedures for determining the validity of these properties from the graphs,

(b) Which of the graphs in Figure 6.3.6 are of equivalence relations or of partial orderings?

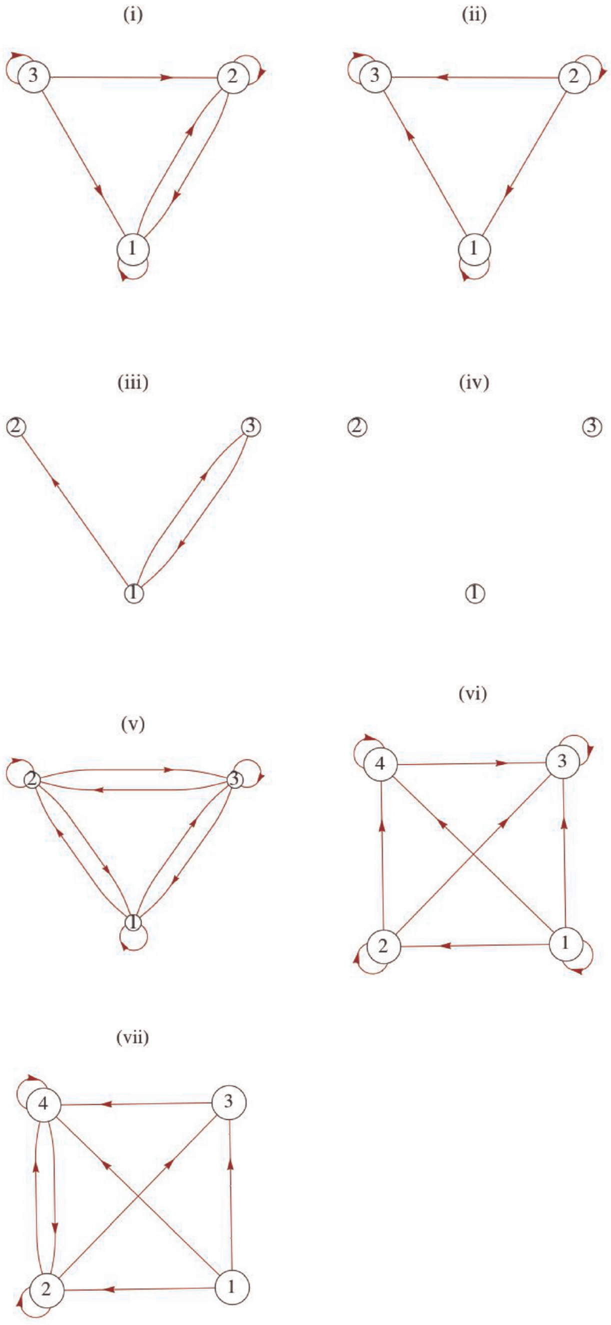


Figure 6.3.6

4. Determine which of the following are equivalence relations and/or partial ordering relations for the given sets:

   (a) $A = \{\text{lines in the plane}\}$; $x\, r\, y$ if and only if x is parallel to y.

   (b) $A = \mathbb{R}$; $x\, r\, y$ if and only if $| x - y | \leq 7$.

5. Consider the following relation on $\{1, 2, 3, 4, 5, 6\}$. $r = \{(i, j) : | i - j | = 2\}$.

   (a) Is r reflexive?

   (b) Is r symmetric?

   (c) Is r transitive?

(d) Draw a graph of r.

6. For the set of cities on a map, consider the relation $x\,r\,y$ if and only if city x is connected by a road to city y. A city is considered to be connected to itself, and two cities are connected even though there are cities on the road between them. Is this an equivalence relation or a partial ordering? Explain.

7. Let $A = \{0, 1, 2, 3\}$ and let

$$r = \{(0, 0), (1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (3, 2), (2, 3), (3, 1), (1, 3)\}.$$

(a) Show that r is an equivalence relation on A.

(b) Let $a \in A$ and define $c(a) = \{b \in A \mid a\,r\,b\}$. c(a) is called the *equivalence class of a under r*. Find $c(a)$ for each element $a \in A$.

(c) Show that $\{c(a) \mid a \in A\}$ forms a partition of A for this set A.

(d) Let r be an equivalence relation on an arbitrary set A. Prove that the set of all equivalence classes under r constitutes a partition of A.

8. Define r on the power set of $\{1, 2, 3\}$ by $A\,r\,B \Leftrightarrow |A| = |B|$. Prove that r is an equivalence relation. What are the equivalence classes under r?

9. Consider the following relations on $\mathbb{Z}_8 = \{0, 1, \ldots, 7\}$. Which are equivalence relations? For the equivalence relations, list the equivalence classes.

(a) $a\,r\,b$ iff the English spellings of a and b begin with the same letter.

(b) $a\,s\,b$ iff $a - b$ is a positive integer.

(c) $a\,t\,b$ iff $a - b$ is an even integer.

10. (a) Prove that conguence modulo m, introduced in Example 6.3.4, is a transitive.

(b) What are the equivalence classes under conguence modulo 2?

(c) What are the equivalence classes under conguence modulo 10?

B Exercises

11. In this exercise, we prove that implication is a partial ordering. Let A be any set of propositions.

(a) Verify that $q \to q$ is a tautology, thereby showing that $\Rightarrow$ is a reflexive relation on A.

(b) Prove that $\Rightarrow$ is antisymmetric on A. Note: we do not use = when speaking of propositions, but rather equivalence, $\Leftrightarrow$.

(c) Prove that $\Rightarrow$ is transitive on A.

(d) Given that q_i is the proposition $n < i$ on $\mathbb{N}$, draw the Hasse diagram for the relation $\Rightarrow$ on $\{q_1, q_2, q_3, \ldots\}$.

C Exercise

12. Let $S = \{1, 2, 3, 4, 5, 6, 7\}$ be a poset $(S, \leq)$ with the Hasse diagram shown in Figure 6.3.7. Another relation $r \subseteq S\times S$ is defined as follows: $(x, y) \in r$ if and only if there exists $z \in S$ such that $z < x$ and $z < y$ in the poset $(S, \leq)$.

(a) Prove that r is reflexive.

(b) Prove that r is symmetric.

(c) A compatible with respect to relation r is any subset Q of set S such that $x \in Q$ and $y \in Q \Rightarrow (x, y) \in r$. A compatible g is a maximal compatible if Q is not a proper subset of another compatible. Give all maximal compatibles with respect to relation r defined above.

(d) Discuss a characterization of the set of maximal compatibles for relation *r* when (S, $\leq$) is a general finite poset. What conditions, if any, on a general finite poset (S, $\leq$) will make r an equivalence relation?

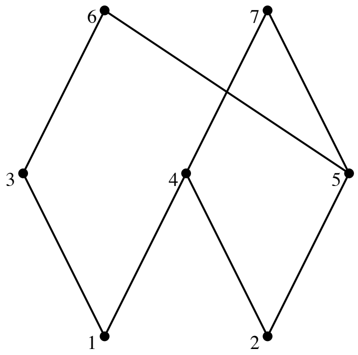


FIGURE 6.3.7

6.4 Matrices of Relations

We have discussed two of the many possible ways of representing a relation, namely as a digraph or as a set of ordered pairs. In this section we will discuss the representation of relations by matrices and some of its applications.

Definition: Adjacency Matrix. *Let $A = \{a_1, a_2, \ldots, a_m\}$ and $B = \{b_1, b_2, \ldots, b_n\}$ be finite sets of cardinality m and n, respectively. Let r be a relation from A into B. Then r can be represented by the $m \times n$ matrix R defined by*

$$R_{ij} = \begin{cases} 1 & \text{if } a_i \, r \, b_j \\ 0 & \text{otherwise} \end{cases}$$

R is called the adjacency matrix (or the Boolean matrix, or the relation matrix) of r.

Example 6.4.1. Let $A = \{2, 5, 6\}$ and let r be the relation $\{(2, 2), (2, 5), (5, 6), (6, 6)\}$ on A. Since r is a relation from A into the same set A (the B of the definition), we have $a_1 = 2, a_2 = 5$, and $a_3 = 6$, and $b_1 = 2, b_2 = 5$, and $b_3 = 6$. Next, since

$2 \, r \, 2$, we have $R_{11} = 1$;

$2 \, r \, 5$, we have $R_{12} = 1$;

$5 \, r \, 6$, we have $R_{23} = 1$; and

$6 \, r \, 6$, we have $R_{33} = 1$;

All other entries of R are zero, so

$$R = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

From the definition of r and of composition, we note that

$$r^2 = \{(2, 2)(2, 5)(2, 6)(5, 6)(6, 6)\},$$

The adjacency matrix of r^2 is

$$R^2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

We do not write R^2 only for notational purposes. In fact, R^2 can be obtained from the matrix product $R\,R$; however, we must use a slightly different form of arithmetic.

Definition: Boolean Arithmetic. *Boolean arithmetic is the arithmetic defined on {0, 1} using Boolean addition and Boolean multiplication, defined as:*

$$0 + 0 = 0 \qquad 0 + 1 = 1 + 0 = 1 \qquad 1 + 1 = 1$$

$$0 \cdot 0 = 0 \qquad 0 \cdot 1 = 1 \cdot 0 = 0 \qquad 1 \cdot 1 = 1.$$

Notice that from Chapter 3, this is the "arithmetic of logic," where + replaces "or" and · replaces "and."

Example 6.4.2.

$$\text{If} \quad R = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad S = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

$$\text{Then using Boolean arithmetic,} \quad R\;S = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad S\,R = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Theorem 6.4.1. *Let A_1, A_2, and A_3 be finite sets where r_1 is a relation from A_1 into A_2 and r_2 is a relation from A_2 into A_3. If R_1 and R_2 are the adjacency matrices of r_1 and r_2 , respectively, then the product $R_1 R_2$ using Boolean arithmetic is the adjacency matrix of the composition $r_1 r_2$.*

Remark: A convenient help in constructing the adjacency matrix of a relation from a set A into a set B is to write the elements from A in a column preceding the first column of the adjacency matrix, and the elements of B in a row above the first row. Initially, R in Example 6.4.1 would be

$$\begin{array}{c} \\ 2 \\ 5 \\ 6 \end{array}\begin{array}{c} \begin{array}{ccc} 2 & 5 & 6 \end{array} \\ \left(\begin{array}{ccc} \ & \ & \ \\ \ & \ & \ \\ \ & \ & \ \end{array}\right) \end{array}$$

and R_{ij} is 1 if and only if $\left(a_i, b_j\right) \in r$. So that, since the pair $(2, 5) \in r$, the entry of R corresponding to the row labeled 2 and the column labeled 5 in the matrix is a 1.

Example 6.4.3, This final example gives an insight into how relational data base programs can systematically answer questions pertaining to large masses of information. Matrices R (on the left) and S (on the right) define the relations r and s where $a\,r\,b$ if software a can be run with operating system b, and $b\,s\,c$ if operating system b can run on computer c.

$$\begin{array}{c} \\ \text{P1} \\ \text{P2} \\ \text{P3} \\ \text{P4} \end{array}\begin{array}{c} \begin{array}{cccc} \text{OS1} & \text{OS2} & \text{OS3} & \text{OS4} \end{array} \\ \left(\begin{array}{cccc} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right) \end{array} \qquad \begin{array}{c} \\ \text{OS1} \\ \text{OS2} \\ \text{OS3} \\ \text{OS4} \end{array}\begin{array}{c} \begin{array}{ccc} \text{C1} & \text{C2} & \text{C3} \end{array} \\ \left(\begin{array}{ccc} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{array}\right) \end{array}$$

Although the relation between the software and computers is not implicit from the data given, we can easily compute this information. The matrix of rs is RS, which is

$$\begin{array}{c} \\ \text{P1} \\ \text{P2} \\ \text{P3} \\ \text{P4} \end{array}\begin{array}{c} \begin{array}{ccc} \text{C1} & \text{C2} & \text{C3} \end{array} \\ \left(\begin{array}{ccc} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{array}\right) \end{array}$$

This matrix tells us at a glance which software will run on the computers listed. In this case, all software will run on all computers with the exception of program P2, which will not run on the computer C3, and program P4, which will not run on the computer C1.

EXERCISES FOR SECTION 6.4

A Exercises

1. Let $A_1 = \{1, 2, 3, 4\}$, $A_2 = \{4, 5, 6\}$, and $A_3 = \{6, 7, 8\}$. Let r_1 be the relation from A_1 into A_2 defined by $r_1 = \{(x, y) \mid y - x = 2\}$, and let r_2 be the relation from A_2 into A_3 defined by $r_2 = \{(x, y) \mid y - x = 1\}$.

(a) Determine the adjacency matrices of r_1 and r_2 .

(b) Use the definition of composition to find $r_1 r_2$.

(c) Verify the result in part by finding the product of the adjacency matrices of r_1 and r_2.

2. (a) Determine the adjacency matrix of each relation given via the digraphs in Exercise 3 of Section 6.3.

(b) Using the matrices found in part (a) above, find r^2 of each relation in Exercise 3 of Section 6.3.

(c) Find the digraph of r^2 directly from the given digraph and compare your results with those of part (b).

3. Suppose that the matrices in Example 6.4.2 are relations on $\{1, 2, 3, 4\}$. What relations do R and S describe?

4. Let D be the set of weekdays, Monday through Friday, let W be a set of employees $\{1, 2, 3\}$ of a tutoring center, and let V be a set of computer languages for which tutoring is offered, {A(PL), B(asic), C(++), J(ava), L(isp), P(ython)}. We define s (schedule) from D into W by $d\,s\,w$ if w is scheduled to work on day d. We also define r from W into V by $w\,r\,l$ if w can tutor students in language l. If s and r are defined by matrices

$$S = \begin{array}{c} \\ M \\ T \\ W \\ Th \\ F \end{array}\begin{array}{c} \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \left(\begin{array}{ccc} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{array}\right) \end{array} \quad \text{and } R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array}\begin{array}{c} \begin{array}{cccccc} A & B & C & J & L & P \end{array} \\ \left(\begin{array}{cccccc} 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{array}\right) \end{array}$$

(a) compute $S\,R$ using Boolean arithmetic and give an interpretation of the relation it defines, and

(b) compute $S\,R$ using regular arithmetic and give an interpretation of the result describes.

5. How many different reflexive, symmetric relations are there on a set with three elements? (Hint: Consider the possible matrices.)

6. Let $A = \{a, b, c, d\}$. Let r be the relation on A with adjacency matrix

$$\begin{array}{c|cccc} & a & b & c & d \\ a & 1 & 0 & 0 & 0 \\ b & 0 & 1 & 0 & 0 \\ c & 1 & 1 & 1 & 0 \\ c & 0 & 1 & 0 & 1 \end{array}$$

(a) Explain why r is a partial ordering on A.

(b) Draw its Hasse diagram.

7. Define relations p and q on $\{1, 2, 3, 4\}$ by $p = \{(a, b) : |a - b| = 1\}$ and $q = \{(a, b) \mid a - b \text{ is even}\}$

(a) Represent p and q as both graphs and matrices.

(b) Determine $p\,q$, p^2, and q^2; and represent them clearly in any way.

B Exercises

8. (a) Prove that if r is a transitive relation on a set A, then $r^2 \subseteq r$.

(b) Find an example of a transitive relation for which $r^2 \neq r$.

9. We define $\leq$ on the set of all $n \times n$ relation matrices by the rule that if R and S are any two $n \times n$ relation matrices, $R \leq S$ if and only if $R_{\text{ij}} \leq S_{\text{ij}}$ for all $1 \leq i, j \leq n$.

(a) Prove that $\leq$ is a partial ordering on all $n \times n$ relation matrices.

(b) Prove that $R \leq S \Rightarrow R^2 \leq S^2$, but the converse is not true.

(c) If R and S are matrices of equivalence relations and $R \leq S$, how are the equivalence classes defined by R related to the equivalence classes defined by S?

6.5 Closure Operations on Relations

In Section 6.1, we studied relations and one important operation on relations, namely composition. This operation enables us to generate new relations from previously known relations. In Section 6.3, we discussed some key properties of relations. We now wish to consider the situation of constructing a new relation r^+ from a previously known relation r where, first, r^+ contains r and, second, r^+ satisfies the transitive property.

Consider a telephone network in which the main office a is connected to, and can communicate to, individuals b and c. Both b and c can communicate to another person, d; however, the main office cannot communicate with d. Assume communication is only one way, as indicated. This situation can be described by the relation $r = \{(a, b), (a, c), (b, d), (c, d)\}$. We would like to change the system so that the main office a can communicate with person d and still maintain the previous system. We, of course, want the most economical system.

This can be rephrased as follows; Find the smallest relation r^+ which contains r as a subset and which is transitive; $r^+ = \{(a, b), (a, c), (b, d), (c, d), (a, d)\}$.

Definition: Transitive Closure. *Let A be a set and r be a relation on A. The transitive closure of r, denoted by r^+, is the smallest transitive relation that contains r as a subset.*

Example 6.5.1. Let $A = \{1, 2, 3, 4\}$, and let $\mathcal{S} = \{(1, 2), (2, 3), (3, 4)\}$ be a relation on A. This relation is called the successor relation on A since each element is related to its successor. How do we compute $\mathcal{S}^+$? By inspection we note that $(1, 3)$ must be in $\mathcal{S}^+$. Let's analyze why. This is so because $(1, 2) \in \mathcal{S}$ and $(2, 3) \in \mathcal{S}$, and the transitive property forces $(1, 3)$ to be in $\mathcal{S}^+$.

In general, it follows that if $(a, b) \in \mathcal{S}$ and $(b, c) \in S$, then $(a, c) \in \mathcal{S} +$. This condition is exactly the membership requirement for the pair (a, c) to be in the composition $\mathcal{S}\mathcal{S} = \mathcal{S}^2$. So every element in $\mathcal{S}^2$ must be an element in $\mathcal{S}^+$. So far, $\mathcal{S}^+$ contains at least $\mathcal{S} \cup \mathcal{S}^2$. In particular, for this example, since $\mathcal{S} = \{(1, 2), (2, 3), (3, 4)\}$ and $\mathcal{S}^2 = \{(1, 3), (2, 4)\}$, we have

$$\mathcal{S} \cup \mathcal{S}^2 = \{(1, 2), (2, 3), (3, 4), (1, 3), (2, 4)\}.$$

Is the relation $\mathcal{S} \cup \mathcal{S}^2$ transitive? Again, by inspection, $(1, 4)$ is not an element of $\mathcal{S} \cup \mathcal{S}^2$, but it must be an element of $\mathcal{S}^+$ since (1, 3) and $(3, 4)$ are required to be in $\mathcal{S}^+$. From above, $(1, 3) \in \mathcal{S}^2$ and $(3, 4) \in \mathcal{S}$. Therefore, the composite $\mathcal{S}^2\mathcal{S} = \mathcal{S}^3$ produces $(1, 4)$. This shows that $\mathcal{S}^3 \subseteq \mathcal{S}^+$. This process must be continued until the resulting relation is transitive. If A is finite, as is true in this example, the transitive closure will be obtained in a finite number of steps. For this example,

$$\mathcal{S}^+ = \mathcal{S} \cup \mathcal{S}^2 \cup \mathcal{S}^3 = \{(1, 2), (2, 3), (3, 4), (1, 3), (2, 4), (1, 4)\} .$$

Theorem 6.5.1. *If r is a relation on a set A and $|A| = n$, then the transitive closure of r is the union of the first n powers of r. That is,*

$$r^+ = r \cup r^2 \cup r^3 \cup \cdots \cup r^n.$$

Let's now consider the matrix analogue of the transitive closure.

Example 6.5.2. Consider the relation

$$r = \{(1, 4), (2, 1), (2, 2), (2, 3), (3, 2), (4, 3), (4, 5), (5, 1)\}$$

on the set $A = \{1, 2, 3, 4, 5\}$. The matrix of r is

$$R = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Recall that $r^2, r^3, \ldots$ can be determined through computing the matrix powers R^2, R^3, …. Here,

$$R^2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \qquad R^3 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix},$$

$$R^4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}, \text{ and } \qquad R^5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix},$$

How do we relate $\bigcup_{i=1}^{5} r^i$ to the powers of R?

Theorem 6.5.2. *Let r be a relation on a finite set and let R^+ be the matrix of r^+ , the transitive closure of r. Then $R^+ = R + R^2 + \cdots + R^n$, using Boolean arithmetic.*

Using this theorem, we find R^+ is the 5×5 matrix consisting of all $1's$, thus, r^+ is all of $A \times A$.

WARSHALL'S ALGORITHM

Let r be a relation on the set $\{1, 2, \ldots, n\}$ with relation matrix R. The matrix of the transitive closure R^+ , can be computed by the equation $R^+ = R + R^2 + \cdots + R^n$. By using ordinary polynomial evaluation methods, you can compute R^+ with $n - 1$ matrix multiplications:

$$R^+ = R(I + R(I + (\cdots R(I + R)\cdots))).$$

For example, if $n = 3, R = R(I + R(I + R))$.

We can make use of the fact that if T is a relation matrix, $T + T = T$ due to the fact that $1 + 1 = 1$ in Boolean arithmetic. Let $S_k = R + R^2 + \cdots + R^k$. Then

$$R = S_1$$

$$S_1\,(I + S_1) = R\,(I + R) = R + R^2 = S_2$$

$$\begin{aligned} S_2\,(I + S_2) &= (R + R^2)\,(I + R + R^2) \\ &= \left(R + R^2\right) + \left(R^2 + R^3\right) + (R^3 + R^4) \\ &= R + R^2 + R^3 + R^4 = S_4 \end{aligned}$$

Similarly,

$$S_4(I + S_4) = S_8$$

etc..

Notice how each matrix multiplication doubles the number of terms that have been added to the sum that you currently have computed. In algorithmic form, we can compute R^2 as follows.

Algorithm 6.5.1: Transitive Closure Algorithm 1. Let R be a known relation matrix and let R^+ be its transitive closure matrix, which is to be computed.

```
1.0. $T := R$
2.0. Repeat
        2.1  $S := T$
        2.2  $T := S\,(I + S)$   // using Boolean arithmetic
     Until $T = S$
3.0. Terminate with $T = R^+$.
```

Notes:

(a) Often the higher-powered terms in S_n do not contribute anything to R^+. When the condition $T = S$ becomes true in Step 2, this is an indication that no higher-powered terms are needed.

(b) To compute R^+ using this algorithm, you need to perform no more than $\lceil \log_2 n \rceil$ matrix multiplications, where $\lceil x \rceil$ is the least integer that is greater than or equal to x. For example, if r is a relation on 25 elements, no more than $\lceil \log_2 25 \rceil = 5$ matrix multiplications are needed.

A second algorithm, Warshall's Algorithm, reduces computation time to the time that it takes to perform one matrix multiplication.

Algorithm 6.5.2; Warshall's Algorithm. Let R be a known relation matrix and let R^+ be its transitive closure matrix, which is to be computed.

```
1.0  $T := R$
2.0  FOR $k$ : = 1 to $n$ DO
          FOR $i$ : = 1 to $n$ DO
              FOR $j$ := 1 to $n$ DO
                  $T[i, j] := T[i, j] + T[i, k] \cdot T[k, j]$
3.0 Terminate with $T = R^+$.
```

EXERCISES FOR SECTION 6.5

A Exercises

1. Let A and $\mathcal{S}$ be as in Example 6.5.1. Compute $\mathcal{S}^+$ as in Example 6.5.2. Verify your results by checking against the relation $\mathcal{S}^+$ obtained in Example 6.5.1.

2. Let A and r be as in Example 6.5.2. Compute the relation r^+ as in Example 6.5.1. Verify your results.

3. (a) Draw digraphs of the relations $\mathcal{S}$, $\mathcal{S}^2$, $\mathcal{S}^3$, and $\mathcal{S}^+$ of Example 6.5.1.

(b) Verify that in terms of the graph of $\mathcal{S}$, $a\, \mathcal{S}^+\, b$ if and only if b is reachable from a along a path of any finite nonzero length.

4. Let r be the relation represented by the digraph in Figure 6.5,1.

(a) Find r^+ .

(b) Determine the digraph of r^+ directly from the digraph of r.

(c) Verify your result in part (b) by computing the digraph from your result in part (a).

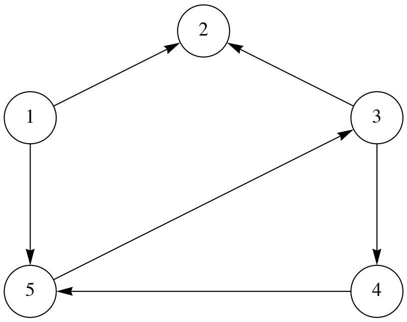


FIGURE 6.5.1

5. (a) Define reflexive closure and symmetric closure by imitating the definition of transitive closure.

(b) Use your definitions to compute the reflexive and symmetric closures of Examples 6.5.1 and 6.5.2.

(c) What are the transitive reflexive closures of these examples?

(d) Convince yourself that the reflexive closure of the relation < on the set of positive integers $\mathbb{P}$ is ≤.

6. What common relations on $\mathbb{Z}$ are the transitive closures of the following relations?

(a) $a\, S\, b$ if and only if $a + 1 = b$.

(b) $a\, R\, b$ if and only if $| a - b | = 2$.

B Exercise

7. (a) Let A be any set and r a relation on A, prove that $(r^+)^+ = r^+$.

(b) Is the transitive closure of a symmetric relation always both symmetric and reflexive? Explain.

SUPPLEMENTARY EXERCISES FOR CHAPTER 6

Section 6.1

1. Give an example to illustrate how the relation "is a grandparent of" is a composition of the relation "is a parent of" on people.

2. Three students, Melissa, John, and Ted, would like to set up a tutorial program in the languages Pascal, FORTRAN, and COBOL. Melissa is proficient in all three languages, John in Pascal and FORTRAN, and Ted in just FORTRAN.

(a) Let S = {three students}, L = {three Languages}, and let p be the relation "is proficient in the language of". Describe this relation as a set of ordered pairs and illustrate the relation by a diagram similar to that of Figure 6.1.1.

(b) Two P.C.s are available for tutoring purposes; one has software for Pascal and FORTRAN, and the second only for Pascal. Describe by a composite relation which student can tutor on each machine. Illustrate this composite relationship.

Section 6.2

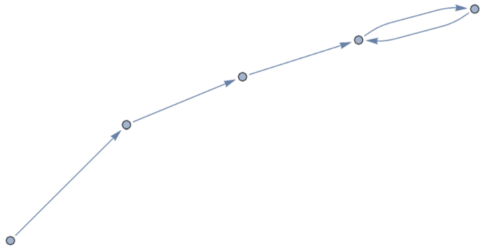
3. Let $A = \{-1, 0, 1, 2\}$. List the ordered pairs and draw the digraphs of each of the following relations on A.

(a) $r = \{(x, y) \mid y = x + 1\}$
(b) $s = \{(x, y) \mid x^2 = y^2\}$
(c) $t = \{(x, y) \mid x \neq y\}$

4. List the ordered pairs and draw the digraph of the relation s^2 for the relation s of Exercise 2, Section 6.2.

5. In Figure 6.2, 1, assume the nodes stand for four separate cities where a manufacturer has warehouses, while the arrows represent one-way streets. Where should the manufacturer place his main office? Where is the least desirable location? How can we interpret the arrows in both directions between nodes 1 and 2?

6. Suppose we selected a set of points, $\mathcal{P}$, on the cartesian plane such that the distances between them are all different. Consider the relation c on $\mathcal{P}$ defined by $P_1 \, c \, P_2$ if and only if the closest other point in $\mathcal{P}$ to P_1 is P_2. For example, with the set $\left\{\left(k, \sqrt{k}\right) \mid k = 0, 1, 2, 3, 4\right\}$, the graph of c would look like this, where we locate the vertices in our graph at the actual points in $\mathcal{P}$.



(a) In general, how many pairs are there in c?

(b) Look at various possible configurations of c's graph of sets of five points. What other possible configurations can you find? Are there any general observations that you can make?

Section 6.3

7. In Figure 6.3.2 (vii), interpret the four nodes as representing people, and an arrow from one node to another as "being friendly toward". Note that some friendships are not mutual.

(a) Is there any individual in this group unfriendly to everyone else?
(b) If this group were a committee, who is most likely to be the chairperson; that is, who is friendly toward the most people?
(c) If an arrow from one vertex to itself is interpreted as "great personality," does your answer to part b still hold?
(d) The four people are to be seated at a round table. A person is to be seated between two people only if he is friendly toward both of them. Does a seating arrangement exist? Is there more than one?

8. Let $A = \{a, b, c, d, e\}$ and let r, s, and t be the following relations on A:

$r = \{(a, a), (a, b), (b, b), (b, c), (c, c), (c, d), (d, d), (d, e), (e, e), (e, a)\}$
$s = \{(a, a), (a, b), (a, d), (b, a), (b, b), (b, d), (c, c), (d, a), (d, b), (d, d), (e, e)\}$
$t = \{(a, a), (a, b), (b, b), (c, b), (c, c), (d, d), (e, a), (e, b), (e, c), (e, d), (e, e)\}$

(a) Which relation is a partial ordering? Draw its Hasse diagram.
(b) Which relation is an equivalence relation? List its equivalence classes.

9. Demonstrate that the relation "living in the same house" on the set of people in a given city is an equivalence relation. State the necessary assumption for this to be the case.

10. Let $A = \{00, 01, 10, 11\}$, the set of strings of 0s and 1s with length two. Given r and s defined by

$x\, r\, y \Leftrightarrow x$ and y differ in exactly one position (for example $01\, r\, 11$, but not $10\, r\, 01$), and
$x\, s\, y \Leftrightarrow x$ and y have the same number of 0s.

(a) Draw a directed graph of r.
(b) Which of the adjectives, reflexive, symmetric, antisymmetric, and transitive, describe r? Explain your answers.
(c) Which of the adjectives, reflexive, symmetric, antisymmetric, and transitive, describe s?
(d) Describe with a directed graph the relation rs.

11. Determine whether the following relations are partial orderings and/or equivalence relations on the given set:

(a) C = {students in this class}; $x\, r\, y$ iff x and y have the same grade point average.
(b) C = {students in this class}; $x\, s\, y$ iff x is taller than y,
(c) Rephrase (slightly) the relation in part b so it is a partial ordering relation.

12. Let $A = \{a, b, c, d\}$. Draw the graph of a relation where the relation is:

(a) reflexive, symmetric, but not transitive.
(b) transitive, but not symmetric and not reflexive.
(c) both an equivalence relation and a partial ordering.

Section 6.4

13. How many symmetric relations can there be on a four-element set? Hint: Think of the possible relation matrices.

14. Let $A = \{1, 2, 3, 4, 5, 6\}$ and let $p = \{(i, j) \mid i \text{ divides } j\}$ be a relation on A.

(a) List the elements in p.
(b) Determine the relation matrix of p.
(c) Construct the digraph and the Hasse diagram of p.

15. Let $A = \{a, b, c\}$. The following matrices describe relations on A:

$$\text{(i)} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{(ii)} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

(a) Draw the graph of the relation.
(b) Describe each relation as a set of ordered pairs.
(c) Compute r^2 for each relation r.

Section 6.5

16. Let the relation s on the set $\{a, b, c, d, e\}$ be given by the matrix

$$\begin{array}{c|ccccc} & a & b & c & d & e \\ \hline a & 0 & 0 & 0 & 0 & 0 \\ b & 1 & 0 & 1 & 0 & 0 \\ c & 0 & 1 & 0 & 0 & 0 \\ d & 0 & 0 & 1 & 0 & 0 \\ e & 1 & 1 & 0 & 0 & 0 \end{array}$$

(a) Draw the digraph of s.
(b) Find the transitive closure of s. Give the adjacency matrix or the digraph or the set of ordered pairs.

17. Consider the relation r on $\{1, 2, 3, 4\}$ whose Boolean matrix is

$$R = \begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 0 & 0 & 1 & 1 \\ 2 & 0 & 1 & 0 & 0 \\ 3 & 0 & 0 & 1 & 0 \\ 4 & 1 & 0 & 0 & 0 \end{array}$$

(a) Draw the graph of r.
(b) Determine whether r is reflexive, symmetric, antisymmetric, and/or transitive. Explain fully.
(c) Find the transitive closure of r and draw the graph of r^+.

18. In a small town a bank (b), school (s), town hall (t), and shopping mall (m) are connected by a series of narrow one-way streets; a street

from the town hall to the bank, one from the bank to the school, one from the school to the shopping mall, and one from the shopping mall to the town hall.

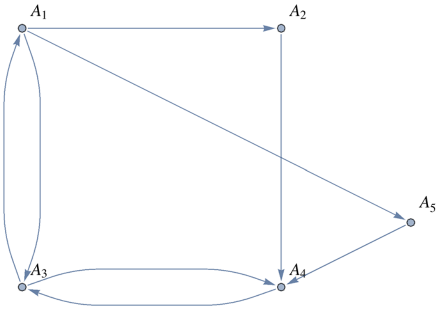
(a) Draw a digraph of this system of roads.

(b) Find the matrix representation of the digraph in part a.

(c) Assuming that the given streets cannot be widened, assist the mayor in planning the construction of new roads to increase traffic flow. Assume that if there is a one-way street from point *a* to *b* and one from point *b* to *c*, there should be one from point *a* to *c*.

(d) If you have not done so yet, draw the matrix representation and the graph of your answer to part c and interpret the results for the mayor.

19. The ambassadors of four countries are to meet with the ambassador of the United States (A_1) to discuss world problems. Some countries are friendly to each other, some are not, and in certain situations the friendship is one-way. The U.S. ambassador's daughter (who obviously took a discrete structures course) assists her father in diagnosing this complex situation and, using the relation "is friendly toward," has come up with the following digraph.

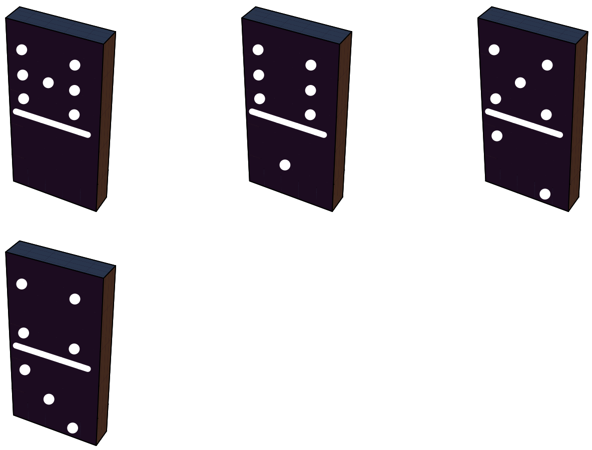


(a) Is there any person friendly to no one?

(b) Who should be the chairman of this committee; that is, who is friendly to most people?

(c) The U.S. ambassador would like to graph all friendships that can be developed through intermediaries on the committee. That is, if person *a* is friendly toward person *b* and person *b* is friendly toward person *c*, then *a* can communicate to *c* through *b*. Draw this digraph. Can the U.S. ambassador communicate to every person on the committee through some person(s)? If not, what friendships should he develop to do so?

chapter 7



FUNCTIONS

GOALS

In this chapter we will consider some basic concepts of the relations that are called functions. A large variety of mathematical ideas and applications can be more completely understood when expressed through the function concept.

7.1 Definition of a Function and Notation

Definition: Function. *A function from a set A into a set B is a relation from A into B such that each element of A is related to exactly one element of the set B. The set A is called the* ***domain*** *of the function and the set B is called the* ***codomain***.

The reader should note that a function f is a relation from A into B with two important restrictions:

1. Each element in the set A, the domain of f, must be related to some element of B, the codomain.

2. The phrase "is related to exactly one element of the set B" means that if $(a, b) \in f$ and $(a, c) \in f$, then $b = c$.

Example 7.1.1. Let $A = \{-2, -1, 0, 1, 2\}$ and $B = \{0, 1, 2, 3, 4\}$, and if $s = \{(-2, 4), (-1, 1), (0, 0), (1, 1), (2, 4)\}$, then s is a function from A into B.

Example 7.1.2. Let $\mathbb{R}$ be the real numbers. Then $L = \{(x, 3x) \mid x \in \mathbb{R}\}$ is a function from $\mathbb{R}$ into $\mathbb{R}$, or, more simply, L is a function on $\mathbb{R}$.

We will use a different system of notation for functions than the one we used for relations. If f is a function from the set A into the set B, we will write $f : A \to B$.

The reader is probably more familiar with the notation for describing functions that is used in basic algebra or calculus courses. For example, $y = \frac{1}{x}$ or $f(x) = \frac{1}{x}$ both define the function $\left\{\left(x, \frac{1}{x}\right) \middle| x \in \mathbb{R}, x \neq 0\right\}$. Here the domain was assumed to be those elements of $\mathbb{R}$ whose substitutions for x make sense, the nonzero real numbers, and the codomain was assumed to be $\mathbb{R}$. In most cases, we will make a point of listing the domain and codomain in addition to describing what the function does in order to define a function.

The terms mapping, map, and transformation are also used for functions.

One way to imagine a function and what it does is to think of it as a machine. The machine could be mechanical, electronic, hydraulic, or abstract. Imagine that the machine only accepts certain objects as raw materials or input. The possible raw materials make up the domain. Given some input, the machine produces a finished product that depends on the input. The possible finished products that we imagine could come out of this process make up the codomain.

Example 7.13. f: $\mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is an alternate description of $f = \{(x,\ x^2) \mid x \in \mathbb{R}\}$.

Definition: Image of an Element. *Let $f : A \to B$, (read "let f be a function from the set A into the set B"). If $a \in A$, then $f(a)$ is used to denote that element of B to which a is related. $f(a)$ is called the image of a, or, more precisely, the image of a under f. We write $f(a) = b$ to indicate that the image of a is b.*

In Example 7.1.3, the image of 2 under *f* is 4; that is, $f(2) = 4$. In Example 7.1.1, the image of -1 under *s* is 1; that is, $s(-1) = 1$.

Definition: Range of a Function. *The range of a function is the set of images of its domain. If $f{:}X \to Y$, then the range of f is denoted $f(X)$, and*

$$\begin{aligned} f(X) &= \{f(a) \mid a \in X\} \qquad . \\ &= \{b \in Y \mid \exists\, a \in X \text{ such that } f(a) = b\} \end{aligned}$$

Note that the range of a function is a subset of its codomain. $f(X)$ is also read as "the image of the set *X* under the function *f*" or simply "the image of *f*."

In Example 7.1.1, $s(A) = \{0,\ 1,\ 4\}$. Notice that 2 and 3 are not images of any element of *A*. In addition, note that both 1 and 4 are related to more than one element of the domain $s(1) = s(-1) = 1$ and $s(2) = s(-2) = 4$. This does not violates the definition of a function. Go back and read the definition if this isn't clear to you.

In Example 7.1.2, the range of *L* is equal to its codomain, $\mathbb{R}$. If *b* is any real number, we can demonstrate that it belongs to L($\mathbb{R}$) by finding a real number *x* for which $L(x) = b$. By the definition of *L*, $L(x) = 3x$, which leads us to the equation $3x = b$. This equation always has a solution, $\frac{b}{3}$; thus $L(\mathbb{R}) = \mathbb{R}$.

The formula that we used to describe image of a real number under *L*, $L(x) = 3x$, is preferred over the set notation for *L* due to its brevity. Any time a function can be described with a rule or formula, we will use this form of description. In Example 7.1.1, the image of each element of *A* is its square. To describe that fact, we write $s(a) = a^2$ $(a \in A)$, or $S : A \to B$ defined by $S(a) = a^2$.

There are many ways that a function can be described. The complexity of the function often dictates its representation.

Example 7.1.4. Suppose a survey of 1,000 persons is done asking how many hours of television each watches per day. Consider the function $W : \{0,\ 1,\ \ldots,\ 24\} \to \{0, 1, 2, \ldots, 1000\}$ defined by

$$W(t) = \text{number of persons who gave a response of } t \text{ hours}.$$

This function will probably have no formula such as the ones for s and L above. Besides listing the data in a table, a bar graph might be a good way to represent *W*.

Example 7.1.5. Consider the function $m : \mathbb{P} \to \mathbb{Q}$ defined by the set

$$m = \{(1,\ 1),\ (2,\ 1/2),\ (3,\ 9),\ (4,\ 1/4),\ (5,\ 25),\ \ldots\}.$$

No simple single formula could describe *m*, but if we assume that the pattern given continues, we can write

$$m(x) = \begin{cases} x^2 & \text{if } x \text{ is odd} \\ 1/x & \text{if } x \text{ is even} \end{cases}$$

FUNCTIONS OF TWO VARIABLES

If the domain of a function is the Cartesian product of two sets, then our notation and terminology is changed slightly. For example, consider the function $C : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $C((n_1, n_2)) = n_1^2 + n_2^2 - n_1 n_2 + 10$. For this function, we would drop one set of parentheses and write $C(4,\ 2) = 22$, not $C((4,\ 2)) = 22$. We call *C* a function of two variables. From one point of view, this function is no different from any others that we have seen. The elements of the domain happen to be slightly more complicated. On the other hand, we can look at the individual components of the ordered pairs as being separate. If we interpret *C* as giving us the cost of producing quantities of two products, we can imagine varying n_1 while n_2 is fixed, or vice versa.

Mathematica Note

There are several ways to define a function in *Mathematica*. One way is using a **`Function`** expression. For example the function $f : \mathbb{Z} \to \mathbb{Z}$, where $f(x) = x^2$ can be defined by evaluating the expression

$$\mathbf{f = Function}\left[\mathbf{x,\ x^2}\right]$$

$$x \longmapsto x^2$$

Then we can compute the image of various numbers. Since *Mathematica* isn't a typed programming language the concept of a domain doesn't apply unless you specify a bit more structure. As it stands we can take the image of numbers, strings, matrices, or symbols, among other things:

$$\left\{\mathbf{f[-5],\ f[2.5],\ f[\text{"Hello"}],\ f}\left[\begin{pmatrix} \mathbf{1} & \mathbf{2} \\ \mathbf{3} & \mathbf{-1} \end{pmatrix}\right]\mathbf{,\ f[\theta]}\right\}$$

$$\left\{25,\ 6.25,\ \text{Hello}^2,\ \begin{pmatrix} 1 & 4 \\ 9 & 1 \end{pmatrix},\ \theta^2\right\}$$

Notice the syntax of *Mathematica* is to use square brackets such as **`f[x]`** instead of parentheses, **`f(x)`** for computing images under *f*. Notice that the square of the matrix isn't the matrix product, rather it is simpler componentwise product.

If we want to restrict the possible inputs to a function that implements *f*, we might use the following alternate way of defining a function.

$$\texttt{fa[x\_?IntegerQ] := x}^{2}$$

If the "**`?IntegerQ`**" had been left out, **`fa`** and **`f`** would be identical, but as it is defined, the formula for **`fa`** only applies to integers. This makes **`fa`** more similar to *f*. We get what we expect when we ask for the image of an integer:

```
{fa[-5], fa[25!]}
```

{25, 240 597 637 008 332 048 087 335 626 345 604 448 256 000 000 000 000}

If we ask for the image of anything that isn't an integer, the expression is left unevaluated.

$$\left\{\texttt{fa[2.5], fa["Hello"], fa}\left[\begin{pmatrix}1 & 2\\ 3 & -1\end{pmatrix}\right]\texttt{, fa[}\theta\texttt{]}\right\}$$

```
{fa[2.5], fa[Hello], fa[{{1, 2}, {3, -1}}], fa[θ]}
```

It is also possible to program *Mathematica* to issue an error message for these unintended cases.

Sage Note

There are several ways to define a function in Sage. The simplest way to implement *f* is as follows.

```
sage: f(x)=x^2
sage: f
x |--> x^2
 sage : f (4)
16
sage : f (-5.1)
26.0100000000000
```

Sage is built upon the programming language Python, which is a *strongly typed language* and so you can't evaluate expressions such as `f("Hello")`. However a function like `f` above will accept any type of number, so a bit more work is needed to restrict the inputs of f to the integers.

A second way to define a function in Sage is based on Python syntax.

```
sage: def fa(x): return x^2
....:
sage: fa(-4)
16
sage: fa(5.1)
26.0100000000000
```

We close this section with two examples of relations that are not functions.

Example 7.1.6. Let $A = B = \{1, 2, 3\}$ and let $f = \{(1, 2), (2, 3)\}$. Here f is not a function since f does not act on, or "use," all elements of A.

Example 7.1.7. Let $A = B = \{1, 2, 3\}$ and let $g = \{(1, 2), (2, 3), (2, 1), (3, 2)\}$. We note that g acts on all of A. However, g is still not a function since $(2, 3) \in g$ and $(2, 1) \in g$ and the condition on each domain being related to exactly one element of the codomain is violated.

EXERCISES FOR SECTION 7.1

A Exercises

1. Let $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c, d\}$. Determine which of the

following are functions. Explain.

(a) $f \subseteq A \times B$, where $f = \{(1, a), (2, b), (3, c), (4, d)\}$.

(b) $g \subseteq A \times B$, where $g = \{(1, a), (2, a), (3, b), (4, d)\}$.

(c) $h \subseteq A \times B$, where h = $\{(1, a), (2, b), (3, c)\}$.

(d) $k \subseteq A \times B$, where $k = \{(1, a), (2, b), (2, c), (3, a), (4, a)\}$.

(e) $L \subseteq A \times A$, where $L = \{(1,\ 1),\ (2,\ 1),\ (3,\ 1),\ (4,\ 1)\}$.

2. Let A be a set and let S be any subset of A. Let $\chi_S :\ A \to \{0,\ 1\}$ be defined by

$$\chi_S(x) = \begin{cases} 1 & \text{if } x \in S \\ 0 & \text{if } x \notin S \end{cases}$$

The function χ_S, is called the *characteristic function* of S,

(a) If $A = \{a,\ b,\ c\}$ and $S = \{a,\ b\}$, list the element of χ_S .

(b) If $A = \{a,\ b,\ c,\ d,\ e\}$ and $S = \{a,\ c,\ e\}$, , list the element of χ_S.

(c) If $A = \{a,\ b,\ c\}$, what are $\chi_\emptyset$ and χ_A.

3. Find the ranges of each of the relations that are functions in Exercise 1.

4. Find the ranges of the following functions on $\mathbb{Z}$:

(a) $g = \{(x,\ 4x + 1) \mid x \in \mathbb{Z}\}$

(b) $h(x) =$ least integer that is greater than or equal to $\sqrt{\mid x \mid}$.

(c) $P(x) = x + 10$.

B Exercise

5. If $\mid A \mid$ and $\mid B \mid$ are both finite, how many different functions are there from A into B?

6. Let f be a function with domain A and codomain B. Consider the relation $K \subseteq A \times A$ defined on the domain of f by $(x,\ y) \in K$ if and only if $f(x) = f(y)$. The relation K is called *the kernel of f*.

(a) Prove that K is an equivalence relation.

(b) For the specific case of $A = \mathbb{Z}$, where $\mathbb{Z}$ is the set of integers, let $f :\ \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = x^2$. Describe the equivalence classes of the kernel for this specific function.

7.2 Injective, Surjective, and Bijective Functions

Consider the following functions;

Example 7.2.1. Let $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c, d\}$, and defined $f : A \to B$ by

$$f(1) = a,\ f(2) = b,\ f(3) = c \text{ and } f(4) = d.$$

Example 7.2.2. Let $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c, d\}$, and defined $g : A \to B$ by

$$g(1) = a\ , g(2) = b,\ g(3) = a \text{ and } g(4) = b.$$

The function in the first example gives us more information about the set B than the second function. Since A clearly has four elements,/tells us that the set B contains at least four elements since each element of the set A is mapped onto one and only one element of the set B, The properties that / has and g does not have are the most basic properties that we look for in a function. The following definitions summarize the basic vocabulary for function properties.

Definition Injective Function: *A function f: A → B is injective if*

$$a, b \in A,\ a \neq b \ \Rightarrow\ f(a) \neq f(b).$$

Notice that the condition for a injective function is equivalent to

$$a,\ b \in A,\ f(a) = f(b) \Rightarrow a = b$$

Injective functions are also called *injections*, or *one-to-one functions*.

Definition Surjective Function *A function f: A → B is surjective if its range, f(A), is equal to its codomian B*

Notice that the condition for a surjective function is equivalent to

For all $b \in B$, there exists $a \in A$ such that $f(a) = b$.

Surjective functions are also called *surjections*, or *onto functions*.

Definition Bijective Function: *A function f: A → B is bijective if it is both injective and surjective.*

Bijective functions are also called *one-to-one, onto functions*.

Example 7.2.3. The function *f* of Example 7.2.1 is bijective. The function *g* of Example 7.2.2 is neither injective nor surjective.

Example 7.2.4. Let $A = \{1, 2, 3\}$ and $B = \{a, b, c, d\}$, and define $f : A \to B$ by $f(1) = b$, $f(2) = c$, and $f(3) = a$. Then *f* is injective but not surjective.

Example 7.2.5. The characteristic function, χ_S in Exercise 2 of Section 7.1, is surjective if *S* is a proper subset of *A*, but never injective if $|A| > 2$.

Example 7.2.6. Let *A* be the set of students who are sitting in a classroom, and let *B* be the set of seats in the classroom, and let *s* be the function which maps each student into the chair he or she is sitting in. When is *s* one to one? When is it onto? Under normal circumstances, *s* would always be one to one since no two different students would be in the same seat. In order for *s* to be onto, we need all seats to be used, so *s* is onto if the classroom is filled to capacity.

Functions can also be used for counting the elements in large finite sets or in infinite sets. Let's say we wished to count the occupants in an auditorium containing 1,500 seats. If each seat is occupied, the answer is obvious, namely 1,500 people. What we have done is to set up a one-to-one correspondence, or bijection, from seats to people. We formalize in a definition.

Definition: Cardinality. *Two sets are said to have the same cardinality if there exists a bijection between them.*

The function *f* in Example 7.2.1 serves to show that the two sets $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c, d\}$ have the same cardinality. Notice in applying the definition of cardinality, we don't actually appear to count either set, we just match up the elements. However, matching the letters in *B* with the number 1, 2, 3, an 4. is precisely how we count the letters.

Definition: Countable Set. *If a set is finite or has the same cardinality as the set of positive integers, it is called a countable set.*

If a set is finite, and its cardinality is *n*, then it has the same cardinality as the set $\{1, 2, 3, \ldots, n\}$.

Example 7.2.7. The alphabet $\{A, B, C, \ldots, Z\}$ has cardinality 26 through the following bijection into the set $\{1, 2, 3, \ldots, 26\}$

$$\begin{array}{cccc} A & B & C & \cdots & Z \\ \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\ 1 & 2 & 3 & \cdots & 26 \end{array}$$

Reminder: $2\mathbb{P} = \{b \in \mathbb{P} \mid b = 2k \text{ for some } k \in \mathbb{P}\}$

Example 7.2.8. The set $2\mathbb{P}$ of even positive integers has the same cardinality as the set $\mathbb{P}$ of positive integers. To prove this, we must find a bijection from $\mathbb{P}$ to $2\mathbb{P}$. Such a function isn't unique, but this one is the simplest: $f : \mathbb{P} \to 2\mathbb{P}$ by $f(m) = 2m$. Two statements must be proven to justify our claim that *f* is a bijection.

(1) f is one-to-one.

Proof: Let $a,\ b \in \mathbb{P}$ and assume that $f(a) = f(b)$. We must prove that $a = b$.

$$f(a) = f(b) \implies 2a = 2b \implies a = b. \quad \blacksquare$$

(2) f is onto.

Proof: Let $b \in 2\mathbb{P}$. We want to show that there exists an element $a \in \mathbb{P}$ such that $f(a) = b$. If $b \in 2\mathbb{P}$, $b = 2k$ for some $k \in \mathbb{P}$ by the definition of $2\mathbb{P}$. So we have $f(k) = 2k = b$. Hence, each element of $2\mathbb{P}$ is the image of some element of $\mathbb{P}$. ■

An even easier way to look at any function with $\mathbb{P}$ as its domain by creating a list of the form $f(1)$, $f(2)$, $f(3)$, …, which is 2, 4, 6, … for the function we've just defined. This infinite list clearly has no duplicate entries and every even positive integer appears in the list eventually.

Bijections with domain $\mathbb{P}$***:*** *A function $f : \mathbb{P} \to A$ is a bijection if the infinite list $f(1)$, $f(2)$, $f(3)$, … contains no duplicates, and every element of A appears on in the list.*

Readers who have studied real analysis should realize that the set of rational numbers is a countable set, while the set of real numbers is not a countable set. See the exercises at the end of this section for an example of such a set.

We close this section with an theorem called the Pigeonhole Principle, which has numerous applications even though it is an obvious, common-sense statement. Never underestimate the importance of simple ideas. The Pigeonhole Principle states that if there are more pigeons than pigeonholes, then two or more pigeons must share the same pigeonhole. A more rigorous mathematical statement of the principle follows.

The Pigeonhole Principle. *Let f be a function from a finite set X onto a finite set Y. If $n \geq 1$ and $|X| > n|Y|$, then there exists an element of Y that is the image of at least $n + 1$ elements of X.*

Example 7.2.9. Assume that a room contains four students with the first names John, James, and Mary. Prove that two students have the same first name. We can visualize a mapping from the set of students to the set of first names; each student has a first name. The pigeonhole principle applies with $n = 1$, and we can conclude that two of the students have the same first name.

EXERCISES FOR SECTION 7.2

A Exercises

1. Determine which of the functions in Exercise 1 of Section 7.1 are one- to-one and which are onto.

2. (a) Determine all bijections from the $\{1,\ 2,\ 3\}$ into $\{a,\ b,\ c\}$.

(b) Determine all bijections from $\{1,\ 2,\ 3\}$ into $\{a,\ b,\ c,\ d\}$.

3. Which of the following are one-to-one, onto, or both?

(a) $f_1 : \mathbb{R} \to \mathbb{R}$ defined by $f_1(x) = x^3 - x$.

(b) $f_2 : \mathbb{Z} \to \mathbb{Z}$ defined by $f_2(x) = -x + 2$.

(c) $f_3 : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $f_3(j,\ k) = 2^j 3^k$.

(d) $f_4 : \mathbb{P} \to \mathbb{P}$ defined by $f_4(n) = \lceil n/2 \rceil$, where $\lceil x \rceil$ is the ceiling of x, the smallest integer greater than or equal to x.

(e) $f_5 : \mathbb{N} \to \mathbb{N}$ defined by $f_5(n) = n^2 + n$.

(f) $f_6 : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ defined by $f_6(n) = (2n,\ 2n + 1)$.

4. Which of the following are injections, surjections, or bijections on $\mathbb{R}$, the set of real numbers?

(a) $f(x) = -2x$.

(b) $g(x) = x^2 - 1$.

(c) $h(x) = \begin{cases} x & x < 0 \\ x^2 & x \geq 0 \end{cases}$

(d) $q(x) = 2^x$

(e) $r(x) = x^3$

(f) $s(x) = x^3 - x$.

5. Suppose that m pairs of socks are mixed up in your sock drawer. Use the Pigeonhole Principle to explain why, if you pick $m + 1$ socks at random, at least two will make up a matching pair,

6. In your own words explain the statement "The sets of integers and even integers have the same cardinality."

7. Let $A = \{1,\ 2,\ 3,\ 4,\ 5\}$. Find functions, if they exist that have the properties specified below

(a) A function that is one-to-one and onto.

(b) A function that is neither one-to-one nor onto

(c) A function that is one-to-one but not onto.

(d) A function that is onto but not one-to-one.

8. (a) Define functions, if they exist, on the positive integers, ℙ, with the same properties as in Exercise 7 (if possible).

(b) Let A and B be finite sets where $|A| = |B|$. Is it possible to define a function $f : A \to B$ that is one-to-one but not onto? Is it possible to find a function $g : A \to B$ that is onto but not one-to-one?

B Exercises

9. (a) Prove that the set of natural numbers is countable.

(b) Prove that the set of integers is countable.

(c) Prove that the set of rational numbers is countable.

10. (a) Prove that the set of finite strings of 0's and 1's is countable.

(b) Prove that the set of odd integers is countable.

(c) Prove that the set $\mathbb{N} \times \mathbb{N}$ is countable.

11. Use the Pigeonhole Principle to prove that an injection cannot exist between a finite set A and a finite set B if the cardinality of A is greater than the cardinality of B.

12. The important properties of relations are not generally of interest for functions. Most functions are not reflexive, symmetric, antisymmetric, or transitive. Can you give examples of functions that do have these properties?

13. Prove that the set of all infinite sequences of 0's and 1's is not a countable set (i. e., that it is an uncountable set).

14. Prove that the set of all functions on the integers is an uncountable set.

7.3 Composition, Identity, and Inverse

Now that we have a good understanding of what a function is, our next step is to consider an important operation on functions. Our purpose is not to develop the algebra of functions as completely as we did for the algebras of logic, matrices, and sets, but the reader should be aware of the similarities between the algebra of functions and that of matrices. We first define equality of functions.

Definition: Equality of Functions. *Let $f,\ g : A \to B$; that is, let f and g both be functions from A into B. Then f is equal to g (i. e., $f = g$) if and only if $f(x) = g(x)$ for all $x \in A$.*

Two functions that have different domains cannot be equal. For example, $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2$ and $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^2$ are not equal even though the formula that defines them is the same.

On the other hand, it is not uncommon for two functions to be equal even though they are defined differently. For example consider the functions h and k, *where* $h : \{-1, 0, 1, 2\} \to \{0, 1, 2\}$ is defined by $h(x) = |x|$ and $k : \{-1, 0, 1, 2\} \to \{0, 1, 2\}$ is defined by $k(x) = -\frac{x^3}{3} + x^2 + \frac{x}{3}$ appear to be very different functions. However, they are equal because $h(x) = k(x)$ for $x = -1,\ 0,\ 1,$ and 2.

COMPOSITION

One of the most important operations on functions is that of composition.

Definition: Composition of Functions. *Let $f : A \to B$ and $g : B \to C$. Then the composition of f followed by g, written $g \circ f$ is a function from A into C defined by $(g \circ f)(x) = g(f(x))$, which is read " g of f of x."*

The reader should note that it is traditional to write the composition of functions from right to left. Thus, in the above definition, the first function performed in computing $g \circ f$, which is f. On the other hand, for relations, the composition $r s$ is read from left to right, so that the first relation is r.

Example 7.3.1.

(a) Let $f : \{1, 2, 3\} \to \{a, b\}$ be defined by $f(1) = a$, $f(2) = a$, and $f(3) = b$. Let $g : \{a, b\} \to \{5, 6, 7\}$ be defined by $g(a) = 5$ and $g(b) = 7$. Then $g \circ f : \{1, 2, 3\} \to \{5, 6, 7\}$ is defined by $(g \circ f)(1) = 5$, $(g \circ f)(2) = 5$, and $(g \circ f)(3) = 7$. For example, $(g \circ f)(1) = g(f(l)) = g(a) = 5$. Note that f∘g is not defined. Why?

(b) Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^3$ and let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = 3x + 1$. Then, since

$$(g \circ f)(x) = g(f(x)) = g(x^3) = 3x^3 + 1,$$

we have $g \circ f : \mathbb{R} \to \mathbb{R}$ is defined by $(g \circ f)(x) = 3x^3 + 1$. Here $f \circ g$ is also defined and $f \circ g : \mathbb{R} \to \mathbb{R}$ is defined by $(f \circ g)(x) = (3x + 1)^3$. Moreover, since $3x^3 + 1 \neq (3x + 1)^3$ for at least one real number, $g \circ f \neq f \circ g$. Therefore, the commutative law is not true for functions under the operation of composition. However, the associative law is true for functions under the operation of composition.

Theorem 7.3.1. *Function composition is associative. That is, if $f : A \to B, g : B \to C$, and $h : C \to D$, then $h \circ (g \circ f) = (h \circ g) \circ f$.*

Proof Technique: In order to prove that two functions are equal, we must use the definition of equality of functions. Assuming that the functions have the same domain, they are equal if, for each domain element, the images of that element under the two functions are equal.

Proof; We wish to prove that $(h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$ for all $x \in A$, which is the domain of both functions.

$(h \circ (g \circ f))(x) = h((g \circ f)(x))$ by the definition of composition of h with $g \circ f$
$= h(g(f(x)))$ by the definition of composition of g with f

Similarly,

$((h \circ g) \circ f)(x) = (h \circ g)(f(x))$ by the definition of composition of $h \circ g$ with f
$= h(g(f(x)))$ by the definition of composition of h withg

Notice that no matter how the functions the expression $h \circ g \circ f$ is grouped, the final image of any element of $x \in A$ is $h(g(f(x)))$ and so $h \circ (g \circ f) = (h \circ g) \circ f$. ■

If f is a function from a set A onto itself, we can find $f \circ f$, $f \circ f \circ f$, … ,which we write as f^2 , f^3 , ... This idea can be expressed more elegantly as follows; If $f : A \to A$, the repeated composition of f with itself is defined recursively as;

Definition: Powers of Functions. *Let $f : A \to A$.*

(1) $f^1 = f$; that is, $f^1(a) = f(a)$, for $a \in A$.

(2) For $n \geq 1$, $f^{n+1} = f \circ f^n$; that is, $f^{n+1}(a) = f(f^n(a))$ and $a \in A$.

Two useful theorems concerning composition are given below. The proofs are left for the exercises.

Theorem 7.3.2. *If $f : A \to B$ and $g : B \to C$ are injections, then $g \circ f : A \to C$ is an injection.*

Theorem 7.3.3. *If $f : A \to B$ and $g ; B \to C$ are surjections, then $g \circ f : A \to C$ is a surjection.*

We would now like to define the concepts of identity and inverse for functions under composition. The motivation and descriptions of the definitions of these terms come from the definitions of the terms in the set of real numbers and for matrices. For real numbers, the numbers 0 and 1 play the unique role that $x + 0 = 0 + x = x$ and $x \cdot 1 = 1 \cdot x = x$ for any real number x. 0 and 1 are the identity elements for the reals under the operations of addition and multiplication, respectively. Similarly, the $n \times n$ zero matrix 0 and the $n \times n$ identity matrix I are such that for any $n \times n$ matrix A, $A + 0 = 0 + A = A$ and $A I = I A = I$. Hence, an elegant way of defining the identity function under the operation of composition would be to imitate the above well-known facts.

IDENTITY FUNCTION

Definition; Identity Function. *For any set A, the identity function on A is a function from A onto A, denoted by i (or, more specifically, i_A) such that $i(a) = a$ for all $a \in A$*

Based on the definition of i, we can show that for all functions $f : A \to A$, $f \circ i = i \circ f = f$.

An alternate description is that the identity function on A is the function j*(a) = a for all a ∈ A. This can be proven from the above definition.

Example 7.3.2. If $A = \{1, 2, 3\}$, then the identity function $i : A \to A$ is defined by $i(1) = 1$, $i(2) = 2$, and $i(3) = 3$.

Example 7.3.3. The identity function on $\mathbb{R}$ is $i : \mathbb{R} \to \mathbb{R}$ defined by $i(x) = x$.

INVERSE FUNCTIONS

We will introduce the inverse of a function with a special case: the inverse of a function on a set. After you've taken the time to understand this concept, you can read about the inverse of a function from one set into another. The reader is encouraged to reread the definition of the inverse of a matrix in Section 5.4 to see that the following definition of the inverse function is a direct analogue of that definition.

Definition: Inverse Function. *Let $f : A \to A$. If there exists a function $g : A \to A$ such that $g \circ f = f \circ g = i$, then g is called the inverse of f and is denoted by f^{-1}, read "f inverse."*

Notice that in the definition we refer to "the inverse" as opposed to "an inverse." It can be proven that a function can never have more than one inverse (see exercises).

An alternate description of the inverse of a function, which can be proven from the definition, is as follows:

Let $f : A \to A$ be such that $f(a) = b$. Then when it exists, f^{-1} is a function from A to A such that $f^{-1}(b) = a$. Note that f^{-1} "undoes" what f does.

Example 7.3.4. Let $A = \{1, 2, 3\}$ and let f be the function defined on A such that $f(1) = 2$, $f(2) = 3$, and $f(3) = 1$. Then $f^{-1} : A \to A$ is defined by $f^{-1}(I) = 3$, $f^{-1}(2) = 1$, and $f^{-1}(3) = 2$.

Example 7.3.5. If $g : \mathbb{R} \to \mathbb{R}$ is defined by $g(x) = x^3$, then g^{-1} is the function that undoes what g does. Since g cubes real numbers, g^{-1} must be the "reverse" process, namely, takes cube roots. Therefore, $g^{-1} : \mathbb{R} \to \mathbb{R}$ is defined by $g^{-1}(x) = \sqrt[3]{x}$. We should show that $g^{-1} \circ g = i$ and $g \circ g^{-1} = i$. We will do the first, and the reader is encouraged to do the second.

$$\begin{aligned}
(g^{-1} \circ g)(x) &= g^{-1}(g(x)) && \text{Definition of composition} \\
&= g^{-1}(x^3) && \text{Definition of } g \\
&= \sqrt[3]{x^3} && \text{Definition of } g^{-1} \\
&= x && \text{Definition of cube root} \\
&= i(x) && \text{Definition of the identity function}
\end{aligned}$$

Therefore, $g^{-1} \circ g = i$. Why?

The definition of the inverse of a function alludes to the fact that not all functions have inverses. How do we determine when the inverse of a function exists?

Theorem 7.3.4. *Let $f : A \to A$. f^{-1} exists if and only if f is a bijection; i. e. f is one-to-one and onto.*

Proof: (⇒) In this half of the proof, assume that f^{-1} exists and we must prove that f is one-to-one and onto. To do so, it is convenient for us to use the relation notation, where $f(s) = t$ is equivalent to $(s, t) \in f$. To prove that f is one-to-one, assume that $f(a) = f(b) = c$. Alternatively, that means (a, c) and (b, c) are elements of f. We must show that $a = b$. Since (a, b), $(c, b) \in f$, (c, a) and (c, b) are in f^{-1}. By the fact that f^{-1} is a function and c cannot have two images, a and b must be equal, so f is one-to-one.

Next, to prove that f is onto, observe that for f^{-1} to be a function, it must use all of its domain, namely A. Let b be any element of A. Then b has an image under f^{-1}, $f^{-1}(b)$. Another way of writing this is $(b, f^{-1}(b)) \in f^{-1}$, By the definition of the inverse, this is equivalent to $(f^{-1}(b), b) \in f$. Hence, b is in the range of f. Since b was chosen arbitrarily, this shows that the range of f must be all of A.

(⇐) Assume f is one-to-one and onto and we are to prove f^{-1} exists. We leave this half of the proof to the reader. ■

Definition; Permutation. A bijection of a set A into itself is called a permutation of A,

Next, we will consider the situation where f: A→B and B is not necessarily equal to A. How do we define the inverse in this case?

Definition: Inverse of a Function (General Case). *Let $f : A \to B$, If there exists a function $g : B \to A$ such that $g \circ f = i_A$ and $f \circ g = i_B$, then g is called the inverse of f and is denoted by f^{-1}, read "f inverse."*

Note the slightly more complicated condition for the inverse in this case because the domains of $f \circ g$ and $g \circ f$ are different if A and B are different. The proof of the following theorem isn't really very different from the special case where $A = B$.

Theorem 7.3.5. *Let $f : A \to B$. f^{-1} exists if and only if f is a bijection.*

Example 7.3.6. Let $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$. Define $f : A \to B$ by $f(1) = a$, $f(2) = b$, and $f(3) = c$. Then $g : B \to A$ defined by $g(a) = 1$, $g(b) = 2$, and $g(c) = 3$ is the inverse of f.

$$\left.\begin{array}{l} (g\circ f)(1) = 1 \\ (g\circ f)(2) = 2 \\ (g\circ f)(3) = 3 \end{array}\right\} \Rightarrow g\circ f = i_A \text{ and } \left.\begin{array}{l} (f\circ g)(a) = a \\ (f\circ g)(b) = b \\ (f\circ g)(c) = c \end{array}\right\} \Rightarrow f\circ g = i_B$$

Mathematica Note

Computer languages have many functions that also have inverses. Here are a few examples in *Mathematica*:

`RotateRight` and `RotateLeft` are both functions on lists. For example,

```
RotateRight[{1, 2, 3, 4, 5}]

{5, 1, 2, 3, 4}

RotateLeft[{1, 2, 3, 4, 5}]

{2, 3, 4, 5, 1}

RotateLeft[RotateRight[{1, 2, 3, 4, 5}]]

{1, 2, 3, 4, 5}
```

`IntegerDigits` and `FromDigits` are inverses of one another, with domains being the positive integers and lists of digits, respectively. For example

```
IntegerDigits[1492]

{1, 4, 9, 2}

FromDigits[{1, 4, 9, 2}]

1492

FromDigits[IntegerDigits[193 410]]

193 410

IntegerDigits[FromDigits[{4, 3, 1, 7, 8}]]

{4, 3, 1, 7, 8}
```

EXERCISES FOR SECTION 7.3

A Exercises

1. Let $A = \{1, 2, 3, 4, 5\}$, $B = \{a, b, c, d, e, f\}$, and $C = \{+, -\}$. Define $f : A \to B$ by $f(k)$ equal to the k^{th} letter in the alphabet, and define $g : B \to C$ by $g(\alpha) = +$ if α is a vowel and $g(\alpha) = -$ if α is a consonant.

(a) Find $g\circ f$.

(b) Does it make sense to discuss $f\circ g$? If not, why not?

(c) Does f^{-1} exist? Why?

(d) Does g^{-1} exist? Why?

2. Let $A = \{1, 2, 3\}$. Define $f : A \to A$ by $f(1) = 2$, $f(2) = 1$, and $f(3) = 3$. Find f^2, f^3, f^4 and f^{-1}.

3. Let $A = \{1, 2, 3\}$.

(a) List all permutations of A.

(b) Find the inverse of each of the permutations of part a.

(c) Find the square of each of the permutations of part a.

(d) Show that the composition of any two permutations of A is a permutation of A.

(e) Prove that if A be any set where the $|A| = n$, then the number of permutations of A is $n!$.

4. Define s, u, and d, all functions on the integers, by $s(n) = n^2$, $u(n) = n + 1$, and $d(n) = n - 1$. Determine:

(a) $u \circ s \circ d$

(b) $s \circ u \circ d$

(c) $d \circ s \circ u$

5. Based on the definition of the identity function, show that for all functions $f : A \to A$, $f \circ i = i \circ f = f$.

6. **Inverse images.** If f is any function from A into B, we can describe the inverse image of from B into $\mathcal{P}(A)$, which is also commonly denoted f^{-1}. If $b \in B$, $f^{-1}(b) = \{a \in A \mid f(a) = b\}$. If f does have an inverse, the inverse image of b is $\{f^{-1}(b)\}$.

(a) Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^2$. What are $g^{-1}(4)$, $g^{-1}(0)$ and $g^{-1}(-1)$?

(b) If $r : \mathbb{R} \to \mathbb{Z}$, where $r(x) = \lceil x \rceil$, what is $r^{-1}(1)$?

7. Let f, g, and h all be functions from $\mathbb{Z}$ into $\mathbb{Z}$ defined by $f(n) = n + 5$, $g(n) = n - 2$, and $h(n) = n^2$. Define:

(a) $f \circ g$

(b) f^3

(c) $f \circ h$

8. Define the following functions on the integers by $f(k) = k + 1$, $g(k) = 2k$, and $h(k) = \lceil k/2 \rceil$

(a) Which of these functions are one-to-one?

(b) Which of these functions are onto?

(c) Express in simplest terms the compositions $f \circ g$, $g \circ f$, $g \circ h$, $h \circ g$, and h^2 ,

B Exercises

9. State and prove a theorem on inverse functions analogous to Theorem 5.4.1 (if a matrix has an inverse, that inverse is unique).

10. Let f and g be functions whose inverses exist. Prove that $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$. (Hint: See Exercise 3 of Section 5.4.)

11. Prove Theorems 7.3.2 and 7.3.3.

12. Prove the second half of Theorem 7.3.4.

13. Prove by induction that if $n \geq 2$ and $f_1, f_2, \ldots, f_n$ are invertible functions on some nonempty set A, then $(f_1 \circ f_2 \circ \cdots \circ f_n)^{-1} = f_n^{-1} \circ \cdots \circ f_2^{-1} \circ f_1^{-1}$. The basis has been taken care of in Exercise 10.

C Exercises

14. (a) Our definition of cardinality states that two sets, A and B, have the same cardinality if there exists a bijection between the two sets. Why does it not matter whether the bijection is from A into B or B into A? (b) Prove that "has the same cardinality as" is an equivalence relation on sets.

15. Construct a table listing as many "Laws of Function Composition" as you can identify. Use previous lists of laws as a guide.

SUPPLEMENTARY EXERCISES FOR CHAPTER 7

Section 7.1

1. If $f : \mathbb{Z} \rightarrow \mathbb{Z}$ is defined by $f(a) = 2\,|a| + 1$,

   (a) What is the domain of f ?

   (b) What is the codomain of f ?

   (c) What is the image of -5 under f ?

   (d) What is the range of f ?

   (e) Given that $f(a) = 11$, can you tell exactly what a must be?

2. Let $f : \mathbb{P} \rightarrow \mathbb{P}$, where $f(a)$ is the largest power of two that evenly divides a; for example, $f(12) = 4$, $f(9) = 1$, and $f(8) = 8$. Describe the equivalence classes of the kernel of f.

3. Are any of the relations given in Figure 6.3.2 functions on the set A of nodes? Explain.

4. Let U be a set with subsets A and B.

   (a) Show that $g : U \rightarrow \{0, 1\}$ defined by $g(a) = \min(C_A(a), C_B(a))$ is the characteristic function of $A \cap B$. (See Exercise 2 of Section 7.1.)

   (b) What characteristic function is $h : U \rightarrow \{0, 1\}$ defined by $h(a) = \max(C_A(a), C_B(a))$?

   (c) How are the characteristic functions of A and A^c related?

Section 7.2

5. Recall that every function is a relation. Suppose that f is a function on $\{1, 2, \ldots, n\}$, where n is a positive integer.

(a) What must the matrix of f look like? In other words, what distinguishes the matrix of f from the matrix of the typical relation? How many 1 *s* appear in the matrix?

(b) If f is a bijection, what further property does the matrix of f have? (*Hint* for those who know chess: We will call the matrix of a bijection a "rook matrix.")

6. Let $S = \{a, b, c\}$ and let $T = \{1, 2, 3, 4\}$

   (a) Give an example of a relation from S to T that is not a function.

   (b) Give an example of a relation from S to T that is an injection.

   (c) How many injections are there from S to T?

   (d) How many surjections are there from S to T?

7. Prove that the following sets are countable.

   (a) $\{n^2 : n \in \mathbb{N}\}$

   (b) $\left\{\frac{1}{n} : n \in \mathbb{P}\right\}$

   (c) $\{3, 9, 27, 81, \ldots\} \cup \{2, 4, 8, 16, \ldots\}$

8. Prove that if A and B are countable sets, then their union is also countable.

9. Prove that if A and B are any two sets, then $|(A \times B)| = |(B \times A)|$; that is, prove that $A \times B$ and $B \times A$ have the same cardinality.

10. Let A be a finite set.

   (a) Is every injection $f : A \rightarrow A$ a surjection? Explain.

   (b) Is every surjection $f : A \rightarrow A$ an injection? Explain.

   (c) Are parts a and b true if A is an infinite set? Give a counterexample.

11. Two children playing "spy" have devised a code that consists of spelling each word backwards and replacing the letters a and t by m and q, respectively. Let A be the set of letters in the English alphabet. Assume the boys use characters only from A. Explain this code using the concept of functions. Explain why this code will or will not work, using the concept of functions.

Section 7.3

12. Consider the functions $f,\ g : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 8\,x + 5$ and $g(x) = x^2$.

(a) Show that f is injective.

(b) Show that f is surjective.

(c) Find $f^{-1}(x)$.

(d) Find $g \circ f(x)$.

(e) Find $f \circ g(x)$.

13. If $f,\ g,\ h : \mathbb{N} \to \mathbb{N}$, where $f(a) = 10\,a,\ \ g(a) = a + 10$, and $h(a) = a$ div 10 (*the quotient in* $a \div 10$), calculate

(a) $(f \circ g)\,(a)$.

(b) $g^2(a) = (g \circ g)\,(a)$.

(c) $(h \circ f)\,(a)$.

(d) $(h \circ g)\,(a)$.

14. If $f,\ u,\ d : \mathbb{N} \to \mathbb{N}$, where $f(a) = 2\,a,\ \ u(a) = a + 1$, and $d(a) = \max(0,\ a - 1)$, calculate

(a) $(f \circ u)\,(a)$.

(b) $f^2(a)$.

(c) $(d \circ (f \circ u))\,(a)$.

(d) $(d \circ u)\,(a) = a$; therefore, what is $d \circ u$?

(e) Explain why d is *not* the inverse of u.

15. Let f be a function on $A = \{a,\ b,\ c,\ d\}$ such that $f(a) = c$, and $f(d) = b$.

(a) What are $f(b)$ and $f(c)$ if $f \circ f = f$?

(b) What are $f(b)$ and $f(c)$ if $f \circ f = i$?

16. Let A be a nonempty set. Prove that if f is a bijection on A and $f \circ f = f$, then f is the identity function, i. *Hint:* You have seen a similar proof in matrix algebra.

17. For the real matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\det A = ad - bc$.

A bijection from a set to *itself* is also referred to as a *permutation* of the set. Let π be a permutation of $\{a,\ b,\ c,\ d\}$ such that a becomes $\pi(a)$, b becomes $\pi(b)$, etc.

Let $B = \begin{pmatrix} \pi(a) & \pi(b) \\ \pi(c) & \pi(d) \end{pmatrix}$. How many permutations of π leave the determinant of A invariant, that is, $\det A\ =\ \det B$?

18. (For those who have had calculus): Let V be the set of all functions that are defined and have infinitely many derivatives over some fixed interval of the real line. Let $f \in V$ and define $D : V \to V$ by $D(f) = f\,'$, that is, D is the act of taking the derivative. Hence: $D(x^2 + 3\,x + 5) = 2\,x + 3$.

(a) Is D a function? Explain.

(b) Is D a bijection? Explain.

(c) What is the interpretation of $D^2 = D \circ D,\ D^3,\ \ldots,\ D^n$?

(d) Does D^{-1} exist? If not, is there a function in calculus that is "close to" D^{-1}? What is it?

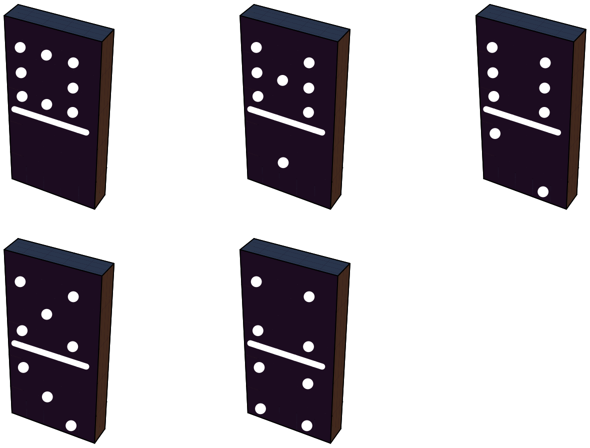
19. The exponential function $f : \mathbb{R} \to \mathbb{R}^+$ defined by $f(x) = b^x$ has as its inverse the logarithmic function $g(x) = \log_b x$.

(a) What are the domain and codomain of g?

(b) Prove that g is the inverse of f.

20. In high school, many of us saw the notation $\sin^{-1} x$. Why is this notation used?

chapter 8



RECURSION AND RECURRENCE RELATIONS

GOALS

An essential tool that anyone interested in computer science must master is how to think recursively. The ability to understand definitions, concepts, algorithms, etc., that are presented recursively and the ability to put thoughts into a recursive framework are essential in computer science. One of our goals in this chapter is to help the reader become more comfortable with recursion in its commonly encountered forms.

A second goal is to discuss recurrence relations. We will concentrate on methods of solving recurrence relations, including an introduction to generating functions.

8.1 The Many Faces of Recursion

Consider the following definitions, all of which should be somewhat familiar to you. When reading them, concentrate on how they are similar.

Example 8.1.1. A very common alternate notation for the binomial coefficient $\binom{n}{k}$ is $C\,(n;\ k)$. We will use the latter notation in this chapter.

Here is a recursive definition of binomial coefficients.

Definition: Binomial Coefficients. *Assume* $n \geq 0$ *and* $n \geq k \geq 0$.

$C(n; 0) = 1$

$C(n,\ n) = 1$

and $C\,(n;\ k) = C(n-1;\ k) + C(n-1;\ k-1)$ *if* $n > k > 0$.

POLYNOMIALS AND THEIR EVALUATION

Definition: Polynomial Expression in x over S (Non-Recursive). *Let n be an integer,* $n \geq 0$. *An* n^{th} *degree polynomial in x is an expression of the form* $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, *where* $a_n,\ a_{n-1}, \ldots, a_1, a_0$ *are elements of some designated set of numbers, S, called the set of coefficients and* $a_n \neq 0$.

We refer to x as a variable here, although the more precise term for x is an *indeterminate*. There is a distinction between the terms indeterminate and variable, but that distinction will not come into play in our discussions.

Zeroth degree polynomials are called constant polynomials and are simply elements of the set of coefficients.

This definition is often introduced in algebra courses to describe expressions such as $f\,(n) = 4\,n^3 + 2\,n^2 - 8\,n + 9$, a third-degree, or cubic, polynomial in n. This definitions has has drawbacks when the variable is given a value and the expression must be evaluated, For example, suppose that n = 7. Your first impulse is likely to do this:

$$\begin{aligned} f(7) &= 4\times 7^3 + 2\times 7^2 - 8\times 7 + 9 \\ &= 4\times 343 + 2\times 49 - 8\times 7 + 9 = 1423 \end{aligned}$$

A count of the number of operations performed shows that five multiplications and three additions/subtractions were performed. The first two multiplications compute 7^2 and 7^3, and the last three mutiply the powers of 7 times the coefficients. This gives you the four terms; and adding/-subtacting a list of k numbers requires $k - 1$ addition/subtractions. The following definition of a polynomial expression suggests another more efficient method of evaluation.

Definition: Polynomial Expression in x over S (Recursive)*. Let S be a set of coefficients and x any variable.*

(a) A zeroth degree polynomial expression in x over S is a nonzero element of S.

(b) For $n \geq 1$, an n^{th} degree polynomial expression in x over S is an expression of the form $p(x)\,x + a$ where $p(x)$ is an $(n-1)^{st}$ degree polynomial expression in x and $a \in S$.

We can easily verify that f(n) is a third-degree polynomial expression in n over the $\mathbb{Z}$ based on this definition:

$$f(n) = (4\,n^2 + 2\,n - 8)\,n + 9 = ((4\,n + 2)\,n - 8)\,n + 9$$

Notice that 4 is a zeroth degree polynomial since it is an integer. Therefore $4\,n + 2$ is a first-degree polynomial; therefore, $(4\,n + 2)\,n - 8$ is a second-degree polynomial in n over $\mathbb{Z}$; therefore, $f(n)$ is a third-degree polynomial in n over $\mathbb{Z}$. The final expression for $f(n)$ is called its *telescoping form*. If we use it to calculate $f(7)$, we need only three multiplications and three additions /subtractions. This is called Horner's method for evaluating a polynomial expression.

Example 8.12. (a) The telescoping form of $p(x) = 5\,x^4 + 12\,x^3 - 6\,x^2 + x + 6$ is $(((5\,x + 12)\,x - 6)\,x + 1)\,x + 6$. Using Horner's method, computing the value of $p(c)$ requires four multiplications and four additions/subtractions for any real number c.

(b) $g(x) = -x^5 + 3\,x^4 + 2\,x^2 + x$ has the telescoping form $((((-x + 3)\,x)\,x + 2)\,x + 1)\,x$.

Many computer languages represent polynomials as lists of coefficients, usually starting with the constant term. For example, $g(x) = -x^5 + 3\,x^4 + 2\,x^2 + x$ would be represented with the list $\{0, 1, 2, 0, 3, -1\}$. In both *Mathematica* and Sage, polynomial expressions can be entered and manipulated, so the list representation is only internal. Some lower-leveled languages do require users to program polynomial operations with lists. We will leave these programming issues to another source.

Example 8.1.3. A recursive algorithm for a binary search of a sorted list of items: $r = \{r(1), r(2) \ldots, r(n)\}$ represent a list of n items sorted by a numeric key in descending order. The j^{th} item is denoted $r(j)$ and its key value by $r(j)$.key. For example, each item might contain data on the buildings in a city and the key value might be the height of the building. Then $r(1)$ would be the item for the tallest building. The algorithm BinarySearch (j, k) can be applied to search for an item in r with key value C. This would be accomplished by the execution of BinarySearch $(1, n)$. When the algorithm is completed, the variable `Found` will have a value of true if an item with the desired key value was found, and the value of `location` will be the index of an item whose key is C. If `Found` stays false, no such item exists in the list. The general idea behind the algorithm is illustrated in Figure 8.1.2.

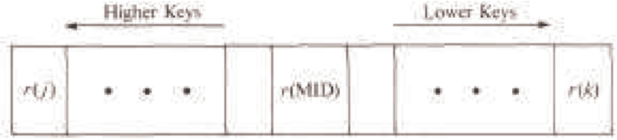


FIGURE 8.1.2 Illustration of BinarySearch

In this algorithm, `Found` and `location` are "global" variables to execution of the algorithm.

```
BinarySearch ($j, k$) :
 Found = False
 If $J < K$
   Then
       Mid = $\lfloor (j + k) / 2 \rfloor$
       If $r$(Mid).key == $C$
         Then
             location = Mid
             Found = TRUE
         Else
           If $r$(Mid).key < $C$
               Then execute BinarySearch(j, Mid - 1)
               Else execute BinarySearch(Mid + 1 , $k$)
```

For the next two examples, consider a sequence of numbers to be a list of numbers consisting of a zeroth number, first number, second number, … . If a sequence is given the name S, the k^{th} number of S, is usually written S_k or $S(k)$.

Example 8.1.4 Define the sequence of numbers B by

$$B_0 = 100 \text{ and}$$

$$B_k = 1.08\ B_{k-1} \text{ for } k \geq 1$$

These rules stipulate that each number in the list is 1.08 times the previous number, with the starting number equal to 100. For example

$$\begin{aligned} B_3 &= 1.08\, B_2 \\ &= 1.08\,(1.08\, B_1) \\ &= 1.08\,(1.08\,(1.08\, B_0)) \\ &= 1.08\,(1.08\,(1.08\ 100)) \\ &= 1.08^3\ 100 \\ &= 125.971 \end{aligned}$$

Example 8.1.5. The Fibonacci sequence is the sequence F defined by

$$F_0 = 1,\ \ F_1 = 1 \text{ and}$$

$$F_k = F_{k-2} + F_{k-1} \text{ for } k \geq 2.$$

RECURSION

All of the previous examples were presented recursively. That is, every "object" is described in one of two forms. One form is by a simple definition, which is usually called the basis for the recursion. The second form is by a recursive description in which objects are described in terms of themselves, with the following qualification. What is essential for a proper use of recursion is that the objects can be expressed in terms of simpler objects, where "simpler" means closer to the basis of the recursion. To avoid what might be considered a circular definition, the basis must be reached after a finite number of applications of the recursion.

To determine, for example, the fourth item in the Fibonacci sequence we repeatedly apply the recursive rule for F until we are left with an expression involving F_0 and F_1:

$$\begin{aligned} F_4 &= F_2 + F_3 \\ &= (F_0 + F_1) + (F_1 + F_2) \\ &= (F_0 + F_1) + (F_1 + (F_0 + F_1)) \\ &= (1 + 1) + (1 + (1 + 1)) \\ &= 5 \end{aligned}$$

ITERATION

On the other hand, we could compute a term in the Fibonacci sequence, say F_5 by starting with the basis terms and working forward as follows:

$$\begin{aligned} F_2 &= F_0 + F_1 = 1 + 1 = 2 \\ F_3 &= F_1 + F_2 = 1 + 2 = 3 \\ F_4 &= F_2 + F_3 = 2 + 3 = 5 \\ F_5 &= F_3 + F_4 = 3 + 5 = 8 \end{aligned}$$

This is called an iterative computation of the Fibonacci sequence. Here we start with the basis and work our way forward to a less simple number, such as. Try to compute F_5 using the recursive definition for F as we did for F_4 . It will take much more time than it would have taken to do the computations above. Iterative computations usually tend to be faster than computations that apply recursion. Therefore, one useful skill is being able to convert a recursive formula into a nonrecursive formula, such as one that requires only iteration or a faster method, if possible.

An iterative formula for $C(n;\ k)$ is also much more efficient than an application of the recursive definition. The recursive definition is not without its merits, however. First, the recursive equation is often useful in manipulating algebraic expressions involving binomial coefficients. Second, it gives us an insight into the combinatoric interpretation of $C(n;\ k)$. In choosing k elements from $\{1, 2, \ldots, n\}$, there are $C(n - 1;\ k)$ ways of choosing all k from $\{1, 2, \ldots, n - 1\}$, and there are $C(n - 1; k - 1)$ ways of choosing the k elements if n is to be selected and the remaining $k - 1$ elements come from $\{1, 2, \ldots, n - 1\}$. Note how we used the Law of Addition from Chapter 2 in our reasoning.

BinarySearch Revisited. In the binary search algorithm, the place where recursion is used is easy to pick out. When an item is examined and the key is not the one you want, the search is cut down to a sublist of no more than half the number of items that you were searching in before. Obviously, this is a simpler search. The basis is hidden in the algorithm. The two cases that complete the search can be thought of as the basis. Either you find an item that you want, or the sublist that you have been left to search in is empty (j > k).

BinarySearch can be translated without much difficulty into any language that allows recursive calls to its subprograms. The advantage to such a program is that its coding would be much shorter than a nonrecursive program that does a binary search. However, in most cases the recursive version will be slower and require more memory at execution time.

INDUCTION AND RECURSION

The definition of the positive integers in terms of Peano's Postulates (Section 3.7) is a recursive definition. The basis element is the number 1 and the recursion is that if n is a positive integer, then so is its successor. In this case, n is the simple object and the recursion is of a forward type. Of course, the validity of an induction proof is based on our acceptance of this definition. Therefore, the appearance of induction proofs when recursion is used is no coincidence.

Example 8.1.6. A formula for the sequence B in Example 8.1.4 is $B = 100\,(1.08)^k$ for $k \geq 0$. A proof by induction follows: If $k = 0$, then $B = 100\,(1.08)^0 = 100$, as defined. Now assume that for some $k \geq 1$, the formula for B_k is true.

$$\begin{aligned} B_{k+1} &= 1.08\,B_k && \text{by the recursive definition} \\ &= 1.08\left(100\,(1.08)^k\right) && \text{by the induction hypothesis} \\ &= 100\ (1.08)^{k+1} && \text{hence the formula is true for } k+1 \end{aligned}$$

The formula that we have just proven for B is called a closed form expression. It involves no recursion or summation signs.

Definition: Closed Form Expression. *Let $E = E(x_1, x_2, \ldots, x_n)$ he an algebraic expression involving variables $x_1, x_2, \ldots, x_n$ which are allowed to take on values from some predetermined set. E is a closed form expression if there exists a number B such that the evaluation of E with any allowed values of the variables will take no more than B operations (alternatively, B time units).*

Example 8.1.7. The sum $E(n) = \sum_{k=1}^{n} k$ is not a closed form expression because the number of additions needed evaluate $E(n)$ grows indefinitely with n. A closed form expression that computes the value of $E(n)$ is $\frac{n(n+1)}{2}$, which only requires $B = 3$ operations.

EXERCISES FOR SECTION 8.1

A Exercises

1. By the recursive definition of binomial coefficients, $C(5;\ 2) = C(4;\ 2) + C(4;\ 1)$. Continue expanding $C(5;\ 2)$ to express it in terms of quantities defined by the basis. Check your result by applying the factorial definition of $C(n;\ k)$.

2. Define the sequence L by $L_0 = 5$ and for $k \geq 1$, $L_k = 2\,L_{k-1} - 7$. Determine L_4 and prove by induction that $L_k = 7 - 2^{k+1}$.

3. Let $p(x) = x^5 + 3\,x^4 - 15\,x^3 + x - 10$.

(a) Write $p(x)$ in telescoping form.

(b) Use a calculator to compute $p(3)$ using the original form of $p(x)$.

(c) Use a calculator to compute $p(3)$ using the telescoping form of $p(x)$.

(d) Compare your speed in parts b and c.

B Exercises

4. Suppose that a list of nine items, (r(l), r(2), . . . , r(9)), is sorted by key in decending order so that $r(3)$.key $= 12$ and $r(4)$.key $= 10$. List the executions of BinarySearch that would be needed to complete BinarySearch(1,9) for:

(a) C = 12
(b) C = 11

Assume that distinct items have distinct keys.

5. What is wrong with the following definition of $f : \mathbb{R} \to \mathbb{R}$?

$f(0) = 1$ and $f(x) = f(x/2)/2$ if $x \neq 0$.

8.2 Sequences

Definition: Sequence. *A sequence is a function from the natural numbers into some predetermined set. The image of any natural number k can be written interchangeably as $S(k)$ or S_k and is called the k^{th} term of S. The variable k is called the index or argument of the sequence.*

For example, a sequence of integers would be a function $S : \mathbb{N} \to \mathbb{Z}$.

Example 8.2.1.

(a) The sequence A defined by $A(k) = k^2 - k,\ \ k \geq 0$, is a sequence of integers.

(b) The sequence B defined recursively by $B(0) = 2$ and $B(k) = B(k-1) + 3$ for $k \geq 1$ is a sequence of integers. The terms of B can be computed either by applying the recursion formula or by iteration. For example;

$$\begin{aligned} B(3) &= B(2) + 3 \\ &= (B(1) + 3) + 3 \\ &= ((B(0) + 3) + 3) + 3) \\ &= ((2 + 3) + 3) + 3 \\ &= 11 \end{aligned}$$

or

$$B(1) = B(0) + 3 = 2 + 3 = 5$$

$$B(2) = B(1) + 3 = 5 + 8 = 8$$

$$B(3) = B(2) + 3 = 8 + 3 = 11.$$

(c) Let C_r be the number of strings of 0's and 1's of length r having no consecutive zeros. These terms define a sequence C of integers.

Remarks;

(1) A sequence is often called a *discrete function*.

(2) Although it is important to keep in mind that a sequence is a function, another useful way of visualizing a sequence is as a list. For example, the sequence A could be written as $(0, 0, 2, 6, 12, 20, \ldots)$. Finite sequences can appear much the same way when they are the input to or output from a computer. The index of a sequence can be thought of as a time variable. Imagine the terms of a sequence flashing on a screen every second. The s_k would be what you see in the k^{th} second. It is convenient to use terminology like this in describing sequences. For example, the terms that precede the k^{th} term of A would be $A(0),\ A(1),\ \ldots,\ A(k-1)$. They might be called the earlier terms.

A FUNDAMENTAL PROBLEM

Given the definition of any sequence, a fundamental problem that we will concern ourselves with is to devise a method for determining any specific term in a minimum amount of time. Generally, time can be equated with the number of operations needed. In counting operations, the application of a recursive formula would be considered an operation.

Example 8.2.2.

(a) The terms of A in Example 8.2.1 are very easy to compute because of the closed form expression. No matter what term you decide to compute, only three operations need to be performed.

(b) How to compute the terms of B is not so clear. Suppose that you wanted to know $B(100)$. One approach would be to apply the definition recursively:

$$B(100) = B(99) + 3 = (B(98) + 3) + 3 = \ldots$$

The recursion equation for B would be applied 100 times and 100 additions would then follow. To compute $B(k)$ by this method, $2k$ operations are needed. An iterative computation of $B(k)$ is an improvement:

$$\begin{aligned} B(1) &= B(0) + 3 = 2 + 3 = 5 \\ B(2) &= B(1) + 3 = 5 + 3 = 8 \\ &\text{etc.} \end{aligned}$$

Only k additions are needed. This still isn't a good situation. As k gets large, we take more and more time to compute $B(k)$. The formula $B(k) = B(k-1) + 3$ is called a recurrence relation on B. The process of finding a closed form expression for $B(k)$, one that requires no more than some fixed number of operations, is called solving the recurrence relation.

(c) The determination of C_k is a standard kind of problem in combinatorics. One solution is by way of a recurrence relation. In fact, many problems in combinatorics are most easily solved by first searching for a recurrence relation and then solving it. The following observation will suggest the recurrence relation that we need to determine C_k : If $k \geq 2$, then every string of 0's and 1's with length k and no two consecutive 0's is either $1 s_{k-1}$ or $01 s_{k-2}$, where s_{k-1} and s_{k-2} are strings with no two consecutive 0's of length $k-1$ and $k-2$ respectively. From this observation we can see that $C_k = C_{k-2} + C_{k-1}$ for $k \geq 2$. The terms $C_0 = 1$ and $C_1 = 2$ are easy to determine by enumeration. Now, by iteration, any C_k can be easily determined. For example, $C_5 = 21$ can be computed with five additions. A closed form expression for C_k would be an improvement. Note that the recurrence relation for C_k is identical to the one for the Fibonacci sequence (Example 8.1.4). Only the basis is different.

EXERCISES FOR SECTION 8.2

A Exercises

1. Prove by induction that $B(k) = 3k + 2, k \geq 0$, is a closed form expression for the sequence B in Example 8.2.1.

2. (a) Consider sequence Q defined by $Q(k) = 2k + 9, k \geq 1$. Complete the table below and determine a recurrence relation that describes Q.

k	$Q(k)$	$Q(k) - Q(k-1)$
2		
3		
4		
5		
6		
7		

(b) Let $A(k) = k^2 - k, \quad k \geq 0$. Complete the table below and determine a recurrence relation for A . Notice that $(A(k) - A(k-1) - (A(k-1) - A(k-2)) = A(k) - 2A(k-1) + A(k-2)$

k	$A(k)$	$A(k) - A(k-1)$	$A(k) - 2A(k-1) + A(k-2)$
2			
3			
4			
5			

3. Given k lines $(k \geq 0)$ on a plane such that no two lines are parallel and no three lines meet at the same point, let $P(k)$ be the number of regions into which the lines divide the plane (including the infinite ones (see Figure 8.2.1). Describe geometrically how the recurrence relation $P(k) = P(k \text{—} 1) + k$ can be obtained. Given that $P(0) = 1$, determine $P(5)$.

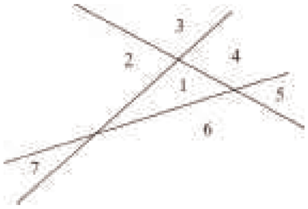


FIGURE 8.2.1 Exercise 3

4. A sample of a radioactive substance is expected to decay by 0.15 percent each hour. If $w_t, t \geq 0$, is the weight of the sample t hours into an experiment, write a recurrence relation for w.

B Exercise

5. Let $M(n)$ be the number of multiplications needed to evaluate an n^{th} degree polynomial. Use the recursive definition of a polynomial expression to define M recursively.

8.3 Recurrence Relations

In this section we will begin our study of recurrence relations and their solutions. Our primary focus will be on the class of finite order linear recurrence relations with constant coefficients (shortened to finite order linear relations). First, we will examine closed form expressions from which these relations arise. Second, we will present an algorithm for solving them. In later sections we will consider some other common relations (8.4) and introduce two additional tools for studying recurrence relations: generating functions (8.5) and matrix methods (Chapter 12).

Definition: Recurrence Relation. *Let S be a sequence of numbers, A recurrence relation on S is a formula that relates all but a finite number of terms of S to previous terms of S. That is, there is a k_0 in the domain of S such that if $k \geq k_0$, then S(k) is expressed in terms of some (and possibly all) of the terms that precede S(k). If the domain of S is $\{0, 1, 2, \ldots\}$, the terms $S(0), S(1), \ldots, S(k_0 - 1)$ are not defined by the recurrence formula. Their values are the initial conditions (or boundary conditions, or basis) that complete the definition of S.*

Example 8.3.1.

(a) The Fibonacci sequence is defined by the recurrence relation $F_k = F_{k-2} + F_{k-1}$, $k \geq 2$, with the initial conditions $F_0 = 1$ and $F_1 = 1$. The recurrence relation is called a second-order relation because F_k depends on the two previous terms of F. Recall that the sequence C in Section 8.2 can be defined with the same recurrence relation, but with different initial conditions.

(b) The relation $T(k) = 2\,T(k-1)^2 - k\,T(k-3)$ is a third-order recurrence relation. If values of $T(0)$, $T(1)$, and $T(2)$ are specified, then T is completely defined.

(c) The recurrence relation $S(n) = S(\lfloor n/2 \rfloor) + 5$, $n > 0$, with $S(0) = 0$ has infinite order. To determine $S(n)$ when n is even, you must go back $n/2$ terms. Since $n/2$ grows unbounded with n, no finite order can be given to S.

SOLVING RECURRENCE RELATIONS

Sequences are often most easily defined with a recurrence relation; however, the calculation of terms by directly applying a recurrence relation can be time consuming. The process of determining a closed form expression for the terms of a sequence from its recurrence relation is called solving the relation. There is no single technique or algorithm that can be used to solve all recurrence relations. In fact, some recurrence relations cannot be solved. The relation that defines T above is one such example. Most of the recurrence relations that you are likely to encounter in the future as classified as finite order linear recurrence relations with constant coefficients. This class is the one that we will spend most of our time with in this chapter.

Definition: n^{th} Order Linear Recurrence Relation. *Let S be a sequence of numbers with domain $k \geq 0$. An n^{th} order linear recurrence relation on S with constant coefficients is a recurrence relation that can be written in the form*

$$S(k) + C_1\,S(k-1) + \ldots + C_n\,S(k-n) = f(k) \quad \text{for } k \geq n$$

where $C_1, C_2, \ldots, C_n$ are constants and f is a numeric function that is defined for $k \geq n$.

Note: We will shorten the name of this class of relations to n^{th} order linear relations. Therefore, in further discussions, $S(k) + 2\,k\,S(k-1) = 0$ would not be considered a first-order linear relation.

Example 8.3.2.

(a) The Fibonacci sequence is defined by the second-order linear relation because $F_k - F_{k-1} - F_{k-2} = 0$

(b) The relation $P(j) + 2\,P(j-3) = j^2$ is a third-order linear relation. In this case, $C_1 = C_2 = 0$.

(c) The relation $A(k) = 2\,(A(k-1) + k)$ can be written as $A(k) - 2\,A(k-1) = 2\,k$. Therefore, it is a first-order linear relation.

RECURRENCE RELATIONS OBTAINED FROM "SOLUTIONS"

Before giving an algorithm for solving finite order linear relations, we will examine recurrence relations that arise from certain closed form expressions. The closed form expressions are selected so that we will obtain finite order linear relations from them. This approach may seem a bit contrived, but if you were to write down a few simple algebraic expressions, chances are that most of them would be similar to the ones we are about to examine.

Example 8.3.3.

(a) Consider D, defined by $D(k) = 5 \cdot 2^k$, $k \geq 0$. If $k \geq 1$,

$$D(k) = 5 \cdot 2^k = 2 \cdot 5 \cdot 2^{k-1} = 2\,D(k-1).$$

Therefore, D satisfies the first order linear relation $D(k) - 2\,D(k-1) = 0$ and the initial condition $D(0) = 5$ serves as an initial condition for D.

(b) If $C(k) = 3^{k-1} + 2^{k+1} + k$, $k \geq 0$, quite a bit more algebraic manipulation is required to get our result:

$C(k) = 3^{k-1} + 2^{k+1} + k$	Original equation
$3\,C(k-1) = 3^{k-1} + 3\cdot 2^{k} + 3\,(k-1)$	Substitute $k-1$ for k and multipy by 3
	Subtract the second equation from the first
$C(k) - 3\,C(k-1) = -2^{k} - 2\,k + 3$	3^{k-1} term is eliminated, this is a first order relation
$2\,C(k-1) - 6\,C(k-2) = -2^{k} - 2\,(2\,(k-1) + 3)$	Substitute $k-1$ for k in the 3rd equation, mult. by 2
	Subtract the fourth equation from the third equation
$C(k) - 5\,C(k-1) - 6\,C(k-2) = 2\,k - 7$	2^{k+1} term eliminated, this is a 2nd order relation

The recurrence relation that we have just obtained, defined for k ≥ 2, together with the initial conditions $C(0) = 7/3$ and $C(1) = 5$, define C. We could do more algebra to obtain a third-order linear relation in this case.

Table 8.3.1 summarizes our results together with a few other examples that we will let the reader derive. Based on these results, we might conjecture that any closed form expression for a sequence that combines exponential expressions and polynomial expressions will be solutions of finite order linear relations. Not only is this true, but the converse is true: a finite order linear relation defines a closed form expression that is similar to the ones that were just examined. The only additional information that is needed is a set of initial conditions.

Closed Form Expression	Recurrence Relation
$D(k) = 5\cdot 2^{k}$	$D(k) - 2\,D(k-1) = 0$
$C(k) = 3^{k-1} + 2^{k+1} + k$	$C(k) - 2\,C(k-1) - 6\,C(k-2) = 2\,k - 7$
$Q(k) = 2\,k + 9$	$Q(k) - Q(k-1) = 2$
$A(k) = k^{2} - k$	$A(k) - 2\,A(k-1) + A(k-2) = 2$
$B(k) = 2\,k^{2} + 1$	$B(k) - 2\,B(k-1) + B(k-2) = 4$
$G(k) = 2\cdot 4^{k} - 5\,(-3)^{k}$	$G(k) - G(k-1) + 12\,G(k-2) = 0$
$J(k) = (3 + k)\,2^{k}$	$J(k) - 4\,J(k-1) + 4\,J(k-2) = 0$

Table 8.3.1
Recurrence Relation Obtained from Certain Sequences

Definition: Homogeneous Recurrence Relation. *An n^{th} order linear relation is homogeneous if $f(k) = 0$ for all k. For each recurrence relation $S(k) + C_1\,S(k-1) + \ldots + C_n\,S(k-n) = f(k)$, the associated homogeneous relation is $S(k) + C_1\,S(k-1) + \ldots + C_n\,S(k-n) = 0$*

Example 8.3.4. $D(k) - 2\,D(k-1) = 0$ is a first-order homogeneous relation. Since it can also be written as $D(k) = 2\,D(k-1)$, it should be no surprise that it arose from an expression that involves powers of 2 (see Example 8.3.3a). More generally, you would expect that the solution of $L(k) - a\,L(k-1)$ would involve a^{k}. Actually, the solution is $L(k) = L(0)\,a^{k}$, where the value of $L(0)$ is given by the the initial condition.

Example 8.3.5. Consider the second-order homogeneous relation $S(k) - 7\,S(k-1) + 12\,S(k-2) = 0$ together with the initial conditions $S(0) = 4$ and $S(1) = 4$. From our discussion above, we can predict that the solution to this relation involves terms of the form $b\,a^{k}$, where b and a are nonzero constants that must be determined. If the solution were to equal this quantity exactly, then

$$S(k) = b\,a^{k}$$
$$S(k-1) = b\,a^{k-1}$$
$$S(k-2) = b\,a^{k-2}$$

Substitute these expressons into the recurrence relation to get

$$b\,a^{k} - 7\,b\,a^{k-1} + 12\,b\,a^{k-1} = 0 \qquad \text{(Eq 8.3 } a\text{)}$$

Each term on the left-hand side of the equation has a factor of $b\,a^{k-2}$, which is nonzero. Dividing through by this common factor yields

$$a^{2} - 7\,a + 12 = (a - 3)(a - 4) = 0. \quad \text{(Eq 8.3b)}$$

Therefore, the only possible values of a are 3 and 4. Equation (8.3b) is called the characteristic equation of the recurrence relation. The fact is that our original recurrence relation is true for any sequence of the form $S(k) = b_1\,3^{k} + b_2\,4^{k}$, where b_1 and b_2 are real numbers. This set of sequences is called the general solution of the recurrence relation. If we didn't have initial conditions for S, we would stop here. The initial conditions make it possible for us to obtain definite values for b_1 and b_2.

$$\left\{\begin{array}{c} S(0) = 4 \\ S(1) = 4 \end{array}\right\} \Rightarrow \left\{\begin{array}{c} b_1\,3^{0} + b_2\,4^{0} = 4 \\ b_1\,3^{1} + b_2\,4^{1} = 4 \end{array}\right\} \Rightarrow \left\{\begin{array}{c} b_1 + b_2 = 4 \\ 3\,b_1 + 4\,b_2 = 4 \end{array}\right\}$$

The solution of this set of simultaneous equations is $b_1 = 12$ and $b_2 = -8$ and so the solution is $S(k) = 12\;3^{k} - 8\;4^{k}$.

Definition: Characteristic Equation. *The characteristic equation of the homogeneous n^{th} order linear relation $S(k) + C_1\,S(k-1) + \ldots + C_n\,S(k-n) = 0$ is the nth degree polynomial equation*

$$a^n + \sum_{j=1}^{n} C_j\, a^{n-j} = a^n + C_1\, a^{n-1} + \cdots + C_{n-1}\, x + C_n = 0$$

The left-hand side of this equation is called the characteristic polynomial.

Example 8.3.6.

(a) The characteristic equation of $F(k) - F(k-1) - F(k-2) = 0$ is $a^2 - a - 1 = 0$.

(b) The characteristic equation of $Q(k) + 2\,Q(k-1) - 3\,Q(k-2) - 6\,Q(k-4) = 0$ is $a^4 + 2\,a^3 - 3\,a^2 - 6 = 0$. Note that the absence of a $Q(k-3)$ term means that there is not an $x^{4-3} = x$ term appearing in the characteristic equation.

Algorithm 8.3.1: Algorithm for Solving Homogeneous n^{th} Order Linear Relations.

(a) Write out the characteristic equation of the relation $S(k) + C_1\, S(k-1) + \ldots + C_n\, S(k-n) = 0$, *which is* $a^n + C_1\, a^{n-1} + \cdots + C_{n-1}\, x + C_n = 0$.

(b) Find all roots of the characteristic equation, called characteristic roots.

(c) If there are n distinct characteristic roots, $a_1, a_2, \ldots, a_n$, *then the general solution of the recurrence relation is* $S(k) = b_1\, a_1^k + b_2\, a_2^k + \cdots + b_n\, a_n^k$. *If there are fewer than n characteristic roots, then at least one root is a multiple root. If* a_j *is a double root, then the* $b_j\, a_j^k$ *term is replaced with* $\left(b_{j0} + b_{j1}\, k\right) a_j^k$. *In general, if* a_j *is a root of multiplicity p, then the* $b_j\, a_j^k$ *term is replaced with* $\left(b_{j0} + b_{j1}\, k + \cdots + b_{j(p-1)}\, k^{p-1}\right) a_j^k$.

(d) If n initial conditions are given, obtain n linear equations in n unknowns (the b_j*'s from Step (c)) by substitution. If possible, solve these equations to determine a final form for* $S(k)$.

Although this algorithm is valid for all values of n, there are limits to the size of n for which the algorithm is feasible. Using just a pencil and paper, we can always solve second-order equations. The quadratic formula for the roots of $a\,x^2 + b\,x + c = 0$ is

$$x = \frac{-b \pm \sqrt{b^2 - 4\,a\,c}}{2\,a}$$

The solutions of $a^2 + C_1\, a + C_2 = 0$ are then

$$\frac{1}{2}\left(-C_1 + \sqrt{C_1^{\,2} - 4\,C_2}\right) \quad \text{and} \quad \frac{1}{2}\left(-C_1 - \sqrt{C_1^{\,2} - 4\,C_2}\right)$$

Although cubic and quartic formulas exist, they are too lengthy to introduce here. For this reason, the only higher-order relations ($n \geq 3$) that you could be expected to solve by hand are ones for which there is an easy factorization of the characteristic polynomial.

Example 8.3.7. Suppose that T is defined by $T(k) = 7\,T(k-1) - 10\,T(k-2)$, with , $T(0) = 4$ and $T(1) = 17$. We can solve this recurrence relation with Algorithm 8.3.1:

(a) Note that we had written the recurrence relation in "nonstandard" form. To avoid errors in this easy step, you might consider a rearrangement of the equation to, in this case, $T(k) - 7\,T(k-1) + 10\,T(k-2) = 0$. Therefore, the characteristic equation is $a^2 - 7\,a + 10 = 0$.

(b) The characteristic roots are $\frac{1}{2}\left(7 + \sqrt{49 - 40}\right) = 5$ and $\frac{1}{2}\left(7 - \sqrt{49 - 40}\right) = 2$. These roots can be just as easily obtained by factoring the characteristic polynomial into $(a - 5)(a - 2)$.

(c) The general solution of the recurrence relation is $T(k) = b_1\, 2^k + b_2\, 5^k$,

(d) $$\left\{\begin{array}{c} T(0) = 4 \\ T(1) = 17 \end{array}\right\} \Rightarrow \left\{\begin{array}{c} b_1\, 2^0 + b_2\, 5^0 = 4 \\ b_1\, 2^1 + b_2\, 5^1 = 4 \end{array}\right\} \Rightarrow \left\{\begin{array}{c} b_1 + b_2 = 4 \\ 2\,b_1 + 5\,b_2 = 17 \end{array}\right\}$$

The simulations equations have the solution $b_1 = 1$ and $b_2 = 3$, Therefore, $T(k) = 2^k + 3 \cdot 5^k$.

Here is one rule that might come in handy: If the coefficients of the characteristic polynomial are all integers, with the constant term equal to m, then the only possible rational characteristic roots are divisors of m (both positive and negative).

With the aid of a computer (or possibly only a calculator), we can increase n. Approximations of the characteristic roots can be obtained by any of several well-known methods, some of which are part of standard software packages. There is no general rule that specifies the values of n for which numerical approximations will be feasible. The accuracy that you get will depend on the relation that you try to solve. (See Exercise 17 of this section.)

Example 8.3.8. Solve $S(k) - 7\,S(k-2) + 6\,S(k-3) = 0$, where $S(0) = 8$, $S(1) = 6$, and $S(2) = 22$.

(a) The characteristic equation is $a^3 - 7\,a + 6 = 0$.

(b) The only rational roots that we can attempt are ± 1, ± 2, ± 3, and ± 6. By checking these, we obtain the three roots 1, 2, and —3.

(c) The general solution is $S(k) = b_1\, 1^k + b_2\, 2^k + b_3(-3)^k$. The first term can simply be written b_1 .

(d) $\left\{\begin{array}{c} S(0) = 8 \\ S(1) = 6 \\ S(20 = 22 \end{array}\right\} \Rightarrow \left\{\begin{array}{c} b_1 + b_2 + b_3 = 8 \\ b_1 + 2\,b_2 - 3\,b_3 = 6 \\ b_1 + 4\,b_2 + 9\,b_3 = 22 \end{array}\right\}$

You can solve this system by elimination to obtain $b_1 = 5$, $b_2 = 2$, and $b_3 = 1$. Therefore,

$$S(k) = 5 + 2 \cdot 2^k + (-3)^k = 5 + 2^{k+1} + (-3)^k$$

Example 8.3.9. Solve $D(k) - 8\,D(k - I) + 16\,D(k - 2) = 0$, where $D(2) = 16$ and $D(3) = 80$.

(a) Characteristic equation; $a^2 - 8\,a + 16 = 0$.

(b) $a^2 - 8\,a + 16 = (a - 4)^2$. Therefore, there is a double characteristic root, 4.

(c) General solution: $D(k) = (b_{10} + b_{11}\,k)\,4^k$.

(d) $\left\{\begin{array}{c} D(2) = 16 \\ D(3) = 80 \end{array}\right\} \Rightarrow \left\{\begin{array}{c} (b_{10} + b_{11}\,2)\,4^2 = 16 \\ (b_{10} + b_{11}\,3)\,4^3 = 80 \end{array}\right\} \Rightarrow \left\{\begin{array}{c} 16\,b_{10} + 32\,b_{11} = 16 \\ 64\,b_{10} + 192\,b_{11} = 80 \end{array}\right\} \Rightarrow \left\{\begin{array}{c} b_{10} = \frac{1}{2} \\ b_{11} = \frac{1}{4} \end{array}\right\}$

Therefore $D(k) = (1/2 + (1/4)\,k)\,4^k = (2 + k)\,4^{k-1}$.

SOLUTION OF NONHOMOGENEOUS FINITE ORDER LINEAR RELATIONS

Our algorithm for nonhomogeneous relations will not be as complete as for the homogeneous case. This is due to the fact that different right-hand sides (f(k)'s) call for different procedures in obtaining a particular solution in Steps (b) and (c).

Algorithm 8.3.2: Algorithm for Solving Nonhomogeneous Finite Order Linear Relations.

To solve the recurrence relation $S(k) + C_1\,S(k - 1) + \ldots + C_n\,S(k - n) = f(k)$*:*

(a) Write the associated homogeneous relation and find its general solution (Steps (a) through (c) of Algorithm 8.3.1). Call this the homogeneous solution, $S^{(h)}(k)$*.*

(b) Start to obtain what is called a particular solution, $S^{(p)}(k)$ *of the recurrence relation by taking an educated guess at the form of a particular solu tion. For a large class of right-hand sides, this is not really a guess, since the particular solution is often the same type of function as* $f(k)$ *(see Table 8.3.2).*

Right Hand Side, $f(k)$	*Form of* a *particular Solution,* $S^{(p)}(k)$
constant, q	*constant,* d
linear function $q_0 + q_1\,k$	*linear function* $d_0 + d_1\,k$
m^{th} *degree polynomial,* $q_0 + q_1\,k + \cdots + q_m\,k^m$	m^{th} *degree polynomial,* $d_0 + d_1\,k + \cdots + d_m\,k^m$
exponential function $q\,a^k$	*exponential function* $d\,a^k$

Table 8.3.2
Particular Solutions for Given Right-hand Sides

(c) Substitute your guess from Step (b) into the recurrence relation. If you made a good guess, you should be able to determine the unknown coefficients of your guess. If you made a wrong guess, it should be apparent from the result of this substitution, so go back to Step (b).

(d) The general solution of the recurrence relation is the sum of the homogeneous and particular solutions. If no conditions are given, then you are finished. If n initial conditions are given, they will translate to n linear equations in n unknowns and solve the system, if possible, to get a complete solution.

Example 8.3.10. Solve $S(k) + 5\,S(k - 1) = 9$, with $S(0) = 6$.

(a) The associated homogeneous relation, $S(k) + 5\,S(k - 1) = 0$ has the characteristic equation $a + 5 = 0$; therefore, $a = -5$. The homogeneous solution is $S^{(h)}(k) = b\,(-5)^k$.

(b) Since the right-hand side is a constant, we guess that the particular solution will be a constant, d.

(c) If we substitute $S^{(p)}(k) = d$ into the recurrence relation, we get $d + 5\,d = 9$, or $6\,d = 9$. Therefore, $S^{(p)}(k) = 1.5$

(d) The general solution of the recurrence relation is

$$S(k) = S^{(h)}(k) + S^{(p)}(k) = b\,(-5)^k + 1.5$$

The initial condition will give us one equation to solve in order to determine b.

$$S(0) = 6 \Rightarrow b(-5)^0 + 1.5 = 6 \Rightarrow b + 1.5 = 6$$

Therefore, $b = 4.5$ and $S(k) = 4.5\,(-5)^k + 1.5$.

Example 8.3.11. Consider $T(k) - 7T(k-1) + 10T(k-2) = 6 + 8k$ with $T(0) = 1$ and $T(1) = 2$.

(a) From Example 8.3.7, we know that $T^{(h)}(k) = b_1 2^k + b_2 5^k$. Caution: Don't apply the initial conditions to $T^{(h)}$ until you add $T^{(p)}$!

(b) Since the right-hand side is a linear polynomial, $T^{(p)}$ is linear; that is, $T^{(p)}(k) = d_0 + d_1 k$.

(c) Substitution into the recurrence relation yields:

$$(d_0 + d_1 k) - 7(d_0 + d_1(k-1)) + 10(d_0 + d_1(k-2)) = 6 + 8k$$

$$\Rightarrow (4d_0 - 13d_1) + (4d_1)k = 6 + 8k$$

Two polynomials are equal only if their coefficients are equal. Therefore,

$$\left\{\begin{array}{c} 4d_0 - 13d_1 = 6 \\ 4d_1 = 8 \end{array}\right\} \Rightarrow \left\{\begin{array}{c} d_0 = 8 \\ d_1 = 2 \end{array}\right\}$$

(d) Use the general solution $T(k) = b_1 2^k + b_2 5^k + 8 + 2k$ and the initial conditions to get a final solution:

$$\left\{\begin{array}{c} T(0) = 1 \\ T(1) = 2 \end{array}\right\} \Rightarrow \left\{\begin{array}{c} b_1 + b_2 + 8 = 1 \\ 2b_1 + 5b_2 + 10 = 2 \end{array}\right\}$$

$$\Rightarrow \left\{\begin{array}{c} b_1 + b_2 = -7 \\ 2b_1 + 5b_2 = -8 \end{array}\right\}$$

$$\Rightarrow \left\{\begin{array}{c} b_1 = -9 \\ b_2 = 2 \end{array}\right\}$$

Therefore, $T(k) = -9 \cdot 2^k + 2 \cdot 5^k + 8 + 2k$

A quick note on interest rates: When a quantity, such as a savings account balance, is increased by some fixed percent, it is most easily computed with a multipier. In the case of an 8% increase, the multier is 1.08 because any original amount A, has $0.08A$ added to it, so that the new balance is

$$A + 0.08A = (1 + 0.08)A = 1.08A.$$

Another example is that if the interest rate is 3.5%, the multiplier would be 1.035. This presumes that the interest is applied a the end of year for 3.5% annual interest, often called *simple interest*. If the interest is applied monthly, and we assume a simplifed case where each month has the same length, the multiplier after every month would be $\left(1 + \frac{0.35}{12}\right) \approx 1.0292$. After a year passes, this multiplier would be applied 12 times, which is the same as multiplying by $1.0292^{12} \approx 1.3556$. That increase from 1.035 to 1.3556 is the effect of *compound interest*.

Example 8.3.12. Suppose you open a savings account that pays an annual interest rate of 8%. In addition, suppose you decide to deposit one dollar when you open the account, and you intend to double your deposit each year. Let $B(k)$ be your balance after k years. B can be described by the relation $B(k) = 1.08B(k-1) + 2^k$, with $S(0) = 1$. If, instead of doubling the deposit each year, you deposited a constant amount, q, the 2^k term would be replaced with q, A sequence of regular deposits such as this is called an annuity.

Returning to the original situation, we can obtain a closed form expression for $B^{(h)}$:

(a) $B^{(h)}(k) = b_1(1.08)^k$

(b) $B^{(p)}(k)$ should be of the form $d\,2^k$.

(c) $d\,2^k = 1.08\,d\,2^{k-1} + 2^k$

$$\Rightarrow (2d)2^{k-1} = 1.08\,d\,2^{k-1} + 2 \cdot 2^{k-1}$$
$$\Rightarrow 2d = 1.08d + 2$$
$$\Rightarrow .92d = 2$$
$$\Rightarrow d = 2.174 \text{ (to the nearest thousandth)}$$

Therefore $B^{(p)}(k) = 2.174 \cdot 2^k$

(d) $B(0) = 1 \Rightarrow b_1 + 2.174 = 1$

$$\Rightarrow b_1 = -1.174$$

$B(k) = -1.174 \cdot 1.08^k + 2.174 \cdot 2^k$.

Example 8.3.13. Find the general solution to $S(k) - 3S(k-1) - 4S(k-2) = 4^k$.

(a) The characteristic roots of the associated homogeneous relation are -1 and 4. Therefore, $S^{(h)}(k) = b_1(-1)^k + b_2 4^k$.

(b) A function of the form $d\,4^k$ will not be a particular solution of the nonhomogeneous relation since it solves the associated homogeneous relation. When the right-hand side involves an exponential function with a base that equals a characteristic root, you should multiply your guess at a particular solution by k. Our guess at $S^{(p)}(k)$ would then be $d\,k\,4^k$. See below for a more complete description of this procedure.

(c) Substitute $d\,k\,4^k$ into the recurrence relation for $S\,(k)$:

$$d\,k\,4^k - 3\,d\,(k-1)\,4^{k-1} - 4\,d\,(k-2)\,4^{k-2} = 4^k$$

$$16\,d\,k\,4^{k-2} - 12\,d\,(k-1)\,4^{k-2} - 4\,d\,(k-2)\,4^{k-2} = 4^k$$

Each term on the left-hand side has a factor of 4^{k-2}

$$\text{I}6\,d\,k - 12\,d\,(k-1) - 4\,d(k-2) = 4^2$$
$$20\,d = 16 \Rightarrow d = 0.8$$

Therefore, $S^{(p)}(k) = 0.8\,k\;4^4$

(d) The general solution to the recurrence relation is

$$S(k) = b_1(-1)^k + b_2\,4^k + 0.8\,k\,4^k$$

BASE OF RIGHT-HAND SIDE EQUAL TO CHARACTERISTIC ROOT

If the right-hand side of a nonhomogeneous relation involves an exponential with base a, and a is also a characteristic root of multiplicity p, then multiply your guess at a particular solution as prescribed in Table 8,3.2 by k^p , where k is the index of the sequence.

Example 8.3.14.

(a) If $S\,(k) - 9\,S\,(k-1) + 20\,S(k-2) = 2 \cdot 5^k$, the characteristic roots are 4 and 5. $S^{(p)}(k)$ will take the form $d\,k\,5^k$.

(b) If $S\,(n) - 6\,S\,(n-1) + 9\,S\,(n-2) = 3^{n+1}$ the only characteristic root is 3, but it is a double root (multiplicity 2). Therefore, the form of the particular solution is $d\,n^2\,3^n$.

(c) If $Q(j) - Q(j-1) - 12\,Q(j-2) = (-3)^j + 6 \cdot 4^j$, the characteristic roots are -3 and 4. The form of the particular solution will be $d_1\,j\,(-3)^j + d_2\,j \cdot 4^j$.

(d) If $S\,(k) - 9\,S\,(k-1) + 8\,S(k-2) = 9\,k + 1 = (9\,k + 1)\,1^k$, the characteristic roots are 1 and 8. If the right-hand side is a polynomial, as it is in this case, then the exponential factor 1^k can be introduced. The particular solution will take the form $k(d_0 + d_1\,k)$.

We conclude this section with a comment on the situation in which the characteristic equation gives rise to complex roots. If we restrict the coefficients of our finite order linear relations to real numbers, or even to integers, we can still encounter characteristic equations whose roots are complex. Here, we will simply take the time to point out that our algorithms are still valid with complex characteristic roots, but the customary method for expressing the solutions of these relations is different. Since an understanding of these representations requires some background in complex numbers, we will simply suggest that an interested reader can refer to a more advanced treatment of recurrence relations (see also difference equations).

EXERCISES FOR SECTION 8.3

A Exercises

Solve the following sets of recurrence relations and initial conditions:

1. $S\,(k) - 10\,S\,(k-1) + 9\,S\,(k-2) = 0,\; S\,(0) = 3,\; S\,(1) = 11$

2. $S\,(k) - 9\,S\,(k-1) + 18\,S\,(k-2) = 0\;\; S\,(0) = 0,\; S\,(1) = 3$

3. $S\,(k) - 0.25\,S\,(k-1) = 0\;,\; S\,(0) = 6$

4. $S\,(k) - 20\,S\,(k-1) + 100\,S\,(k-2) = 0,\; S\,(0) = 2,\; S\,(1) = 50$

5. $S\,(k) - 2\,S\,(k-1) + S\,(k-2) = 2\;\; S\,(0) = 25,\; S\,(1) = 16$

6. $S\,(k) - S\,(k-1) - 6\,S\,(k-2) = -30\;\; S\,(0) = 7,\; S\,(1) = 10$

7. $S\,(k) - 5\,S\,(k-1) = 5^k,\;\; S\,(0) = 3$

8. $S\,(k) - 5\,S\,(k-1) + 6\,S\,(k-2) = 2,\;\; S\,(0) = -1,\; S\,(1) = 0$

9. $S\,(k) - 4\,S\,(k-1) + 4\,S\,(k-2) = 3\,k + 2^k.\;\; S\,(0) = 1,\; S\,(1) = 1$

10. $S\,(k) = r\,S(k-1) + a\;,\;\; S\,(0) = 0,\;\; r,\; a \geq 0,\; r \neq 1$

11. $S\,(k) - 4\,S\,(k-1) - 11\,S\,(k-2) + 30\,S\,(k-3) = 0,$

    $S\,(0) = 0,\;\; S\,(1) = -35,\;\; S\,(2) = -85$

12. Find a closed form expression for $P\,(k)$ in Exercise 3 of Section 8.2.

13. (a) Find a closed form expression for the terms of the Fibonacci sequence (see Example 8.1.4).

(b) The sequence C was defined by C_r = the number of strings of zeros and ones with length r having no consecutive zeros (Example 8.2.1(c)). Its recurrence, relation is the same as that of the Fibonacci sequence. Determine a closed form expression for $C_r,\ r \geq 1$,

14. If $S(n) = \sum_{j=1}^{n} g(j),\ n \geq 1$, then S can be described with the recurrence relation $S(n) = S(n-1) + g(n)$. For each of the following sequences that are defined using a summation, find a closed form expression:

(a) $S(n) = \sum_{j=1}^{n} j, \quad n \geq 1$

(b) $Q(n) = \sum_{j=1}^{n} j^2,\ n \geq 1$

(c) $P(n) = \sum_{j=1}^{n} \left(\frac{1}{2}\right)^j,\ n \geq 0$

(d) $T(n) = \sum_{j=1}^{n} j^3,\ n \geq 1$

B Exercises

15. Let $D(n)$ be the number of ways that the set $\{1,\ 2,\ \ldots,\ n\}, n \geq 1$, can be partitioned into two nonempty subsets.

(a) Find a recurrence relation for D. (Hint: It will be a first-order linear relation.)

(b) Solve the recurrence relation.

16. If you were to deposit a certain amount of money at the end of each year for a number of years, this sequence of payment would be called an annuity (see Example 8.3.12,).

(a) Find a closed form expression for the balance or value of an annuity that consists of payments of q dollars at a rate of interest of i. Note that for a normal annuity, the first payment is made after one year.

(b) With an interest rate of 12.5%, how much would you need to deposit into an annuity to have a value of one million dollars after 18 years?

(c) The payment of a loan is a form of annuity in which the initial value is some negative amount (the amount of the loan) and the annuity ends when the value is raised to zero. How much could you borrow if you can afford to pay $5,000 per year for 25 years at 14% interest?

C Exercises

17. Suppose that C is a small positive number. Consider the recurrence relation $B(k) - 2B(k-1) + \left(1 - C^2\right)B(k - 2) = C^2$, with initial conditions $B(0) = 1$ and $B(1) = 1$. If C is small enough, we might consider approximating the relation by replacing $1 - C^2$ with 1 and C^2 with 0. Solve the original relation and its approximation. Let B_a a be the solution of the approximation. Compare closed form expressions for $B(k)$ and $B_a(k)$. Their forms are very different because the characteristic roots of the original relation were close together and the approximation resulted in one double characteristic root. If characteristic roots of a relation are relatively far apart, this problem will not occur. For example, compare the general solutions of

$S(k) + 1.001\,S(k-1) - 2.004002\,S(k-2) = 0.0001$ and

$S_a(k) + S_a(k-1) - 2\,S_a(k-2) = 0.$

8.4 Some Common Recurrence Relations

In this section we intend to examine a variety of recurrence relations that are not finite-order linear with constant coefficients. For each part of this section, we will consider a concrete example, present a solution, and, if possible, examine a more general form of the original relation.

Example 8.4.1. Consider the homogeneous first-order linear relation $S(n) - n\,S(n-1) = 0$, $n \geq 1$, with initial condition $S(0) = 1$. Upon close examination of this relation, we see that the nth term is n times the $(n-1)^{\text{st}}$ term, which is a property of n factorial. $S(n) = n!$ is a solution of this relation, for if $n \geq 1$,

$$S(n) = n! = n \cdot (n-1)! = n \cdot S(n-1).$$

In addition, since $0! = 1$, the initial condition is satisfied. It should be pointed out that from a computational point of view, our "solution" really isn't much of an improvement since the exact calculation of $n!$ takes $n - 1$ multiplications.

If we examine a similar relation, $G(k) - 2^k G(k-1)$, $k \geq 1$ with $G(0) = 1$, a table of values for G suggests a possible solution:

k	0	1	2	3	4	5
$G(k)$	1	2	2^3	2^6	2^{10}	2^{15}

The exponent of 2 in $G(k)$ is growing according to the relation $E(k) = E(k-1) + k$, with $E(0) = 0$. Thus $E(k) = \frac{k(k+1)}{2}$ and $G(k) = 2^{k(k+1)/2}$. Note that $G(k)$ could also be written as $2^0\, 2^1\, 2^2 \cdots 2^k$, for $k \geq 0$, but this is not a closed form expression.

In general, the relation $P(n) = f(n) P(n-1)$ for $n \geq 1$ with $P(0) = f(0)$, where f is a function that is defined for all $n \geq 0$, has the "solution"

$$P(n) = \prod_{k=0}^{n} f(k)$$

This product form of $P(n)$ is not a closed form expression because as n grows, the number of multiplications grow. Thus, it is really not a true solution. Often, as for $G(k)$ above, a closed form expression can be obtained from the product form.

Example 8.4.2. Analysis of a Binary Search Algorithm. Suppose you intend to use a binary search algorithm (see Example 8.1 .3) on lists of zero or more sorted items, and that the items are stored in an array, so that you have easy access to each item. A natural question to ask is "How much time will it take to complete the search?" When a question like this is asked, the time we refer to is often the so - called worst - case time. That is, if we were to search through n items, what is the longest amount of time that we will need to complete the search? In order to make an analysis such as this independent of the computer to be used, time is measured by counting the number of steps that are executed. Each step (or sequence of steps) is assigned an absolute time, or weight; therefore, our answer will not be in seconds, but in absolute time units. If the steps in two different algorithms are assigned weights that are consistent, then analyses of the algorithms can be used to compare their relative efficiencies. There are two major steps that must be executed in a call of the binary search algorithm:

(1) If the lower index is less than or equal to the upper index, then the middle of the list is located and its key is compared to the value that you are searching for.

(2) In the worst case, the algorithm must be executed with a list that is roughly half as large as in the previous execution. If we assume that Step 1 takes one time unit and $T(n)$ is the worst - case time for a list of n items, then

$$T(n) = 1 + T(\lfloor n/2 \rfloor) \qquad \text{for } n > 0 \qquad (8.4\text{ a})$$

For simplicity, we will assume that

$$T(0) = 0 \qquad (8.4\text{ b})$$

even though the conditions of Step 1 must be evaluated as false if $n = 0$. You might wonder why $n/2$ is truncated in 8.4a. If n is odd, then $n = 2k + 1$ for some $k \geq 0$, the middle of the list will be the $(k+1)^{\text{st}}$ item, and no matter what half of the list the search is directed to, the reduced list will have $k = \lfloor n/2 \rfloor$ items. On the other hand, if n is even, then $n = 2k$ for $k > 0$. The middle of the list will be the k^{th} item, and the worst case will occur if we are directed to the k items that come after the middle (the $(k + l)^{\text{st}}$ through $(2k)^{\text{th}}$ items). Again the reduced list has $\lfloor n/2 \rfloor$ items.

Solution to 8.4 a and 8.4 b. To determine $T(n)$, the easiest case is when n is a power of two. If we compute $T(2^m)$, $m \geq 0$, by iteration, our results are

$$\begin{aligned} T(1) &= 1 + T(0) = 1 \\ T(2) &= 1 + T(1) = 2 \\ T(4) &= 1 + T(2) = 3 \\ T(8) &= 1 + T(4) = 4. \end{aligned}$$

The pattern that is established makes it clear that $T(2^m) = m + 1$. This result would seem to indicate that every time you double the size of your list, the search time increases by only one unit.

A more complete solution can be obtained if we represent n in binary form. For each $n \geq 1$, there exists a non - negative integer r such that

$$2^{r-1} \leq n < 2^r \qquad (8.4\text{ c})$$

For example, if $n = 21$, $2^4 \leq 21 < 2^5$; therefore, $r = 5$. If n satisfies (8.4c), its binary representation requires r digits. For example, $21_{\text{ten}} = 10\,101_{\text{two}}$.

In general, $n = (a_1\, a_2 \ldots a_r)_{\text{two}}$. where $a_1 = 1$. Note that in this form, $\lfloor n/2 \rfloor$ is easy to describe: it is the $r-1$ digit binary number $(a_1\, a_2 \ldots a_{r-1})_{\text{two}}$

Therefore,

$$\begin{aligned} T(n) &= T(a_1\, a_2 \ldots a_r) \\ &= 1 + T(a_1\, a_2 \ldots a_{r-1}) \\ &= 1 + (1 + T(a_1\, a_2 \ldots a_{r-2})) \\ &= 2 + T(a_1\, a_2 \ldots a_{r-2}) \\ &\vdots \\ &= (r-1) + T(a_1) \\ &= (r-1) + 1 \qquad \text{since } T(1) = 1 \\ &= r \end{aligned}$$

From the pattern that we've just established, $T(n)$ reduces to r. A formal inductive proof of this statement is possible. However, we expect that most readers would be satisfied with the argument above. Any skeptics are invited to provide the inductive proof. If $n = 21$:

$$\begin{aligned} T(21) &= T(10\,101) \\ &= 1 + T(1010) \\ &= 1 + (1 + T(101)) \\ &= 1 + (1 + (1 + T(10))) \\ &= 1 + (1 + (1 + (1 + T(1)))) \\ &= 1 + (1 + (1 + (1 + (1 + T(0))))) \\ &= 5 \end{aligned}$$

Conclusion; The solution to 8.4 a and 8.4b is that for $n \geq 1$, $T(n) = r$, where $2^{r-1} \leq n < 2^r$.

A less cumbersome statement of this fact is that $T(n) = \lfloor \log_2 n \rfloor + 1$. For example, $T(21) = \lfloor \log_2 21 \rfloor + 1 = 4 + 1 = 5$.

REVIEW OF LOGARITHMS

Any discussion of logarithms must start by establishing a base, which can be any positive number other than 1. With the exception of Theorem 8.4.1, our base will be 2. We will see that the use of a different base (10 and $e \approx 2.171828$ are the other common ones) only has the effect of multiplying each logarithm by a constant. Therefore, the base that you use really isn't very important. Our choice of base 2 logarithms is convenient for the problems that we are considering.

The base 2 logarithm of a positive number represents an exponent and is defined by the following equivalence for any positive real number a.

$$\log_2 a = x \iff 2^x = a \;.$$

For example, $\log_2 8 = 3$ because $2^3 = 8$ and $\log_2 1.414 \approx 0.5$ because $2^{0.5} \approx 1.414$. A graph of the function $f(x) = \log_2 x$ in Figure 8.4.la shows that if $a < b$, the $\log_2 a < \log_2 b$; that is, when x increases, $\log_2 x$ also increases. However, if we move x from $2^{10} = 1024$ to $2^{11} = 2048$, $\log_2 x$ only increases from 10 to 11. This slow rate of increase of the logarithm function is an important point to remember. An algorithm acting on n pieces of data that can be executed in $\log_2 n$ time units can handle significantly larger sets of data than an algorithm that can be executed in $n/100$ or even $\sqrt{n}$ time units (see Figure 8.4.1b). The graph of $T(n) = \lfloor \log_2 n \rfloor + 1$ would show the same behavior.

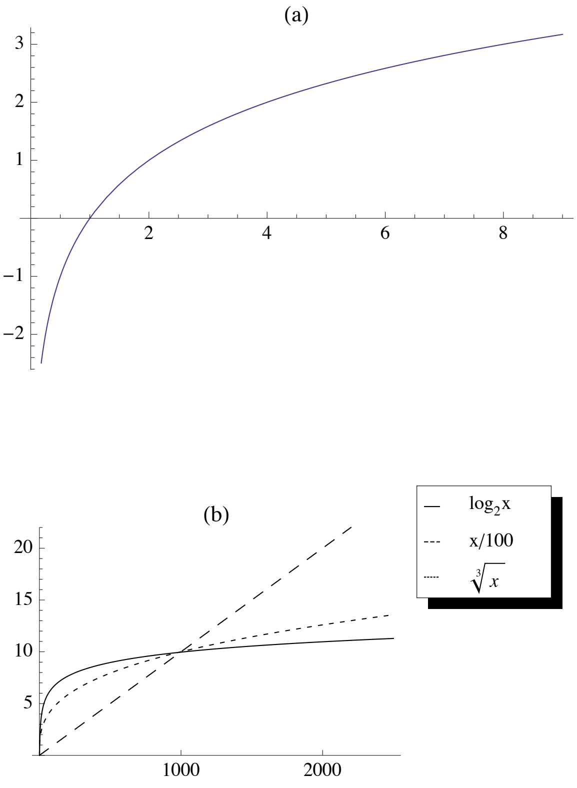


Figure 8.4.1 Log graphs

A few more properties that we will use in subsequent discussions involving logarithms are summarized in the following theorem.

Theorem 8.4.1. Fundamental Properties of Logarithms. Let a and b be positive real numbers, and r a real number.

$$\log_2 1 = 0 \qquad (8.4\text{ d})$$

$$\log_2 a\, b = \log_2 a + \log_2 b \qquad (8.4\text{ e})$$

$$\log_2 \tfrac{a}{b} = \log_2 a - \log_2 b \qquad (8.4\text{ f})$$

$$\log_2 a^r = r \log_2 a \qquad (8.4\text{ g})$$

$$2^{\log_2 a} = a \qquad (8.4\text{ h})$$

Returning to the binary search algorithm, we can derive the final expression for $T(n)$ using the properties of logarithms, including that the logarithm function is increasing so that inequalities are maintained when taking logarithms of numbers.

$$\begin{aligned} T(n) = r \quad &\Leftrightarrow \quad 2^{r-1} \leq n < 2^r \\ &\Leftrightarrow \quad \log_2 2^{r-1} \leq \log_2 n < \log_2 2^r \\ &\Leftrightarrow \quad r - 1 \leq \log_2 n < r \\ &\Leftrightarrow \quad r - 1 = \lfloor \log_2 n \rfloor \\ &\Leftrightarrow \quad T(n) = r = \lfloor \log_2 n \rfloor + 1 \end{aligned}$$

We can apply several of these properties of logarithms to get an alternate expression for $T(n)$:

$$\begin{aligned} \lfloor \log_2 n \rfloor + 1 &= \lfloor \log_2 n + 1 \rfloor \\ &= \lfloor \log_2 n + \log_2 2 \rfloor \\ &= \lfloor \log_2 2\, n \rfloor \end{aligned}$$

***Definition: Logarithms base b**, If $b > 0$, $b \neq 1$, then for $a > 0$,*

$$log_b\, a = x \Leftrightarrow b^x = a$$

Theorem 8.4.2. *Let $b > 0$, $b \neq 1$. Then for all $a > 0$, $\log_b a = \frac{\log_2 a}{\log_2 b}$. Therefore, if $b > 1$, base b logarithms can be obtained from base 2 logarithms by dividing by the positive scaling factor $\log_2 b$. If $b < 1$, this scaling factor is negative.*

Proof: By an analogue of 8.4f, $a = b^{\log_b a}$. Therefore, if we take the base 2 logarithm of both sides of this equality we obtain:

$$\begin{aligned} &\log_2 a = \log_2\left(b^{\log_2 a}\right) \\ &\Rightarrow \quad \log_2 a = \log_b a \, \log_2 b \end{aligned}$$

To obtain the desired result, divide both sides of this last equation by $\log_2 b$. ■

Note: $\log_2 10 \approx 3.32192$ and $\log_2 e = 1.55269$.

If the time that was assigned to Step 1 of the binary search algorithm is changed, we wouldn't expect the form of the solution to be very different. If $T(n) = a + T(\lfloor n/2 \rfloor)$ with $T(0) = c$, then $T(n) = c + a\lfloor \log_2 2n \rfloor$.

A further generalization would be to add a coefficient to $T(\lfloor n/2 \rfloor)$: $T(n) = a + b\,T(\lfloor n/2 \rfloor)$ with $T(0) = c$, where $a, b, c \in \mathbb{R}$, and $b \neq 0$ is not quite as simple to derive. First, if we consider values of n that are powers of 2:

$$\begin{aligned} &T(1) = a + b\,T(0) = a + b\,c \\ &T(2) = a + b(a + b\,c) = a + a\,b + c\,b^2 \\ &T(4) = a + b(a + a\,b + c\,b^2) = a + a\,b + a\,b^2 + c\,b^3 \\ &\quad\vdots \\ &T(2^r) = a + a\,b + a\,b^2 + \cdots + a\,b^r + c\,b^{r+1} \end{aligned}$$

If n is not a power of 2, by reasoning that is identical to what we used to solve 8.4a and 8.4b,

$$T(n) = \sum_{k=0}^{r} a\,b^k + c\,b^{r+1}$$

where $r = \lfloor \log_2 n \rfloor$.

The first term of this expression can be written in closed form. Let x be that sum:

$$\begin{aligned} x &= a + a\,b + a\,b^2 + \cdots + a\,b^r \\ b\,x &= \phantom{a + {}} a\,b + a\,b^2 + \cdots + a\,b^r + a\,b^{r+1} \end{aligned}$$

We've multiplied each term of x by b and aligned the identical terms in x and bx. Now if we subtract the two equations,

$$\begin{aligned} &x - b\,x = a - a\,b^{r+1} \\ &x(1 - b) = a(1 - b^{r+1}) \end{aligned}$$

Therefore,

$$x = a\,\frac{b^{r+1} - 1}{b - 1}$$

A closed form expression for $T(n)$ is

$$T(n) = a\,\frac{b^{r+1} - 1}{b - 1} + c\,b^{r+1} \text{ where } r = \lfloor \log_2 n \rfloor$$

Example 8.4.3. The efficiency of any search algorithm such as the binary search relies on fact that the search list is sorted according to a key value and that the search is based on the key value. There are several methods for sorting a list. One example is the bubble sort. You might be familiar with this one since it is a popular "first sorting algorithm." A time analysis of the algorithm shows that if $B(n)$ is the worst-case time needed to complete the bubble sort on n items, then $B(n) = (n - 1) + B(n - 1)$ and $B(1) = 0$. The solution of this relation is a quadratic function $B(n) = \frac{1}{2}(n^2 - n)$. The growth rate of a quadratic function such as this one is controlled by its squared term. Any other terms are dwarfed by it as n gets large. For the bubble sort, this means that if we double the size of the list that we are to sort, n changes to $2n$ and so n^2 becomes $4n^2$. Therefore, the time needed to do a bubble sort is quadrupled. One alternative to bubble sort is the merge sort. Here is a simple version of this algorithm for sorting $F = \{r(1), r(2), \ldots, r(n)\}$, $n \geq 1$. If $n = 1$, the list is sorted trivially. If $n \geq 2$ then:

(1) Divide F into $F_1 = \{r(1), \ldots, r(\lfloor n/2 \rfloor)\}$ and $F_2 = \{r(\lfloor n/2 \rfloor + 1), \ldots, r(n)\}$.

(2) Sort F_1 and F_2 using a merge sort.

(3) Merge the sorted lists F_1 and F_2 into one sorted list. If the sort is to be done in descending order of key values, you continue to choose the higher key value from the fronts of F_1 and F_2 and place them in the back of F.

Note that F_1 will always have $\lfloor n/2 \rfloor$ items and F_2 will have $\lceil n/2 \rceil$ items; thus, if n is odd, F_2 gets one more item than F_1. We will assume that the time required to perform Step 1 of the algorithm is insignificant compared to the other steps; therefore, we will assign a time value of zero to this step. Step 3 requires roughly n comparisons and n movements of items from F_1 and F_2 to F; thus, its time is proportional to n. For this reason, we will assume that Step 3 takes n time units. Since Step 2 requires $T(\lfloor n/2 \rfloor) + T(\lceil n/2 \rceil)$ time units,

$$T(n) = n + T(\lfloor n/2 \rfloor) + T(\lceil n/2 \rceil) \qquad (8.4i)$$

with the initial condition

$$T(1) = 0. \qquad (8.4j)$$

Instead of an exact solution of 8.4i and 8.4j, we will be content with an estimate for $T(n)$. First, consider the case of $n = 2^r$, $r \geq 1$:

$$\begin{aligned}
T(2^1) &= T(2) = 2 + T(1) + T(1) = 2 = 1 \cdot 2\\
T(2^2) &= T(4) = 4 + T(2) + T(2) = 8 = 2 \cdot 4\\
T(2^3) &= T(8) = 8 + T(4) + T(4) = 24 = 3 \cdot 8\\
&\vdots\\
T(2^r) &= r\, 2^r = 2^r \log_2 2^r
\end{aligned}$$

Thus, if n is a power of 2, $T(n) = n \log_2 n$. Now if, for some $r \geq 2$, $2^{r-1} \leq n \leq 2^r$, then $(r-1)\, 2^{r-1} \leq T(n) < r\, 2^r$. This can be proven by induction on r. As n increases from 2^{r-1} to 2^r, $T(n)$ increases from $(r-1)\, 2^{r-1}$to $r\, 2^r$ and is slightly larger than $\lfloor n \log_2 n \rfloor$. The discrepancy is small enough so that $T_e(n) = \lfloor n \log_2 n \rfloor$ can be considered a solution of 8.4i and 8.4j for the purposes of comparing the merge sort with other algorithms. Table 8.4.1 compares $B(n)$ with $T_e(n)$ for selected values of n.

Table 8.4.1
Comparison of Times for Bubble Sort and Merge Sort

n	$B(n)$	$T_e(n)$
10	45	34
50	1225	283
100	4950	665
500	124 750	4483
1000	499 500	9966

Definition: Derangement. *A derangement of a set A is a permutation of A (i.e., a bijection from A into A) such that* $f(a) \neq a$ *for all* $a \in A$.

Example 8.4.4. If $A = \{1, 2, \ldots, n\}$, an interesting question might be "How many derangements are there of A?" We know that our answer is bounded above by $n!$. We can also expect our answer to be quite a bit smaller than $n!$ since n is the image of itself for $(n-1)!$ of the permutations of A.

Let $D(n)$ be the number of derangements of $\{1, 2, \ldots, n\}$. Our answer will come from discovering a recurrence relation on D. Suppose that $n \geq 3$. If we are to construct a derangement of $\{1, 2, \ldots, n\}, f$, then $f(n) = k \neq n$. Thus, the image of n can be selected in $n-1$ different ways. No matter which of the $n-1$ choices we make, we can complete the definition of f in one of two ways. First, we can decide to make $f(k) = n$, leaving $D(n — 2)$ ways of completing the definition of f, since f will be a derangement of $\{1, 2, \ldots, n\} - \{n, k\}$. Second, if we decide to select $f(k) \neq n$, each of the $D(n-1)$ derangements of $\{1, 2, \ldots, n-1\}$ can be used to define f. If g is a derangement of $\{1, 2, \ldots, n-1\}$ such that $g(p) = k$, then define f by

$$f(j) = \begin{cases} n & \text{if } j = p \\ k & \text{if } j = n \\ g(j) & \text{otherwise} \end{cases}$$

Note that with our second construction of f, $f(f(n)) = f(k) \neq n$, while in the first construction, $f(f(n)) = f(k) = n$. Therefore, no derangement of $\{1, 2, \ldots, n\}$ with $f(n) = k$ can be constructed by both methods.

To recap our result, we see that f is determined by first choosing one of $n-1$ images of n and then constructing the remainder of f in one of $D(n-2) + D(n-1)$ ways. Therefore,

$$D(n) = (n-1)(D(n-2) + D(n-1)). \qquad (8.4k)$$

This homogeneous second-order linear relation with variable coefficients, together with the initial conditions $D(1) = 0$ and $D(2) = 1$, completely defines D. Instead of deriving a solution of this relation by analytical methods, we will give an empirical derivation of an approximation of $D(n)$. Since the derangements of $\{1, 2 \ldots, n\}$ are drawn from a pool of $n!$ permutations, we will see what percentage of these permutations are derangements by listing the values of $n!$, $D(n)$, and $\frac{D(n)}{n!}$. The results we obtain (see Table 8.4.2) indicate that as n grows, $\frac{D(n)}{n!}$ hardly changes at all. If this quotient is computed to eight decimal places, for $n \geq 12$, $D(n)/n! = 0.36787944$. The reciprocal of this number, which $D(n)/n!$ seems to be tending toward, is, to eight places, 2.71828182. This number appears in so many places in mathematics that it has its own name, e. An approximate solution of our recurrence relation on D is then $D(n) \approx \frac{n!}{e}$

n	D(n)	D(n)/n!
1	0	0
2	1	0.50000000
3	2	0.33333333
4	9	0.37500000
5	44	0.36666667
6	265	0.36805556
7	1854	0.36785714
8	14 833	0.36788194
9	133 496	0.36787919
10	1 334 961	0.36787946
11	14 684 570	0.36787944
12	176 214 841	0.36787944
13	2 290 792 932	0.36787944
14	32 071 101 049	0.36787944
15	481 066 515 734	0.36787944

Table 8.4.2
$D(n)$ compared to $n!$

EXERCISES FOR SECTION 8.4

A Exercises

1. Solve the following recurrence relations. Indicate whether your solution is an improvement over iteration.

(a) $n\,S(n) - S(n-1) = 0,\ S(0) = 1.$

(b) $T(k) + 3k\,T(k-1) = 0, T(0) = 1.$

(c) $U(k) - \frac{k-1}{k}\,U(k-1) = 0, k \geq 2, U(1) = 1.$

2. Prove that if $n \geq 0,\ \lfloor n/2 \rfloor + \lceil n/2 \rceil = n.$ (Hint: Consider the cases of n odd and n even separately.)

B Exercises

3. Solve as completely as possible:

(a) $T(n) = 3 + T(\lfloor n/2 \rfloor), T(0) = 0.$

(b) $T(n) = 1 + \frac{1}{2}T(\lfloor n/2 \rfloor),\ T(0) = 2.$

(c) $V(n) = 1 + V\lfloor n/8 \rfloor), V(0) = 0.$ (Hint: Write n in octal form.)

4. Prove by induction that if $T(n) = 1 + T(\lfloor n/2 \rfloor), T(0) = 0,$ and $2^{r-1} \leq n < 2^r$, $r \geq 1,$ then $T(n) = r.$ (Hint: Prove by induction on r.)

5. Use the substitution $S(n) = T(n+1)/T(n)$ to solve

$T(n)\,T(n-2) - T(n)^2 = 1$ for $n \geq 2,$ with $T(0) = 1, T(1) = 6,$ and $T(n) \geq 0.$

6. Use the substitution $G(n) = T(n)^2$ to solve

$T(n)^2 - T(n-1)^2 = 1$ for $n \geq 1,$ with $T(0) = 10.$

7. Solve as completely as possible:

(a) $Q(n) = 1 + Q\left(\left\lfloor \sqrt{n} \right\rfloor\right), n \geq 2, Q(1) = 0.$

(b) $R(n) = n + R(\lfloor n/2 \rfloor), n \geq 1, R(0) = 0.$

8. Suppose Step 1 of the merge sort algorithm did take a significant amount of time. Assume it takes 0.1 time unit, independent of the value of n:

(a) Write out a new recurrence relation for $T(n)$ that takes this factor into account;

(b) Solve for $T(2^r), r \geq 0;$

(c) Assuming the solution for powers of 2 is a good estimate for all n, compare your result to the solution in the text. As gets large, is there really much difference?

8.5 Generating Functions

This section contains an introduction to the topic of generating functions and how they are used to solve recurrence relations, among other problems. Methods that employ generating functions are based on the concept that you can take a problem involving sequences and translate it into a problem involving generating functions. Once you've solved the new problem, a translation back to sequences gives you a solution of the original problem.

This section covers:
(a) The definition of a generating function;
(b) Solution of a recurrence relation using generating functions to identify the skills needed to use generating functions;
(c) An introduction and/or review of the skills identified in point b;
(d) Some applications of generating functions.

Definition: Generating Function of a Sequence. *The generating function of a sequence S with terms $S_0, S_1, S_2, \ldots$ is the infinite sum*

$$G(S; z) = \sum_{n=0}^{\infty} S_n z^n = S_0 + S_1 z + S_2 z^2 + S_3 z^3 + \cdots$$

The domain and codomain of generating functions will not be of any concern to us since we will only be performing algebraic operations on them.

Example 8.5.1.

(a) If $S_n = 3^n, n \geq 0$, then

$$\begin{aligned} G(S; z) &= 1 + 3z + 9z^2 + 27z^3 + \cdots \\ &= \sum_{n=0}^{\infty} 3^n z^n \\ &= \sum_{n=0}^{\infty} (3z)^n \end{aligned}$$

We can get a closed form expression for $G(S; z)$ by observing that $G(S; z) - 3z\,G(S; z) = 1$. Therefore,

$$G(S; z) = \frac{1}{1-3z}.$$

(b) Finite sequences have generating functions. For example, the sequence of binomial coefficients $C(n;\ 0), C(n;\ 1), \ldots, C(n;\ n), n \geq 1$ has generating function

$$\begin{aligned} G(C(n;\ \cdot);\ z) &= C(n;\ 0) + C(n;\ 1)z + \cdots + C(n;\ n)z^n \\ &= \sum_{k=0}^{\infty} C(n; k) z^k \\ &= (1+z)^n \end{aligned}$$

by application of the binomial formula.

(c) If $Q(n) = n^2$,

$$G(Q; z) = \sum_{n=0}^{\infty} n^2 z^n = \sum_{k=0}^{\infty} k^2 z^k$$

Note that the index that is used in the summation has no significance. Also, note that the lower limit of the summation could start at 1 since $Q(0) = 0$.

SOLUTION OF A RECURRENCE RELATION USING GENERATING FUNCTIONS

Problem: Solve $S(n) - 2S(n-1) - 3S(n-2) = 0, n \geq 2$, with $S(0) = 3$ and $S(1) = 1$.

(1) Translate the recurrence relation into an equation about generating functions.

In our example, let $V(n) = S(n) - 2S(n-1) - 3S(n-2), n \geq 2$, with $V(0) = 0$ and $V(1) = 0$. Therefore,

$$G(V; z) = 0 + 0z + \sum_{n=2}^{\infty} (S(n) - 2S(n-1) - 3S(n-2))z^n = 0$$

(2) Solve for the generating function of the unknown sequence, $G(S, z) = \sum_{n=0}^{\infty} S_n z^n$.

$$\begin{aligned} 0 &= \sum_{n=2}^{\infty} (S(n) - 2S(n-1) - 3S(n-2))z^n \\ &= \sum_{n=2}^{\infty} S(n) z^n - 2\left(\sum_{n=2}^{\infty} S(n-1) z^n\right) - 3\left(\sum_{n=2}^{\infty} S(n-2) z^n\right) \end{aligned}$$

Close examination of the three sums above shows:

(a) $$\sum_{n=2}^{\infty} S_n z^n = \sum_{n=0}^{\infty} S_n z^n - S(0) - S(1) z$$
$$= G(S; z) - 3 - z$$

since $S(0) = 3$ and $S(1) = 1$.

(b) $$\sum_{n=2}^{\infty} S(n-1) z^n = z\left(\sum_{n=2}^{\infty} S(n-1) z^{n-1}\right)$$
$$= z\left(\sum_{n=1}^{\infty} S(n) z^n\right)$$
$$= z\left(\sum_{n=0}^{\infty} S(n) z^n - S(0)\right)$$
$$= z(G(S; z) - 3$$

(c) $$\sum_{n=2}^{\infty} S(n-2) z^n = z^2\left(\sum_{n=2}^{\infty} S(n-2) z^{n-2}\right)$$
$$= z^2 G(S; z)$$

Therefore,

$$(G(S; z) - 3 - z) - 2 z(G(S; z) - 3) - 3 z^2 G(S; z) = 0$$
$$\Rightarrow\ G(S; z) - 2 z\, G(S; z) - 3 z^2 G(S; z) = 3 - 5 z$$
$$\Rightarrow\ G(S; z) = \frac{3-5z}{1-2z-3z^2}.$$

(3) Determine the sequence whose generating function is the one obtained in Step 2,

For our example, we need to know one general fact about the closed form expression of an exponential sequence (a proof will be given later):

$$T(n) = b a^n, \quad n \geq 0 \quad \Leftrightarrow \quad G(T; z) = \frac{b}{1-a z} \qquad (8.5a)$$

Now, in order to recognize S in our example, we must write our closed form expression for $G(S; z)$ as a sum of terms like $G(T; z)$ above. Note that the denominator of $G(S; z)$ can be factored:

$$G(S; z) = \frac{3-5z}{1-2z-3z^2} = \frac{3-5z}{(1-3z)(1+z)}$$

If you look at this last expression for $G(S; z)$ closely, you can imagine how it could be the result of addition of two fractions,

$$\frac{3-5z}{(1-3z)(1+z)} = \frac{A}{1-3z} + \frac{B}{1+z} \qquad (8.5b)$$

where A and B are two real numbers that must be determined. Starting on the right of 8.5b, it should be clear that the sum, for any A and B, would look like the left-hand side. The process of finding values of A and B that make 8.5b true is called the partial fractions decomposition of the left-hand side:

$$\frac{A}{1-3z} + \frac{B}{1+z} = \frac{A(1+z)}{(1-3z)(1+z)} + \frac{B(1-3z)}{(1-3z)(1+z)}$$
$$= \frac{(A+B)+(A-3B)z}{(1-3z)(1+z)}$$

Therefore,

$$\left\{\begin{array}{c} A + B = 3 \\ A - 3B = -5 \end{array}\right\} \Rightarrow \left\{\begin{array}{c} A = 1 \\ B = 2 \end{array}\right\}$$

and

$$G(S; z) == \frac{1}{1-3z} + \frac{2}{1+z}$$

We can apply 8.5a to each term of G(S;z):

$\frac{1}{1-3z}$ is the generating function for $S_1(n) = 1 \cdot 3^n = 3^n$ and

$\frac{2}{1+z}$ is the generating function for $S_2(n) = 2(-1)^n$.

Therefore, $S(n) = 3^n + 2(-1)^n$.

From this example, we see that there are several skills that must be mastered in order to work with generating functions. You must be able to:

(a) Manipulate summation expressions and their indices (in Step 2).
(b) Solve algebraic equations and manipulate algebraic expressions, including partial function decompositions (Steps 2 and 3).
(c) Identify sequences with their generating functions (Steps 1 and 3).

We will concentrate on the last skill first, a proficiency in the other skills is a product of doing as many exercises and reading as many examples as possible.

First, we must identify the operations on sequences and on generating functions.

Operations on Sequences: Let S and T be sequences of numbers and let c be a real number. Define the sum $S + T$, the scalar product $c\,S$, the product $S\,T$, the convolution $S * T$, the pop operation $S\uparrow$ (read "S pop"), and the push operation $S\downarrow$ (read "S push") term-wise for $k \geq 0$ by

$$(S + T)(k) = S(k) + T(k)$$

$$(c\,S)(k) = c\,S(k)$$

$$(S\,T)(k) = S(k)\,T(k)$$

$$(S * T)(k) = \sum_{j=0}^{k} S(j)\,T(k-j)$$

$$(S\uparrow)(k) = S(k+1) \quad \text{and}$$

$$(S\downarrow)(k) = \begin{cases} 0 & \text{if } k = 0 \\ S(k-1) & \text{if } k > 0 \end{cases}.$$

If one imagines a sequence to be a matrix with one row and an infinite number of columns, $S + T$ and $c\,S$ are exactly as in matrix addition and scalar multiplication. There is no obvious similarity between the other operations and matrix operations.

The pop and push operations can be understood by imagining a sequence to be an infinite stack of numbers with $S(0)$ at the top, $S(1)$ next, etc., as in Figure 8.5.1a. The sequence $S\uparrow$ is obtained by "popping" S(0) from the stack, leaving a stack as in Figure 8.5.1b, with S(1) at the top, S(2) next, etc. The sequence S I is obtained by placing a zero at the top of the stack, resulting in a stack as in Figure 8.5.1c. Keep these figures in mind when we discuss the pop and push operations.

$S(0)$	$S(1)$	0
$S(1)$	$S(2)$	$S(0)$
$S(2)$	$S(3)$	$S(1)$
$S(3)$	$S(4)$	$S(2)$
$S(4)$	$S(5)$	$S(3)$
$\vdots$	$\vdots$	$\vdots$
(a)	(b)	(c)

FIGURE 8.5.1
Stack interpretation of pop and push operation

Example 8.5.2. If $S(n) = n, T(n) = n^2,\ U(n) = 2^n$, and $R(n) = n\,2^n$,

(a) $(S + T)(n) = n + n^2$

(b) $(U + R)(n) = 2^n + n\,2^n = (1+n)\,2^n$

(c) $(2\,U)(n) = 2 \cdot 2^n = 2^{n+1}$

(d) $\left(\frac{1}{2}\,R\right)(n) = \frac{1}{2}\,n\,2^n = n\,2^{n-1}$

(e) $(S\,T)(n) = n\,n^2 = n^3\,2 = \text{n}\;3$

(f) $$(S * T)(n) = \sum_{j=0}^{n} S(j)\,T(n-j) = \sum_{j=0}^{n} j\,(n-j)^2$$

$$= \sum_{j=0}^{n} (\,j\,n^2 - 2\,n\,j^2 + j^3)$$

$$= n^2 \sum_{j=0}^{n} j - 2\,n \sum_{j=0}^{n} j^2 + \sum_{j=0}^{n} j^3$$

$$= n^2\left(\tfrac{n(n+1)}{2}\right) - 2\,n\left(\tfrac{(2\,n+1)(n+1)\,n}{6}\right) + \tfrac{1}{4}\,n^2\,(n+1)^2$$

by Exercise 14 of Section 8.3.

$$= \tfrac{n^2(n+1)(n-1)}{12}$$

(g) $$(U * U)(n) = \sum_{j=0}^{n} U(j)\, U(n-j)$$

$$= \sum_{j=0}^{n} 2^j\, 2^{n-j}$$

$$= (n+1)\, 2^n$$

(h) $(S\uparrow)(n) = n+1$

(i) $(S\downarrow)(n) = \max(0, n-1)$

(j) $((S\downarrow)\downarrow)(n) = \max(0, n-2)$

(k) $(U\downarrow)(n) = \begin{cases} 2^{n-1} & \text{if } n > 0 \\ 0 & \text{if } n = 0 \end{cases}$

(l) $((U\downarrow)\uparrow)(n) = (U\downarrow)(n+1) = 2^n = U(n)$

(m) $((U\uparrow)\downarrow)(n) = \begin{cases} 0 & \text{if } n = 0 \\ U(n) & \text{if } n > 0 \end{cases}$

Note that $(U\downarrow)\uparrow \neq (U\uparrow)\downarrow$

Definition: Multiple Pop and Push: *If S is a sequence of numbers, define*

$$S\uparrow p = (S\uparrow(p-1))\uparrow \text{ if } p \geq 2 \text{ and } S\uparrow 1 = S\uparrow.$$

Similarly, define

$$S\downarrow p = (S\downarrow(p-1))\downarrow \text{ if } p \geq 2 \text{ and } S\downarrow 1 = S\downarrow.$$

Notice that

$$(S\uparrow 2)(k) = ((S\uparrow 1)\uparrow)(k) = ((S\uparrow)\uparrow)(k) = (S\uparrow)(k+1) = k+2$$

In general,

$$(S\uparrow p)(k) = S(k+p), \text{ and}$$

$$(S\downarrow p)(k) = \begin{cases} 0 & \text{if } k < p \\ S(k-p) & \text{if } k \geq p \end{cases}$$

Operations on Generating Functions

If

$$G(z) = \sum_{k=0}^{\infty} a_k z^k \text{ and } H(z) = \sum_{k=0}^{\infty} b_k z^k$$

are generating functions and c is a real number, then the sum $G + H$, scalar product $c\,G$, product $G\,H$, and monomial product $z^p\,G$, $p \geq 1$ are generating functions, where

$$(G+H)(z) = \sum_{k=0}^{\infty} (a_k + b_k)\, z^k$$

$$(c\,G)(z) = \sum_{k=0}^{\infty} c\, a_k\, z^k$$

$$(G\,H)(z) = \sum_{k=0}^{\infty} c\, z^k \quad \text{where } c_k = \sum_{j=0}^{k} a_j\, b_{k-j}$$

$$(z^p\,G)(z) = z^p \sum_{k=0}^{\infty} a_k\, z^k = \sum_{k=0}^{\infty} a_k\, z^{k+p} = \sum_{n=p}^{\infty} a_{n-p}\, z^n$$

The last sum is obtained by substituting $n - p$ for k in the previous sum.

Example 8.5.3. If

$$D(z) = \sum_{k=0}^{\infty} k\, z^k \text{ and } H(z) = \sum_{k=0}^{\infty} 2^k\, z^k$$

then

$$(D + H)(z) = \sum_{k=0}^{\infty} \left(k + 2^k\right) z^k$$

$$(2\,H)(z) = \sum_{k=0}^{\infty} 2 \cdot 2^k z^k = \sum_{k=0}^{\infty} 2^{k+1} z^k$$

$$\begin{aligned}(z\,D)(z) &= z \sum_{k=0}^{\infty} k\ z^k = \sum_{k=0}^{\infty} k\ z^{k+1} = \sum_{k=1}^{\infty} (k-1)\, z^k \\ &= D(z) - \sum_{k=1}^{\infty} z^k\end{aligned}$$

$$(D\,H)(z) = \sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} j\, 2^{k-j} \right) z^k$$

$$(H\,H)(z) = \sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} 2^j\, 2^{k-j} \right) z^k = \sum_{k=0}^{\infty} (k+1)\, 2^k z^k$$

Note: $D(z) = G(S; z)$, and $H(z) = G(U; z)$ from Example 8.5.2. Now we establish the connection between the operations on sequences and generating functions. Let S and T be sequences and let c be a real number;

$$\begin{aligned} G(S + T; z) &= G(S; z) + G(T; z) && (8.5\,c) \\ G(c\,S; z) &= c\,G(S; z) && (8.5\,d) \\ G(S * T; z) &= G(S; z)\,G(T; z) && (8.5\,e) \\ G(S\uparrow; z) &= (G(S; z) - S(0))/z && (8.5\,f) \\ G(S\downarrow; z) &= z\,G(S; z) && (8.5\,g) \end{aligned}$$

In words, 8.5c says that the generating function of the sum of two sequences equals the sum of the generating functions of those sequences. Take the time to write out the other four identities in your own words. From the previous examples, these identities should be fairly obvious, with the possible exception of the last two. We will prove 8.5f as part of the next theorem and leave the proof of 8.5g to the interested reader. Note that there is no operation on generating functions that is related to sequence multiplication; that is, $G(S\,T; z)$ cannot be simplified.

Theorem 8.5.1. *If $p > 1$,*

(a) $G(S\uparrow p; z) = \left(G(S; z) - \sum_{k=0}^{p-1} S(k)\, z^k \right) \Big/ z^k$

(b) $G(S\downarrow p; z) = z^p\, G(S; z).$

Proof of Part (a): The proof is by induction. Basis:

$$\begin{aligned} G(S\uparrow, z) &= \sum_{k=0}^{\infty} S(k+1)\, z^k = \sum_{k=1}^{\infty} S(k)\, z^{k-1} \\ &= \left(\sum_{k=1}^{\infty} S(k)\, z^k \right) \Big/ z \\ &= \left(S(0) + \sum_{k=1}^{\infty} S(k)\, z^k - S(0) \right) \Big/ z \\ &= (G(S; z) - S(0))/z \end{aligned}$$

Therefore, part (a) is true for $p = 1$.

Induction, Suppose that for some $p \geq 1$, the statement in part (a) is true:

$$\begin{aligned} G(S\uparrow(p+1); z) &= G((S\uparrow p)\uparrow; z) \\ &= (G(S\uparrow p\,; z) - (S\uparrow p)\,(0))/z \quad \text{by the basis} \\ &= \frac{\dfrac{\left(G(S;z) - \sum_{k=0}^{p-1} S(k)\, z^k\right)}{z^p} - S(p)}{z} \end{aligned}$$

by the induction hypothesis. Now write $S(p)$ in the last expression above as $(S(r)\, z^p\,)/z^p$ so that it fits into the finite summation:

$$\begin{aligned} G(S\uparrow(p+1); z) &= \left(\frac{G(S;z) - \sum_{k=0}^{p} S(k)\, z^k}{z^p} \right) \Big/ z \\ &= \left(G(S; z) - \sum_{k=0}^{p} S(k)\, z^k \right) \Big/ z^{p+1} \end{aligned}$$

Therefore the statement is true for $p+1$. ■

CLOSED FORM EXPRESSIONS FOR GENERATING FUNCTIONS

The most basic tool used to express generating functions in closed form is the closed form expression for the geometric series, which is an expression of the form $a + ar + ar^2 + \cdots$. It can either be terminated or extended infinitely.

Finite Geometric Series: $a + ar + ar^2 + \cdots + ar^n = a\left(\frac{1-r^{n+1}}{1-r}\right)$ (8.5h)

Infinite Geometric Series: $a + ar + ar^2 + \cdots = \frac{a}{1-r}$ (8.5i)

Restrictions: a and r represent constants and the right sides of the two equations apply under the following conditions:

(1) r must not equal 1 in the finite case. Note that $a + ar + \cdots ar^n = (n+1)a$ if $r = 1$.

(2) In the infinite case, the absolute value of r must be less than 1.

These restrictions don't come into play with generating functions. We could derive 8.5h by noting that if $S(n) = a + ar + \cdots + ar^n, n > 0$, then $S(n) = rS(n-1) + a$ (See Exercise 10 of Section 8.3). An alternative derivation was used in Section 8.4. We will take the same steps to derive 8.5i. Let

$$\begin{aligned} x &= a + ar + ar^2 + \cdots \\ rx &= \quad\;\; ar + ar^2 + \cdots \\ x - rx &= a \end{aligned}$$

Therefore, $x = \frac{a}{1-r}$.

Example 8.5.4.

(a) If $S(n) = 9 \cdot 5^n, n \geq 0$, $G(S;z)$ is an infinite geometric series with $a = 9$ and $r = 5z$. Therefore,

$$G(S;z) = \frac{9}{1-5z}.$$

(b) If $T(n) = 4, n \geq 0$, then $G(T;z) = 4/(1-z)$.

(c) If $U(n) = 3(-1)^n$, then $G(U;z) = 3/(1+z)$.

(d) Let $C(n) = S(n) + T(n) + U(n) = 9 \cdot 5 + 4 + 3(-1)^n$. Then

$$\begin{aligned} G(C;z) &= G(S;z) + C(T;z) + G(U;z) \\ &= \frac{9}{1-5z} + \frac{4}{1-z} + \frac{3}{1+z} \\ &= -\frac{14z^2+34z-16}{5z^3-z^2-5z+1} \end{aligned}$$

Given a choice between the last form of $G(C;z)$ and the previous sum of three fractions, we would prefer leaving it as a sum of three functions. As we saw in an earlier example, a partial fractions decomposition of a fraction such as the last expression requires some effort to produce.

(e) If $G(Q;z) = 34/(2-3z)$, then Q can be determined by multiplying the numerator and denominator by 1/2 to obtain $\frac{17}{1-\frac{3}{2}z}$. We recognize this fraction as the sum of the infinite geometric series with $a = 17$ and $r = \frac{3}{2}z$. Therefore $Q(n) = 17(3/2)^n$.

(f) If $G(A;z) = (1+z)^3$, then we expand $(1+z)^3$ to $l + 3z + 3z^2 + z^{\square}$. Therefore $A(0) = 1, A(1) = 3$ $A(2) = 3, A(3) = 1$, and, since there are no higher-powered terms, $A(n) = 0, n \geq 4$. A more concise way of describing A is $A(k) = C(3;k)$, since $C(n;k)$ is usually interpreted as 0 of $k > n$.

Table 8.5.1 contains some closed form expressions for the generating functions of some common sequences.

Sequence	Generating Function
$S(k) = b a^k$	$G(S;z) = \frac{b}{1-az}$
$S(k) = k$	$G(S;z) = \frac{z}{(1-z)^2}$
$S(k) = b k a^k$	$G(S;z) = \frac{abz}{(1-az)^2}$
$S(k) = \frac{1}{k!}$	$G(S;z) = e^z$
$S(k) = \begin{cases} C(n;k) & 0 \leq k \leq n \\ 0 & k > n \end{cases}$	$G(S;z) = (1+z)^n$

Table 8.5.1

Closed Form Expressions of some Generating Functions

Example 8.5.5. Solve $S(k) + 3S(k-1) - 4S(k-2) = 0$, $k \geq 2$, with $S(0) = 3$ and $S(1) = -2$. The solution will be obtained using the same steps that were used earlier in this section, with one variation.

(1) Translate to an equation about generating functions. First, we change the index of the recurrence relation by substituting $n + 2$ for k. The result is $S(n+2) + 3S(n+1) - 4S(n) = 0$, $n \geq 0$. Now, if $V(n) = S(n+2) + 35(n+1) - 4S(n)$, then V is the zero sequence, which has a zero generating function. Furthermore, $V = S\uparrow 2 + 3(S\uparrow) - 4S$. Therefore,

$$\begin{aligned} 0 &= G(V;z) \qquad . \\ &= G(S\uparrow 2;\, z) + 3\,G(S\uparrow;\, z) - 4\,G(S;z) \\ &= \frac{G(S;z) - S(0) - S(1)\,z}{z^2} + 4\,\frac{(G(S;z) - S(0))}{z} - 4\,G(S;z) \end{aligned}$$

(2) We want to now solve the following equation for $G(S;z)$:

$$\frac{G(S;z) - S(0) - S(1)\,z}{z^2} + 4\,\frac{(G(S;z) - S(0))}{z} - 4\,G(S;z) = 0$$

Multiply by z^2 :

$$G(S;z) - 3 + 2z + 3z(G(S;z) - 3) - 4z^2\,G(S;z) = 0$$

Expand and collect all terms involving $G(S;z)$ on one side of the equation:

$$G(S;z) + 3z\,G(S;z) - 4z^2\,G(S;z) = 3 + 7z$$

$$(1 + 3z - 4z^2)\,G(S;z) = 3 + 7z$$

Therefore,

$$G(S;z) = \frac{3+7z}{1+3z-4z^2}$$

(3) Determine S from its generating function.

$$1 + 3z - 4z^2 = (1+4z)(1-z)$$

thus a partial fraction decomposition of $G(S;z)$ would be:

$$\begin{aligned} \frac{A}{1+4z} + \frac{B}{1-z} &= \frac{A\,z - A - 4\,B\,z - B}{(z-1)(4z+1)} \\ &= \frac{(A+B) + (4\,B - A)\,z}{(z-1)(4z+1)} \end{aligned}$$

Therefore, $A + B = 3$ and $4B - A = 7$. The solution of this set of equations is $A = 1$ and $B = 2$.

$$G(S;z) = \frac{1}{1+4z} + \frac{2}{1-z}$$

$\frac{1}{1+4z}$ is the generating function of $S_1(n) = (-4)^n$, and

$\frac{2}{1-z}$ is the generating function of $S_2(n) = 2(1)^n = 2$.

In conclusion, since $G(S;z) = G(S_1;z) + G(S_2;z)$, $S(n) = 2 + (-4)^n$.

Example 8.5.6. Let $A = \{a, b, c, d, e\}$ and let A^* be the set of all strings of length zero or more that can be made using each of the elements of A zero or more times. By the generalized rule of products, there are 5^n such strings that have length n, $n \geq 0$, Suppose that X_n is the set of strings of length n with the property that all of the a's and b's precede all of the c's, d's, and e's. Thus aaabde $\in X_6$, but abcabc $\notin X_6$. Let $R(n) = |X_n|$. A closed form expression for R can be obtained by recognizing R as the convolution of two sequences. To illustrate our point, we will consider the calculation of $R(6)$.

Note that if a string belongs to X_6, it starts with k characters from $\{a, b\}$ and is followed by $6 - k$ characters from $\{c, d, e\}$. Let $S(k)$ be the number of strings of a's and b's with length k and let $T(k)$ be the number of strings of c's, d's, and e's with length k. By the generalized rule of products, $S(k) = 2^k$ and $T(k) = 3^k$. Among the strings in X_6 are the ones that start with two a's and b's and end with c's, d's, and e's. There are $S(2)\,T(4)$ such strings. By the law of addition, $|X_6| = R(6) = S(0)\,T(6) + S(1)\,T(5) + \cdots + S(5)\,T(1) + S(6)\,T(0)$. Note that the sixth term of R is the sixth term of the convolution of S with T, $S * T$. Think about the general situation for a while and it should be clear that $R = S * T$. Now, our course of action will be to:

(a) Determine the generating functions of S and T,
(b) Multiply $G(S;z)$ and $G(T;z)$ to obtain $G(S*T;z) = G(R;z)$ (by 10.5e), and
(c) Determine R on the basis of $G(R;z)$.

(a) $G(S;z) = \sum_{k=0}^{\infty} 2^k z^k = \frac{1}{1-2z}$, and $G(T;z) = \sum_{k=0}^{\infty} 3^k z^k = \frac{1}{1-3z}$

(b) $G(R;z) = G(S;z)\,G(T;z) = \frac{1}{(1-2z)(1-3z)}$

(c) To recognize R from $G(R; z)$, we must do a partial fractions decomposition:

$$\frac{1}{(1-2z)(1-3z)} = \frac{A}{1-2z} + \frac{B}{1-3z} = \frac{-3Az+A-2Bz+B}{(2z-1)(3z-1)} = \frac{(A+B)+(-3A-2B)z}{(2z-1)(3z-1)}$$

Therefore, $A + B = 1$ and $-3A - 2B = 0$. The solution of this pair of equations is $A = -2$ and $B = 3$.

Since

$$G(R; z) = \frac{-2}{1-2z} + \frac{3}{1-3z},$$

which is the sum of the generating functions of $-2(2)^k$ and $3(3)^k$,

$$R(k) = -2(2)^k + 3(3)^k = 3^{k+1} - 2^{k+1}$$

For example, $R(6) = 3^7 - 2^7 = 2187 - 128 = 2059$. Naturally, this equals the sum that we get from $(S*T)(6)$. To put this number in perspective, the total number of strings of length 6 with no restrictions is $5^6 = 15625$, and $\frac{2059}{15625} \approx 0.131776$. Therefore approximately 13% of the strings of length 6 satisfy the conditions of the problem.

EXTRA FOR EXPERTS

The remainder of this section is intended for readers who have had, or who intend to take, a course in combinatorics. We do not advise that it be included in a typical course. The method that was used in Example 8.5.6 is a very powerful one and can be used to solve many problems in combinatorics. We close this section with a general description of the problems that can be solved in this way, followed by some examples.

Consider the situation in which $P_1, P_2, \ldots, P_m$ are m actions that must be taken, each of which results in a well-defined outcome. For each $k = 1, 2, \ldots, m$ define X_k to be the set of possible outcomes of P_k . We will assume that each outcome can be quantified in some way and that the quantification of the elements of X_k is defined by the function $Q_k : X_k \to \{0, 1, 2, \ldots\}$. Thus, each outcome has a non-negative integer associated with it. Finally, define a frequency function $F_k : \{0, 1, 2, \ldots\} \to \{0, 1, 2, \ldots\}$ such that $F_k(n)$ is the number of elements of X_k that have a quantification of n.

Now, based on these assumptions, we can define the problems that can be solved. If a process P is defined as a sequence of actions $P_1, P_2, \ldots, P_m$ as above, and if the outcome of P, which would be an element of $X_1 \times X_2 \times \cdots \times X_m$, is quantified by

$$Q(a_1, a_2, \ldots, a_m) = \sum_{k=1}^{m} Q_k(a_k),$$

then the frequency function, F, for P is the convolution of the frequency functions for $P_1, P_2, \ldots, P_m$, which has a generating function equal to the product of the generating functions of the frequency functions $F_1, F_2, \ldots, F_m$. That is,

$$G(F; z) = G(F_1; z)\, G(F_2; z) \cdots \mathrm{G}(F_m; z) \qquad (8.5j)$$

Example 8.5.7. Suppose that you roll a die two times and add up the numbers on the top face for each roll. Since the faces on the die represent the integers 1 through 6, the sum must be between 2 and 12. How many ways can any one of these sums be obtained? Obviously, 2 can be obtained only one way, with two 1's. There are two sequences that yield a sum of 3: 1-2 and 2-1. To obtain all of the frequencies with which the numbers 2 through 12 can be obtained, we set up the situation as follows. For $j = 1, 2$; P_j is the rolling of the die for the j^{th} time. $X_j = \{1, 2, \ldots, 6\}$ and $Q_j : X_j {-}{>} \{0, 1, 2, 3, \ldots\}$ is defined by $Q_j(x) = x$. Since each number appears on a die exactly once, the frequency function is $F_j(k) = 1$ if $1 \leq k \leq 6$, and $F_j(k) = 0$ otherwise. The process of rolling the die two times is quantified by adding up the Q_j's; that is, $Q(a_1, a_2) = Q_1(a_1) + Q_2(a_2)$. The generating function for the frequency function of rolling the die two times is then

$$\begin{aligned} G(F; z) &= G(F_1; z)\, G(F_2; z) \\ &= \left(z^6 + z^5 + z^4 + z^3 + z^2 + z\right)^2 \\ &= \left(z^{12} + 2z^{11} + 3z^{10} + 4z^9 + 5z^8 + 6z^7 + 5z^6 + 4z^5 + 3z^4 + 2z^3 + z^2\right) \end{aligned}$$

Now, to get $F(k)$, just read the coefficient of z^k. For example, the coefficient of z^5 is 4, so there are four ways to roll a total of 5 .

To apply this method, the crucial step is to decompose a large process in the proper way so that it fits into the general situation that we've described.

Example 8.5.8. Suppose that an organization is divided into three geographic sections, A, B, and C. Suppose that an executive committee of 11 members must be selected so that no more than 5 members from any one section are on the committee and that Sections A, B, and C must have minimums of 3, 2, and 2 members, respectively, on the committee. Looking only at the number of members from each section on the committee, how many ways can the committee be made up? One example of a valid committee would be 4 A's, 4 B's, and 3 C's.

Let P_A be the action of deciding how many members (not who) from Section A will serve on the committee. $X_A = \{3, 4, 5\}$ and $Q_A(k) = k$. The frequency function, F_A , is defined by $F_A(k) = 1$ if $k \in X_k$, with $F_A(k) = 0$ otherwise. $G(F_A; z)$ is then $z^3 + z^4 + z^5$. Similarly, $G(F_B; z) = z^2 + z^3 + z^4 + z^5 = G(F_C; z)$. Since the committee must have 11 members, our answer will be the coefficient of z^{11} in $G(F_A; z)\, G(F_B; z)\, G(F_C; z)$, which is 10:

$$\begin{aligned} G(F_A; z)\, G(F_B; z)\, G(F_C; z) &= \left(z^3 + z^4 + z^5\right)\left(z^2 + z^3 + z^4 + z^5\right)^2 \\ &= z^{15} + 3\, z^{14} + 6\, z^{13} + 9\, z^{12} + 10\, z^{11} + 9\, z^{10} + 6\, z^9 + 3\, z^8 + z^7 \end{aligned}$$

EXERCISES FOR SECTION 8.5

A Exercises

1. What sequences have the following generating functions?

(a) 1

(b) $\frac{10}{2-z}$

(c) $1 + z$

(d) $\frac{3}{1+2\,z} + \frac{3}{1-3\,z}$

2. What sequences have the following generating functions?

(a) $\frac{1}{1+z}$

(b) $\frac{1}{4-3\,z}$

(c) $\frac{2}{1-z} + \frac{1}{1+z}$

(d) $\frac{z+2}{z+3}$

B Exercises

3. Find closed form expressions for the generating functions of the following sequences:

(a) $V(n) = 9^n$

(b) P, where $P(k) - 6\,P(k-1) + 5\,P(k-2) = 0$ for $k \geq 2$, with $P(0) = 2$ and $P(1) = 2$.

(c) The Fibonacci sequence: $F(k+2) = F(k+1) + F(k), k \geq 0$, with $F(0) = F(1) = 1$.

4. Find closed form expressions for the generating functions of the following sequences:

(a) $W(n) = C(5; n)\, 2^n$ for $0 \leq n \leq 5$ and $W(n) = 0$ for $n > 5$.

(b) Q, where $Q(k) + Q(k-1) - 42\,Q(k-2) = 0$ for $k \geq 2$, with $Q(0) = 2$ and $Q(1) = 2$.

(c) G, where $G(k+3) = G(k+2) + G(k+1) + G(k)$ for $k \geq 0$, with $G(0) = G(1) = G(2) = 1$.

5. For each of the following expressions, find the partial fraction decomposition and identify the sequence having the expression as a generating function.

(a) $\frac{5+2\,z}{1-4\,z^2}$

(b) $\frac{32-22\,z}{2-3\,z+z^2}$

(c) $\frac{6-29\,z}{1-11\,z+30\,z^2}$

6. Find the partial fraction decompositions and identify the sequence having the following expressions:

(a) $\frac{1}{1-9\,z^2}$

(b) $\frac{1+3\,z}{16-8\,z+z^2}$

(c) $\frac{2\,z}{1-6\,z-7\,z^2}$

7. Given that $S(k) = k$ and $T(k) = 10\,k$, what is the k^{th} term of the generating function of each of the following sequences:

(a) $S + T$

(b) $S\uparrow * T$

(c) $S * T$

(d) $S\uparrow * S\uparrow$

8. Given that $P(k) = C(10; k)$ and $Q(k) = k!$, what is the k^{th} term of the generating function of each of the following sequences:

(a) $P * P$

(b) $P + P\uparrow$

(c) $P * Q$

(d) $Q * Q$

C Exercises

9. A game is played by rolling a die five times. For the k^{th} roll, one point is added to your score if you roll a number higher than k. Otherwise, your score is zero for that roll. For example, the sequence of rolls 2, 3, 4, 1, 2 gives you a total score of three; while a sequence of 1,2,3,4,5 gives you a score of zero. Of the $6^5 = 7776$ possible sequences of rolls, how many give you a score of zero?, of one? … of five?

10. Suppose that you roll a die ten times in a row and record the square of each number that you roll. How many ways could the sum of the squares of your rolls equal 40? What is the most common outcome?

8.6 Recursion and Computer Algebra Systems

There is frequently debate as to if, how, and when computers should be introduced teaching a topic such as recurrence relations. We have chosen to append this information at the end of the chapter. If desired, instructors can intersperse the following subsections with the previous sections, cover this section a the end, or simply ignore this section. Motivated students are welcome to read it at any time, but should be warned that many instructors will still prefer that they do some of the calculations "by hand" within their courses.

Note: At the present time, this section only describes the topics in *Mathematica*. If any readers with a knowledge of *Sage* or any other computer algebra system would like to contribute to this section, contact us through the addresses that appear at http://faculty.uml.edu/klevasseur/ads2/.

Recursive Definitions (8.1 and 8.2)

Mathematica

Functions can be defined recursively in *Mathematica*. For example, the Fibonacci sequence, 1, 1, 2, 3, 5, 8, 13, . . . (each number is the sum of the previous two) can be defined with the following input.

```
fib[0] = 1;
fib[1] = 1;
fib[i_ /; i > 1] := fib[i - 2] + fib[i - 1]
```

The left side of the third line, **fib[i_/;i>1]** indicates that **fib** is being defined in this case for a "pattern" called **i** satisfying the condition that **i** is greater than 1. Any "input" that fits this pattern will have this rule applied to it. Notice that the definitions for **fib[0]** and **fib[1]** coexist with this general rule and define **fib** for two numbers that don't fit the pattern described in the general rule.

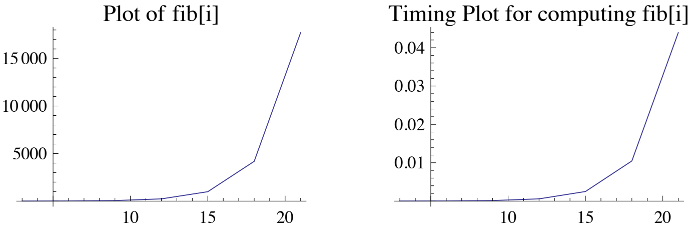
With the input above evaluated, we can determine the 12th Fibonacci number.

```
fib[12]
```

```
233
```

This particular definition is not efficient because previously computed values of **fib** are not saved. As a result, the time it takes to compute **fib[i]** is roughly proportional to the value of **fib[i]**, which grows exponentially. This can be demonstrated with the following bit of code.

```
 fp = ListPlot[({#1, fib[#1]} &) /@ Range[3, 21, 3],
    Joined → True, PlotLabel → "Plot of fib[i]"];
tfp = ListPlot[({#1, First[Timing[fib[#1]]]} &) /@ Range[3, 21, 3],
    Joined → True, PlotLabel → "Timing Plot for computing fib[i]"];
Show[GraphicsRow[{fp, tfp}, ImageSize → 1.5 {288, 84.75`}]]
```


Plot of fib[i]
Timing Plot for computing fib[i]

Taking over three seconds to compute the 30th Fibonacci number is unacceptable.

```
{Timing[fib[30]], $System}
```

```
{{3.32795, 1 346 269}, Mac OS X x86 (64−bit)}
```

The timing result above depends on the system you use, so you might want to execute this expression for comparison.

How to get around the timing problem. You could never get a value like **fib[100]** using the recursive definition because of the obvious time growth. To get around the problem, you can define a variation of the function that saves it's results.

The following definition allows for saving the results that are computed. Notice that the SetDelay (**:=**) involves a Set (**=**).

```
fib2[0] = 1;
fib2[1] = 1;
fib2[i_ /; i > 1] := fib2[i] = fib2[i - 2] + fib2[i - 1]
```

Now let's compute the 30th number in the sequence with this new definition

```
Timing[fib2[30]]
```

{0.000317, 1 346 269}

Now that the value of **fib[30]** has been computed, it's value is returned almost instantly

```
Timing[fib2[30]]
```

{0.000012, 1 346 269}

Now you can see what **fib2[100]** equals in a reasonable time.

```
Timing[fib2[100]]
```

{0.000499, 573 147 844 013 817 084 101}

There is still a problem with using recursion. If we were to ask for the 500th Fibonacci number at this point, *Mathematica* would have difficulty because it still had 400 levels of recursion to negotiate. For this reason, getting to the 500th Fibonacci number is best reached by evaluating every 50th or so of the numbers instead of directly asking for the 500th

```
Do[fib2[50 k], {k, 3, 10}];
fib2[500]
```

```
225 591 516 161 936 330 872 512 695 036 072 072 046 011 324 913 758 190 588 638 866 418 474 627 738 686 883 405 015 987 052 796 ⋱
  968 498 626
```

Solution of Recurrence Relations (8.3 and 8.4)

Mathematica

Mathematica has a function called **RSolve** that will solve some recurrence relations, including linear recurrence relations with constant coefficients. In addition, it can handle some systems of recurrence relations, which we will discuss in a Chapter 12.

```
? RSolve
```

RSolve[eqn, $a[n]$, n] solves a recurrence equation for $a[n]$.
RSolve[$\{eqn_1, eqn_2, \ldots\}$, $\{a_1[n], a_2[n], \ldots\}$, n] solves a system of recurrence equations.
RSolve[eqn, $a[n_1, n_2, \ldots]$, $\{n_1, n_2, \ldots\}$] solves a partial recurrence equation. ≫

Example. Consider the sequence S defined as follows.

$$S(k) = 1.3\, S(k-1) - 0.7 \text{ with } S(0) = 3$$

We can get the general solution to the recursive part of the definition, if desired.

```
recurence = S[k] == 1.3 S[k - 1] - 0.7;
RSolve[recurence, S[k], k]
```

$$\left\{\left\{S(k) \to 1.3^{k-1.} \left(2.33333 \times 2.71828^{0.262364-0.262364\,k} - 3.03333\right) + c_1\, 1.3^{k-1.}\right\}\right\}$$

Or we can add the initial condition to the first argument of **RSolve** and get a unique solution

```
solution = RSolve[{recurence, S[0] == 3}, S[k], k]
```

$$\left\{\left\{S(k) \to 0.769231 \times 2.71828^{-0.262364\,k} \left(3.03333 \times 1.3^{k} + 0.866667 \times 1.3^{k}\, 2.71828^{0.262364\,k}\right)\right\}\right\}$$

Notice that since approximate numbers 1.3 and 0.7 are involved in the definition of S, the solution involves approximate numbers. If we had used $\frac{13}{10}$ and $\frac{7}{10}$, respectively, the solution would be exact.

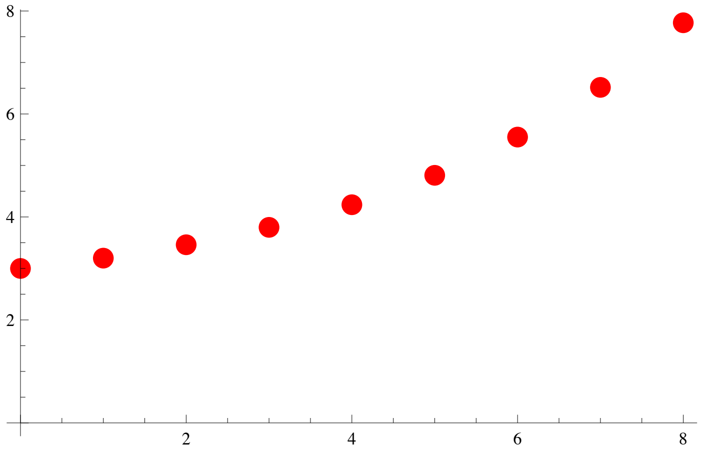
Next we assemble a list of ordered pairs based on the solution.

```
points = Table[{k, S[k]} /. First[solution], {k, 0, 8}]
```

$$\begin{pmatrix} 0 & 3. \\ 1 & 3.2 \\ 2 & 3.46 \\ 3 & 3.798 \\ 4 & 4.2374 \\ 5 & 4.80862 \\ 6 & 5.55121 \\ 7 & 6.51657 \\ 8 & 7.77154 \end{pmatrix}$$

Here is a plot of the first few terms of the solution.

```
ListPlot[points, PlotStyle → {Red, PointSize[0.03]}, AxesOrigin → {0, 0}]
```



Example. Here is the solution to a second order linear recurrence relations with constant coefficients. Initial conditions included. Notice that the exact data in the system produces exact expressions.

```
RSolve[{T[k] - 6 T[k - 1] + 3 T[k - 2] == 2^k, T[0] == 2, T[1] == 3}, T[k], k]
```

$$\left\{\left\{T(k) \to -\left(5 \times 3^{1-k}\left(-19\sqrt{2}\ 3^{k+\frac{1}{2}}\left(3-\sqrt{6}\right)^k - 28 \times 3^{k+1}\left(3-\sqrt{6}\right)^k + 19\sqrt{2}\ 3^{k+\frac{1}{2}}\left(3+\sqrt{6}\right)^k - 28 \times 3^{k+1}\left(3+\sqrt{6}\right)^k + 3 \times 2^{k+4}\left(\left(3-\sqrt{6}\right)\left(3+\sqrt{6}\right)\right)^k\right)\right) \Big/ \left(4\left(2\sqrt{6}-3\right)^2\left(3+2\sqrt{6}\right)^2\right)\right\}\right\}$$

Example. Here is the solution to a recurrence relation similar to the ones described in Section 8.4. The solution is in terms of the Gamma function, which is a generalization of the factorial function.

```
Usol = U[k] /. First[RSolve[{U[k] - k U[k - 1] == 2^-k, U[0] == 1}, U[k], k]]
```

$$\sqrt{e}\ \Gamma\left(k+1, \frac{1}{2}\right)$$

Here is a table of the first few terms of the solution.

```
Table[{j, N[Usol /. {k → j}]}, {j, 0, 10}]
```

$$\begin{pmatrix} 0 & 1. \\ 1 & 1.5 \\ 2 & 3.25 \\ 3 & 9.875 \\ 4 & 39.5625 \\ 5 & 197.844 \\ 6 & 1187.08 \\ 7 & 8309.55 \\ 8 & 66476.4 \\ 9 & 598288. \\ 10 & 5.98288\times 10^{6} \end{pmatrix}$$

Example. Here is the solution to the recurrence for the number of derangements of a set of n elements, $\mathcal{D}(n)$. We use $\mathcal{D}$ instead of D here because *Mathematica* reserves the name D for the derivative function.

```
derangementSol = RSolve[{𝒟[n] == (n - 1) (𝒟[n - 1] + 𝒟[n - 2]), 𝒟[1] == 0, 𝒟[2] == 1}, 𝒟[n], n]
```

$\{\{\mathcal{D}(n) \to (\Gamma(2, -1)\,\Gamma(n+1) - \Gamma(n+1, -1))/(2\,\Gamma(2, -1) - \Gamma(3, -1))\}\}$

```
Table[{n, 𝒟[n]} /. First[derangementSol] /. {n → k}, {k, 1, 10}] // Round
```

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \\ 3 & 2 \\ 4 & 9 \\ 5 & 44 \\ 6 & 265 \\ 7 & 1854 \\ 8 & 14833 \\ 9 & 133496 \\ 10 & 1334961 \end{pmatrix}$$

Generating Functions (8.5)

The examples in Section 8.5 solving recurrence relations with generating functions were selected to keep the algebra reasonably neat. Here we will step through the solution of a second order linear recurrence relation with constant coefficients for which the numbers are not so nice. Using *Mathematica*, the messy work isn't a problem.

Mathematica

Consider the recurrence relation $S(k) = -S(k-1) + 5\,S(k-2)$, with $S(0) = 4$ and $S(1) = 3$. In order to check our computations, lets define S recursively and get its first few terms:

```
S[0] = 4; S[1] = 3;
S[k_] := S[k] = -S[k - 1] + 5 S[k - 2]
```

```
Map[S, Range[0, 10]]
```

$\{4, 3, 17, -2, 87, -97, 532, -1017, 3677, -8762, 27147\}$

We can find the generating function for S by observing that $S = -S\uparrow + 5\,S\uparrow 2$. Using the formulas for the generating functions of $S\uparrow$ and $S\uparrow 2$ that were derived in Section 8.5, we get the following equation which we can solve for $G = G(S; z)$:

```
Clear[G]
```

$$\texttt{gfEquation} = \frac{(\texttt{G} - \texttt{S[0]} - \texttt{S[1] z})}{\texttt{z}^2} + \frac{(\texttt{G} - \texttt{S[0]})}{\texttt{z}} - 5\,\texttt{G} == 0$$

$$\frac{G - 3z - 4}{z^2} + \frac{G - 4}{z} - 5\,G = 0$$

We solve for G and since there is only one solution, we use **`First`** to extract that single solution from the output of **`Solve`**.

```
Gsol = G /. First[Solve[gfEquation, G]]
```

$$\frac{-7 z - 4}{5 z^2 - z - 1}$$

At this stage, we can extract a finite number of coefficients from the generating function. We do so here, but it only verifies the list of terms we computed above. We still don't have a closed form expression for *S*.

```
seriesExpansion = Series[Gsol, {z, 0, 10}]
```

$$4 + 3 z + 17 z^2 - 2 z^3 + 87 z^4 - 97 z^5 + 532 z^6 - 1017 z^7 + 3677 z^8 - 8762 z^9 + 27\,147 z^{10} + O\left(z^{11}\right)$$

```
CoefficientList[seriesExpansion, z]
```

$$\{4, 3, 17, -2, 87, -97, 532, -1017, 3677, -8762, 27\,147\}$$

In order to get a close form expression we need to get partial fractions decomposition of the generating function. The function **Apart** is meant to do this, but the next result isn't very encouraging

```
Apart[Gsol]
```

$$\frac{-7 z - 4}{5 z^2 - z - 1}$$

The difficulty is that **Apart** uses the **Factor** function that only factors polynomials over into factors with rational coefficients.

```
Factor[Gsol]
```

$$-\frac{7 z + 4}{5 z^2 - z - 1}$$

In order for factor to work on this denominator, we need to tell *Mathematica* what square root should be included. The discriminant of the denominator is

```
Discriminant[5 z^2 - z - 1, z]
```

$$21$$

Therefore we need to extend the rational numbers to include $\sqrt{21}$. We will discuss extensions in a more formal setting in Chapter 16.

```
Factor[Gsol, Extension → {√21}]
```

$$(20 (7 z + 4)) \Big/ \left(\left(-10 z + \sqrt{21} + 1\right) \left(10 z + \sqrt{21} - 1\right)\right)$$

With this factored expression, **Apart** will do its job.

```
PF = Apart[Factor[Gsol, Extension → {Sqrt[21]}]]
```

$$\frac{47 - 7 \sqrt{21}}{\sqrt{21} \left(10 z + \sqrt{21} - 1\right)} + \frac{47 + 7 \sqrt{21}}{\sqrt{21} \left(-10 z + \sqrt{21} + 1\right)}$$

We will work with the two terms above, both of which is the generating function of a geometric sequence, individually to get an expression that look like $b_1 {a_1}^k + b_2 {a_2}^k$. The problem is to find the b_i' *s*, which are initial terms of the generating functions and the a_i' *s* with are the ratios of successive coefficients of the generating functions.

```
GS1 = PF[[1]]
```

$$\frac{47 + 7 \sqrt{21}}{\sqrt{21} \left(-10 z + \sqrt{21} + 1\right)}$$

Why isn't the first term that appears in the output for **PF** the same as the first part that we called **GS1**? It has to do with output forms in *Mathematica* and let's not get into that right now. This all works out, believe me!

A quick word on the output from **Series**: If the series expansion up to degree *n* for a function $f(z)$ centered at 0 is $a_0 + a_1 z + \cdots + a_n z^n$, then the internal structure of the output from **Series** is a **SeriesData** expression. The variable and center of the series expansion are the first two arguments of this expression, and the third is the list of coefficients, which is what we will be extracting here.

```
InputForm[Series[ⅇ^(2 z), {z, 0, 4}]]
```

```
SeriesData[z, 0, {1, 2, 2, 4/3, 2/3}, 0, 5, 1]
```

The last three argument of the output indicate the powers of the variable to attach to the variable, 0 through 5 in steps of 1 in the example above. The first part of the third argument is the first term of the first geometric sequence.

```
b1 = Series[GS1, {z, 0, 5}][[3, 1]]
```

$$\frac{147+47\sqrt{21}}{21\left(1+\sqrt{21}\right)}$$

To extract the quotient of the second with the first arguments we use the pure function **(#[[3, 2]]/#[[3, 1]]) &**. This is the common ration of the first geometric sequence.

```
a1 = Series[GS1, {z, 0, 5}] // (#[[3, 2]] / #[[3, 1]]) &
```

$$\frac{10}{1+\sqrt{21}}$$

We repeat the same calculations for the second geometric sequence.

```
GS2 = PF[[2]]
```

$$\frac{47-7\sqrt{21}}{\sqrt{21}\left(10z+\sqrt{21}-1\right)}$$

```
b2 = Series[GS2, {z, 0, 5}][[3, 1]]
```

$$\frac{47\sqrt{21}-147}{21\left(\sqrt{21}-1\right)}$$

```
a2 = Series[GS2, {z, 0, 5}] // (#[[3, 2]] / #[[3, 1]]) &
```

$$-\frac{10}{\sqrt{21}-1}$$

We collect the four constants we've just computed into the sum of two geometric sequences.

```
Ssol[k_] := b1 a1^k + b2 a2^k
```

Next we test our expression to see if it matches the two other lists of terms if S that we've computed. The result may be disturbing, but the reason for the difference is that *Mathematica* hold off simplifying some expressions until requested. This is the case here.

```
Map[Ssol, Range[10]]
```

$$\Big\{\frac{10\left(147+47\sqrt{21}\right)}{21\left(1+\sqrt{21}\right)^2}-\frac{10\left(47\sqrt{21}-147\right)}{21\left(\sqrt{21}-1\right)^2},$$

$$\frac{100\left(47\sqrt{21}-147\right)}{21\left(\sqrt{21}-1\right)^3}+\frac{100\left(147+47\sqrt{21}\right)}{21\left(1+\sqrt{21}\right)^3},\ \frac{1000\left(147+47\sqrt{21}\right)}{21\left(1+\sqrt{21}\right)^4}-\frac{1000\left(47\sqrt{21}-147\right)}{21\left(\sqrt{21}-1\right)^4},$$

$$\frac{10\,000\left(47\sqrt{21}-147\right)}{21\left(\sqrt{21}-1\right)^5}+\frac{10\,000\left(147+47\sqrt{21}\right)}{21\left(1+\sqrt{21}\right)^5},\ \frac{100\,000\left(147+47\sqrt{21}\right)}{21\left(1+\sqrt{21}\right)^6}-\frac{100\,000\left(47\sqrt{21}-147\right)}{21\left(\sqrt{21}-1\right)^6},$$

$$\frac{1\,000\,000\left(47\sqrt{21}-147\right)}{21\left(\sqrt{21}-1\right)^7}+\left(1\,000\,000\left(147+47\sqrt{21}\right)\right)\Big/\left(21\left(1+\sqrt{21}\right)^7\right),$$

$$\frac{10\,000\,000\left(147+47\sqrt{21}\right)}{21\left(1+\sqrt{21}\right)^8}-\left(10\,000\,000\left(47\sqrt{21}-147\right)\right)\Big/\left(21\left(\sqrt{21}-1\right)^8\right),$$

$$\left(100\,000\,000\left(47\sqrt{21}-147\right)\right)\Big/\left(21\left(\sqrt{21}-1\right)^9\right)+\left(100\,000\,000\left(147+47\sqrt{21}\right)\right)\Big/\left(21\left(1+\sqrt{21}\right)^9\right),$$

$$\left(1\,000\,000\,000\left(147+47\sqrt{21}\right)\right)\Big/\left(21\left(1+\sqrt{21}\right)^{10}\right)-\left(1\,000\,000\,000\left(47\sqrt{21}-147\right)\right)\Big/\left(21\left(\sqrt{21}-1\right)^{10}\right),$$

$$\left(10\,000\,000\,000\left(47\sqrt{21}-147\right)\right)\Big/\left(21\left(\sqrt{21}-1\right)^{11}\right)+\left(10\,000\,000\,000\left(147+47\sqrt{21}\right)\right)\Big/\left(21\left(1+\sqrt{21}\right)^{11}\right)\Big\}$$

The simplified result should look familiar.

```
Map[Ssol, Range[0, 10]] // Simplify
```

{4, 3, 17, –2, 87, –97, 532, –1017, 3677, –8762, 27 147}

Finally, the closed form expression for our sequence can be examined.

```
Ssol[k]
```

$$\frac{1}{21}\left(47\sqrt{21}-147\right)(-10)^k\left(\sqrt{21}-1\right)^{-k-1}+\frac{1}{21}\left(147+47\sqrt{21}\right)10^k\left(1+\sqrt{21}\right)^{-k-1}$$

Exercises for Section 8.6

A Exercises

1. If $B(0)=1000$, and $B(n)=1.05^{1/n}\,B(n-1)\ +\ 1000$ for $n \geq 1$, compute $B(20)$ and plot the values of B for $0 \leq n \leq 20$.

2. Compute the a closed form expression for $F(n)$, where $F(0)=1$, $F(1)=2$, $F(2)=2.5$, and if $k \geq 3$,

   $$F(k)=0.9\,F(k-1)+0.52\,F(k-2)-0.42\,F(k-3).$$

   As k gets large, what does $F(k)$ tend toward?

3. Use generating functions to find a closed form expression for

   $W(0)=1,\ \ W(1)=1$
   $W(n)=3\,W(n-1)+W(n-2)$ when $n \geq 2$

SUPPLEMENTARY EXERCISES FOR CHAPTER 8

Section 8.1

1. Write out a recurrence relation to describe the number of n digit positive integers (in decimal form) that contain no repeating digits.

2. The number of k subset partitions of an n-element set, $S(n, k)$, satisfies the recurrence relation $S(n, k) = k\, S(n-1, k) + S(n-1, k-1)$ for $n \geq 3$ and $2 \leq k < n$. The numbers $S(n, k)$ are called *Stirling Numbers of the Second Kind*.

(a) What are $S(n, 1)$ and $S(n, n)$ for $n \geq 1$?
(b) Compute $S(5, 2)$, $S(5, 3)$, and $S(5, 4)$.
(c) How many partitions are there of a five-element set?
(d) What is the significance of $\sum_{k=1}^{n} S(n, k)$?

3. Consider the following algorithm, called *Split:*

```
Input: a list, Lin = $(a_1, a_2, \ldots, a_n)$ of $n$ numbers, where $n$ is a natural number

Output: a list, Lout $= (b_1, b_2 \ldots, b_n)$ of $n$ numbers If $n < 2$, then Lout := Lin

    else $\{n \geq 2\}$

    1. Let $L1 := (a_1, a_3, a_5 \ldots)$ and $L2 := (a_2, a_4, a_6, \ldots)$
    2. Execute Split with input $L1$ and output $L1$ out
    3. Execute Split with input L2 and output $L2$ out
    4. Lout := ($L1$ out, $L2$ out), that is, the list obtained by copying $L1$ out and then copying $L2$ out
```

(a) What is the output from Split if the input is (1, 2, 3, 4)?

(b) What is the output from Split if the input is $(0, 1, 2, \ldots, n-1)$, where n is equal to $2 r$ for some natural number r? Hint: the general answer is related to the binary representations of the numbers in the list.

Section 8.2

4. Prove by induction that $S(k) = (2 + k)\, 10^k$ is a solution of the recurrence relation $S(k) = 20\, S(k-1) - 100\, S(k-2)$; $S(0) = 2$, $S(1) = 30$.

5. Explain why $B(n) = 1 + 2 + \cdots + 2^n$ is not a closed form expression.

6. Between them, Abe and Zeke have n coins. They each flip one coin and if they match (both heads or both tails), then Abe keeps both coins. Otherwise, Zeke keeps both coins. They continue as long as both have at least a coin. Let L (n,k) be the expected number of flips that take place in the game if Abe starts with k coins. If $0 < k < n$, then

$$L(n, k) = 1 + (L(n, k-1) + L(n, k+1))/2$$

(a) Justify this equation.
(b) What are $L(n, 0)$ and $L(n, n)$?
(c) Tabulate $L(n, k)$ for $n = 2$, 3, and 4.

Section 8.3

7. On her nth birthday, Kathryn receives n dollars from her Uncle Dave and deposits it into a special account that pays interest of 10 % each year. On her 21st birthday, how much does she have in the account?

8. Suppose you borrowed \$4,000 at 8% interest and you made payments of \$250 per month. Let $D(n)$ be your debt n months after taking out the loan. Then $D(0) = 4000$ and $D(n) = 1.08\, D(n-1) - 250$ for $n > 0$.

(a) Derive a closed form expression for $D(n)$.
(b) Estimate how long it would take you to pay off the loan. Use logs if necessary. A rough estimate is sufficient.

9. (Tower of Hanoi Problem): A classic problem that can be solved using material of this section is the Tower of Hanoi puzzle. Assume that we have a board with three pegs mounted on it and on one of the pegs n circular disks of decreasing size (smallest on top). The problem is to determine how many moves it takes to move the n disks from one peg to another without placing a larger disk on a smaller one at any time.

(a) If $X(n)$ stands for the number of moves it takes to move n disks from one peg to another, then $X(n) = 2\, X(n-1) + 1$. Justify this recurrence relation.

(b) Solve the recurrence relation in part a. Verify your result, and the formula in part a, using three disks.

Section 8.4

10. Suppose that $T(0) = 0$ and $T(a) = 1 + T(\lfloor a/2 \rfloor)$ for $a > 0$. If $a = (1\,101\,001\,011\,011\,110)_{\text{two}}$, what is $T(a)$?

11. Find a solution for $n = 2^k$: $Q(n) = n + Q(\lfloor n = 4 \rfloor), n \geq 1, Q(0) = 0$.

12. The recurrence relation $x(n+1) = 1 + x(n)^2$ with $x(0) = 1$ has a solution that is approximately equal to $c^{t(n)}$, where c is a constant and $t(n) = 2^n$, Estimate the value of c based on values of $x(0)$, $x(1)$, … , $x(4)$. Test your answer by computing $x(5)$ and comparing it to $c^{t(5)}$. The significance of $x(n)$ is that it equals the number of binary trees of depth n or less (see Chapter 10).

Section 8.5

13. Write out the first five terms of the generating function of sequence S where $S(0) = 1$ and for $k > 0$, $S(k) = S(0) + \cdots + S(k-1)$.

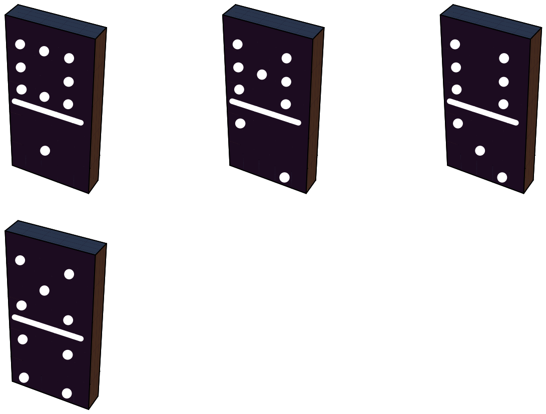
14. (a) Determine the closed form expression for the terms of sequence S,

where $S(k) - 6\,S(k-1) = 0$ for $k \geq 1$ and $S(0) = 7$.

(b) What is the generating function, $G(S; z)$, for sequence S? Write out the first four terms of your answer and then write out the closed form expression for the generating function.

15. Suppose that S is a sequence with generating function $G(S; z)$ and that T has generating function $G(S; cz)$. How is T related to S?

chapter 9



GRAPH THEORY

Bipartite

Draw some lines joining dots in set A
To some dots in set B. Then we say
It' s bipartite if we
Have no "B" joined to "B"
And no "A" joined to "A". That okay?

- a limerick by Chris Howlett from the *The Omnificent English Dictionary In Limerick Form*

GOALS

This chapter has three principal goals. First, we will identify the basic components of a graph and some of the optional features that many graphs have. Second, we will discuss some of the questions that are most commonly asked of graphs. Third, we want to make the reader aware of how graphs are used to model different situations. In Section 9.1, we will discuss these topics in general, and in later sections we will take a closer look at selected topics in the theory of graphs.

Chapter 10 will continue our discussion with an examination of trees, a special type of graph.

9.1 Graphs—A General Introduction

Recall that we introduced directed graphs in Chapter 6.

Definition: Directed Graph. *A directed graph consists of a set of vertices, V, and a set of edges, E, connecting certain elements of V. Each element of E is an ordered pair from V (i.e., an element of $V \times V$). The first entry is the initial vertex of the edge and the second entry is the terminal vertex. In certain cases there will be more than one edge between two vertices, in which cases the different edges are identified with labels.*

Despite the set terminology in this definition, we usually think of a graph as a picture, an aid in visualizing a situation. In Chapter 6, we introduced this concept to help understand relations on sets. Although those relations were principally of a mathematical nature, it remains true that when we see a graph, it tells us how the elements of a set are related to one another.

Definition: Simple Graph and Multigraph. *A simple graph is one for which there is no more than one vertex directed from any vertex to another vertex. All other graphs, ones with at least two edges from one vertex to some other vertex, are called multigraphs.*

To illustrate the points that we will make in this chapter, we will introduce the following examples of graphs.

Example 9.1.1. A Directed Graph. Figure 9.1.1 is an example of a simple directed graph. In set terms, this graph is (V, E), where $V = \{s, a, b\}$ and $E = \{(s, a), (s, b), (a, b), (b, a), (b, b)\}$. Note how each edge is labeled either 0 or 1. There are often reasons for labeling even simple graphs. Some labels are to help make a graph easier to discuss; others are more significant. We will discuss the significance of the labels on this graph later.

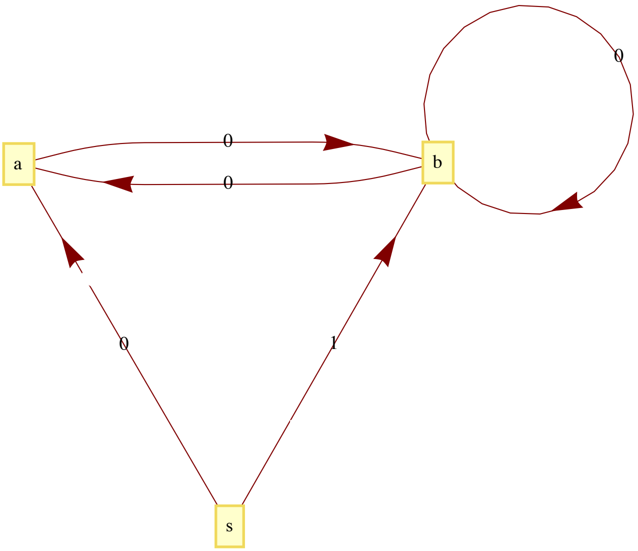


Figure 9.1.1
A directed graph

Example 9.1.2. An Undirected Graph. A network of computers can be described easily using a graph. Figure 9.1.2 describes a network of five computers, a, b, c, d, and e. An edge between any two vertices indicates that direct two-way communication is possible between the two computers. Note that the edges of this graph are not directed. This is due to the fact that the relation that is being displayed is symmetric (i.e., if X can communicate with Y, then Y can communicate with X). Although directed edges could be used here, it would simply clutter the graph.

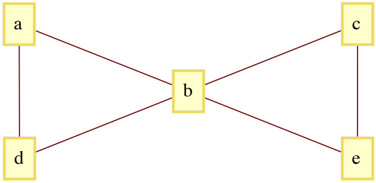


Figure 9.1.2
An undirected graph

There are several other situations for which this graph can serve as a model. One of them is to interpret the vertices as cities and the edges as roads, an abstraction of a map such as the one in Figure 9.1.3. Another interpretation is as an abstraction of the floor plan of a house (Figure 9.1.4). Vertex a represents the outside of the house; all others represent rooms. Two vertices are connected if there is a door between them.

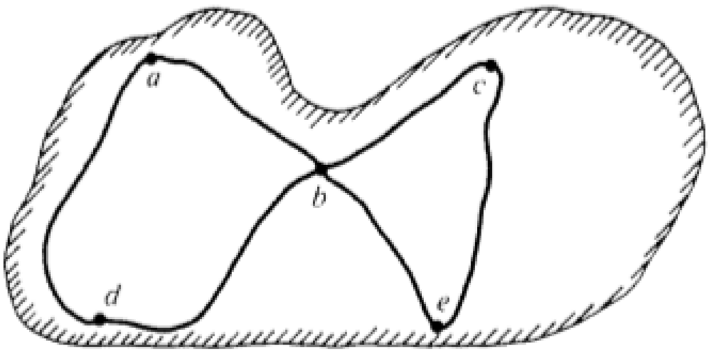


Figure 9.1.3
Road Map

Definition: Undirected Graph. *An undirected graph consists of a set V, called a vertex set, and a set E of two-element subsets of V, called the edge set. The two-element subsets are drawn as lines connecting the vertices.*

The undirected graph of Figure 9.1.2 is $V = \{a, b, c, d, e\}$ and $E = \{\{a, b,\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, e\}, \{b, e\}\}$.

Definition: Complete Undirected Graph. *A complete undirected graph of n vertices is an undirected graph with the property that each pair of distinct vertices are connected to one another. Such a graph is usually denoted by K_n.*

Example 9.1.3. A Multigraph. A common occurrence of a multigraph is a road map. The cities and towns on the map can be thought of as vertices, while the roads are the edges. It is not uncommon to have more than one road connecting two cities. In order to give clear travel directions, we name or number roads so that there is no ambiguity. We use the same method to describe the edges of the multigraph in Figure 9.1.5. There is no question what e3 is; however, referring to the edge $(2, 3)$ would be ambiguous.

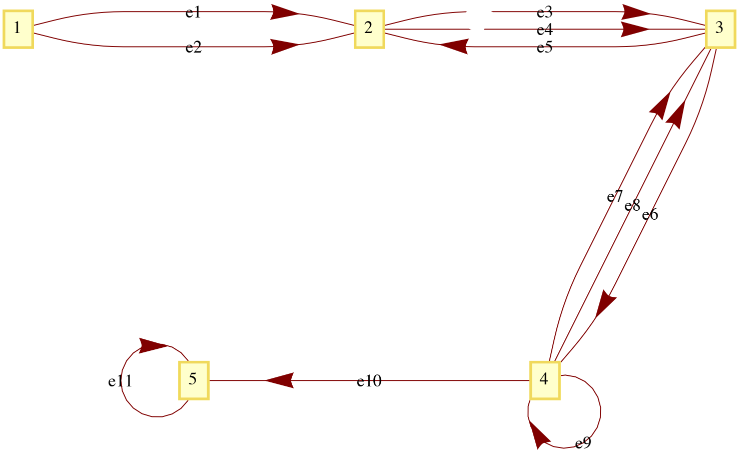


Figure 9.1.5
A multigraph

Example 9.1.4. A flowchart is a common example of a simple graph that requires labels for its vertices and some of its edges. Figure 9.1.6 is one such example that illustrates how many problems are solved.

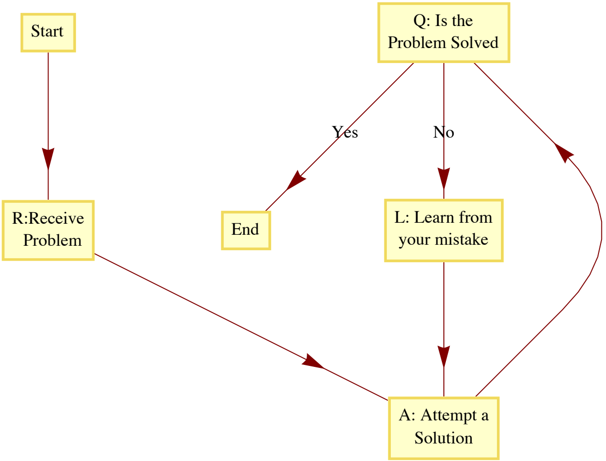


Figure 9.1.5
Flowchart for the problem-solving process

At the start of the problem-solving process, we are at the vertex labeled "Start" and at the end (if we are lucky enough to have solved the problem) we will be at the vertex labeled "End." The sequence of vertices that we pass through as we move from "Start" to "End" is called a path. The "Start" vertex is called the initial vertex of the path, while the "End" is called the final, or terminal, vertex. Suppose that the problem is solved after two attempts; then the path that was taken is Start, R, A, Q, L, A, Q, End. An alternate path description would be to list the edges that were used: 1, 2, 3, No, 4, 3, Yes. This second method of describing a path has the advantage of being applicable for multigraphs. On the graph in Figure 9.1.5, the vertex list 1, 2, 3, 4, 3 does not clearly describe a path between 1 and 3, but e_1, e_4, e_6, e_7 is unambiguous.

A SUMMARY OF PATH NOTATION AND TERMINOLOGY

If x and y are two vertices of a graph, then a path between x and y describes a motion from x and y along edges of the graph. Vertex x is called the initial vertex of the path and y is called the terminal vertex. A path between x and y can always be described by its *edge list*, the list of edges that were used: $(e_1, e_2, \ldots, e_n)$, where : (1) the initial vertex of e_1 is x; (2) the terminal vertex of e_i is the initial vertex of e_{i+1} , $i = 1, 2, \ldots, n - 1$; and (3) the terminal vertex of e_n is y. The number of edges in the edge list is the *path length*. A path on a simple graph can also be described by a *vertex list*. A path of length n will have a list of $n + 1$ vertices $v_0 = x$, v_1, $v_2, \ldots, v_n = y$, where, for $k = 0, 1, 2, \ldots, n-1$, (v_k, v_{k+1}) is an edge on the graph. A *circuit* is a path that terminates at its initial vertex.

Suppose that a path between two vertices has an edge list (e,, e 2 , . . . ,e,,). A *subpath* of this graph is any portion of the path described by one or more consecutive edges in the edge list. For example, (3, No, 4) is a subpath of (1, 2, 3, No, 4, 3, Yes). Any path is its own subpath; however, we call it an improper subpath of itself. All other subpaths are called proper subpaths.

A path or circuit is *simple* if it contains no proper subpath that is a circuit. This is the same as saying that a path or circuit is simple if it does not visit any vertex more than once except for the common initial and terminal vertex in the circuit. In the problem-solving method described in Figure 9.1.6, the path that you take is simple only if you reach a solution on the first try.

Example 9.1.5. The leadership structure of a corporation is often represented with a graph as in Figure 9.1.7.

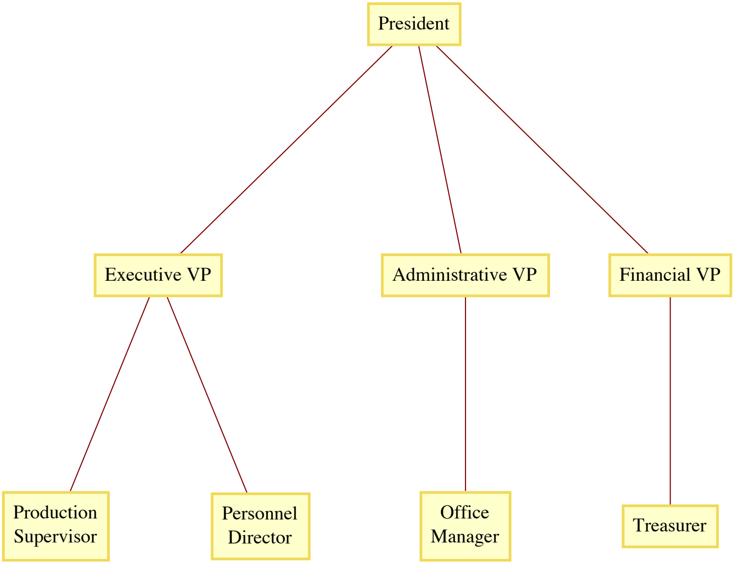


Figure 9.1.7
Organization of a corporation

The principle behind such a structure is that everyone but the president has a single immediate supervisor. Any action that anyone takes can reach the president only through a unique "chain of command." This chain-of-command property is characteristic of a special type of graph called a *tree*. Note that the edges of this graph are not directed, but, as in a Hasse diagram, the relation between two connecting vertices is clear: the top vertex is the supervisor of the lower vertex.

The process of structured (or top-down) problem solving results in a graph that is similar to this tree. Starting with the top of the tree, which would represent the whole problem, the problem is divided into a sequence of separate subproblems. Each subproblem is divided further into smaller sub-problems in the same way until the solutions of the lowest problems are easy enough to recognize.

From these examples, we can see that although a graph can be defined, in short, as a collection of vertices and edges, an integral part of most graphs is the labeling of the vertices and edges that allows us to interpret the graph as a model for some situation.

Example 9.1.6. A Graph as a Model for a Set of Strings. Suppose that you would like to mechanically describe the set of strings of 0's and 1's having no consecutive 1's. One way to visualize a string of this kind is with the graph in Figure 9.1.1. Consider any path starting at vertex s. If the label on each graph is considered to be the output to a printer, then the output will have no consecutive 1's. For example, the path that is described by the vertex list $(s, a, b, b, a, b, b, a, b)$ would result in an output of 10010010. Conversely, any string with no consecutive 1's determines a path starting at s.

Example 9.1.7. A Tournament Graph. Suppose that four teams compete in a round-robin sporting event; that is, each team meets every other team once, and each game is played until a winner is determined. If the teams are named A, B, C, and D, we can define the relation β on the set of teams by $X \beta Y$ if X beat Y. For one set of results, the graph of β might look like Figure 9.1.8.

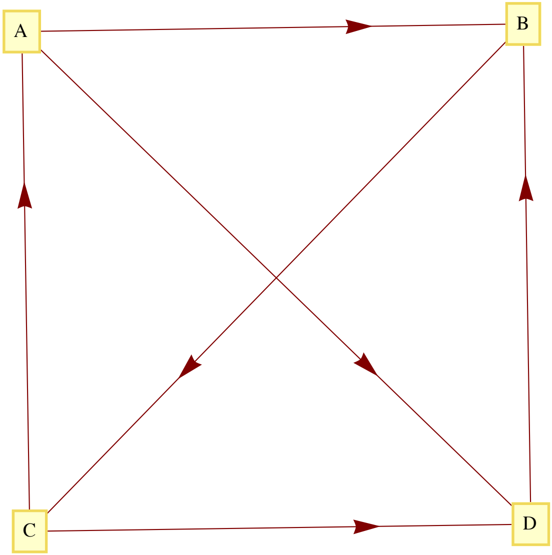


Figure 9.1.8
Round-robin graph with four vertices

Definition: ***Tournament Graph.***

(a) A tournament graph is a directed graph with the property that no edge connects a vertex to itself, and between any two vertices there is at most one edge.

(b) A complete (or round-robin) tournament graph is a tournament graph with the property that between any two distinct vertices there is exactly one edge.

(c) A single-elimination tournament graph is a tournament graph with the properties that: (i) one vertex (the champion) has no edge terminating at it and at least one edge initiating from it; (ii) every other vertex is the terminal vertex of exactly one edge; and (iii) there is a path from the champion vertex to every other vertex.

Example 9.1.8. The major league baseball championship is decided with a single-elimination tournament, where each "game" is actually a series of games. Until 1995, the two divisional champions in the American League (East and West) compete in a series of games. The loser is eliminated and the winner competes against the winner of the National League series (which is decided as in the American League). The tournament graph of the 1983 championship is in Figure 9.1.9.

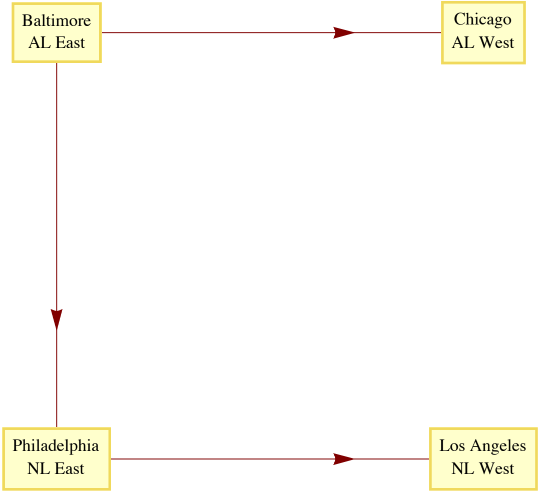


Figure 9.1.9
1983 Major League Baseball Championship

The question "Once you have a graph, what do you do with it?" might come to mind. The following list of common questions and comments about graphs is a partial list that will give you an overview of the remainder of the chapter.

Question 1. How can a graph be represented as a data structure for use on a computer? We will discuss some common Pascal data structures that are used to represent graphs in Section 9.2.

Question 2. Given two vertices in a graph, does there exist a path between them? The existence of a path between any or all pairs of vertices in a graph will be discussed in Section 9.3. A related question is: How many paths of a certain type or length are there between two vertices?

Question 3. Is there a path (or circuit) that passes through every vertex (or uses every edge) exactly once? Paths of this kind are called traversals. We will discuss traversals in Section 9.4.

Question 4, Suppose that a cost is associated with the use of each vertex and/or edge in a path. What is the "cheapest" path, circuit, or traversal of a given kind? Problems of this kind will be discussed in Section 9.5.

Question 5. Given the specifications of a graph, or the graph itself, what is the best way to draw the graph? The desire for neatness makes this a reasonable question. Another goal might be to avoid having edges of the graph cross one another. This is discussed in Section 9.6.

ISOMORPHIC GRAPHS

We will close this section by establishing the relation "is isomorphic to," a form of equality on graphs. The graphs in Figure 9.1.10 obviously share some similarities, such as the number of vertices and the number of edges. It happens that they are even more similar than just that. If the letters a, b, c, and d in a are replaced with the numbers 1,3,4, and 2, respectively, and they are moved around so that they appear as in b, you obtain b.

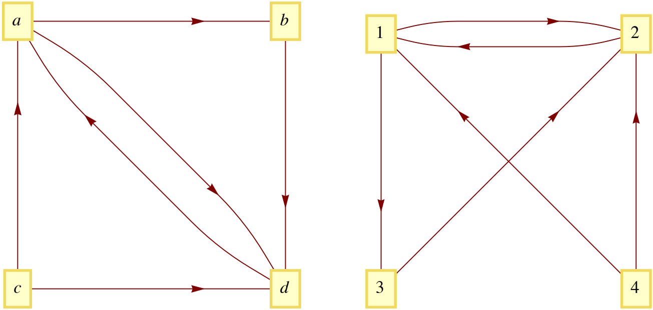


Figure 9.1.10
Two Isomorphic Graphs

Here is a more precise definition that reflects the fact that the actual positioning of vertices isn't an essential part of a graph.

Definition: Isomorphic Graphs. *Two graphs (V, E) and (V', E') are isomorphic if there exists a bijection $f : V \to V'$ such that $(v_i, v_j) \in E$ if and only if $(f(v_i), f(v_j)) \in E'$. For multigraphs, we add that the number of edges connecting v_i to v_j, must equal the number of edges from $f(v_i)$ to $f(v_j)$.*

Degrees and Graphic Sequences

The most significant local characteristic of a vertix within a graph is its degree. Collectively, the degrees can partially characterize a graph.

Definition: Degree.

(a) Let v be a vertex of an undirected graph. The degree of v, denoted deg*(v), is the number of edges that connect v to the other vertices in the graph.*

(b) If v is a vertex of a directed graph, then the outdegree of v, denoted outdeg*(v), is the number of edges of the graph that initiate at v. The indegree of v, denoted* indeg*(v). is the number of edges that terminate at v.*

Example 9.4.9.

(a) The degrees of vertices 1 through 5 in Figure 9.1.11 are 2, 3, 4, 1, and 2, respectively.

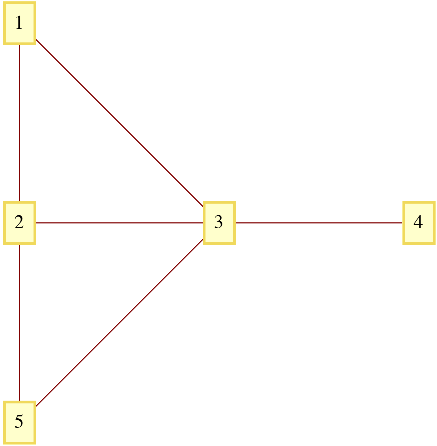
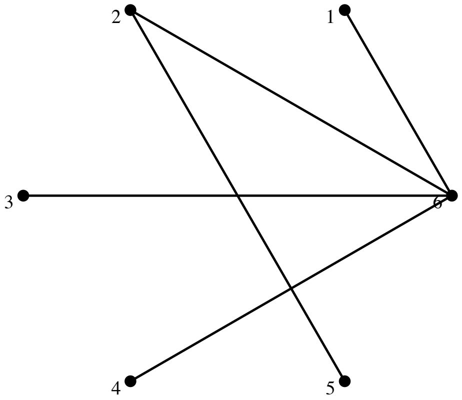


Figure 9.1.11

(b) In a tournament graph, outdeg (v) is the number of wins for v and indeg (v) is the number of losses. In a complete (round-robin) tournament graph with n vertices, outdeg (v) + indeg (v) = $n - 1$ for each vertex.

Graphic Sequences

A finite nonincreasing sequence of integers $d_1, d_2, \ldots, d_n$ is a *graphic* if there exists a simple graph with n vertices having the sequence as its degree sequence. For example, 4, 2, 1, 1, 1, 1 is graphic because the degrees of the following graph match these numbers.



Note: There is no connection between the vertex name/number and its degree.

EXERCISES FOR SECTION 9.1

A Exercises

1. What is the significance of the fact that there is a path connecting vertex b with every other vertex in Figure 9.1.2, as it applies to various situations that it models?

2. Draw a graph similar to Figure 9.1.1 that represents the set of strings of 0's and 1's containing no more than two consecutive 1's.

3. Draw a directed graph that models the set of strings of 0's and 1's where all of the 1's must appear consecutively.

4. In the NCAA final-four basketball tournament, the East champion plays the West champion, and the champions from the Mideast and Midwest play. The winners of the two games play for the national championship. Draw the eight different single-elimination tournament graphs that could occur.

5. What is the maximum number of edges in a simple undirected graph with eight vertices?

6. Which of the graphs in Figure 9.1.11 are isomorphic? What is the correspondence between their vertices?

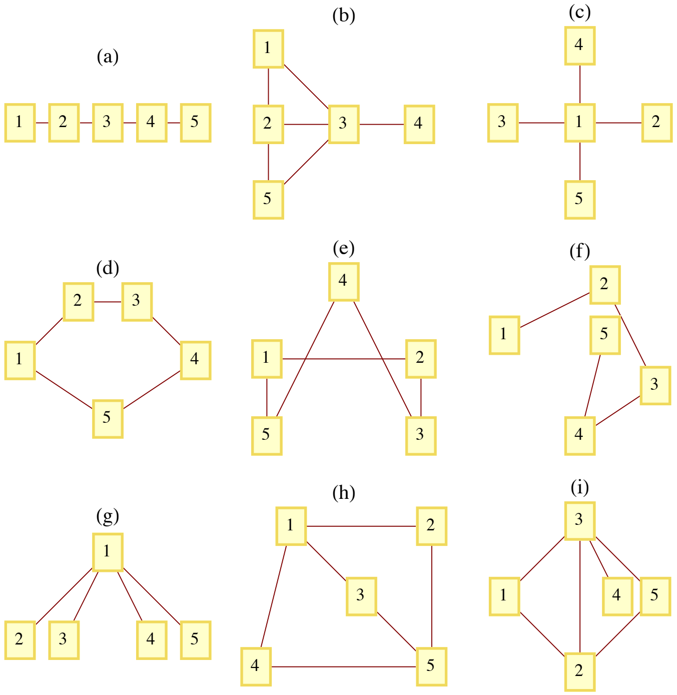


Figure 9.2.11

7. (a) How many edges does a complete tournament graph with n vertices have?

(b) How many edges does a single-elimination tournament graph with n vertices have?

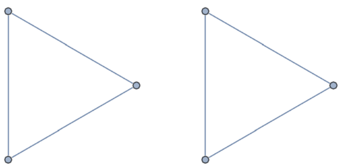
8. Draw complete undirected graphs with 1, 2, 3, 4, and 5 vertices. How many edges does a K_n, a complete undirected graph with n vertices, have?

9. Determine whether the following sequences are graphic. Explain your logic.

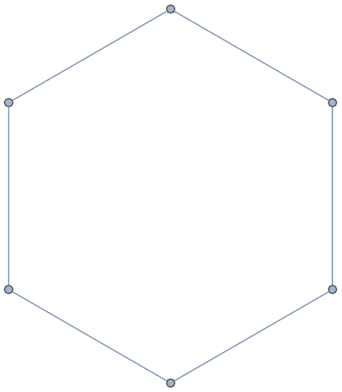
(a) 6, 5, 4, 3, 2, 1, 0
(b) 2, 2, 2, 2, 2, 2, 2
(c) 3, 2, 2, 2, 2, 2
(c) 5, 3, 3, 3, 3, 3
(e) 1, 1, 1, 1, 1, 1
(f) 5, 5, 4, 3, 2, 1

10. (a) Based on observations you might have made in exercise 9, describe as many characteristics as you can about graphic sequences of length n.

(b) Consider the two graphs



and



Notice that they have the same degree sequences, 2, 2, 2, 2, 2, 2. Explain why the two graphs are not isomorphic.

9.2 Data Structures and Computer Generation of Graphs

In this section, we will describe data structures that are commonly used to represent graphs. In addition we will introduce the basic syntax for graphs in *Mathematica* and Sage.

Assume that we have a graph with n vertices that can be indexed by the integers $1, 2, \ldots, n$.

Data Structure 1: Adjacency Matrix. As we saw in Chapter 6, the Information about edges in a graph can be summarized with an adjacency matrix, G, where $G_{ij} = 1$ if and only if vertex i is connected to vertex j in the graph. Note that this is the same as the adjacency matrix for a relation, with the exception.

Data Structure 2: Edge List I. Note that the initializing procedure for an adjacency matrix presumes that a list of edges for the graph exists. This second data structure maintains this list form. For each vertex in our graph, there will be a list of edges that initiate at that vertex. If G represents the graph's edge information, then G_i would be the list of edges initiating at vertex i.

Data Structure 3: Edge List II. An even simpler way to represent the edges is to maintain a list of ordered pairs.

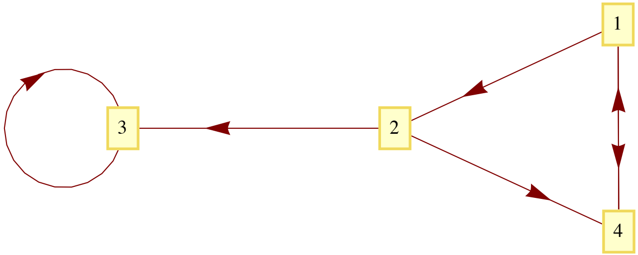


Figure 9.2.1

Example 9.2.1. Given the graph in Figure 9.2.1, the adjacency matrix that represents the graph would be

$$G_1 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

The same graph would be represented with the edge list of type 1:

$$G_1 = \{\{2, 4\}, \{3, 4\}, \{3\}, \{1\}\}$$

Finally, the list

$$G_1 = \{\{1, 2\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 3\}, \{4, 1\}\}$$

describes the same graph with an edge list of type 2.

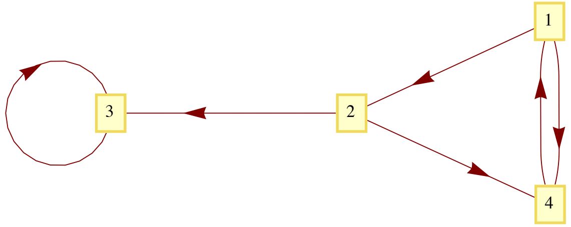
A natural question to ask is: Which data structure should be used in a given situation? For small graphs, it really doesn't make much difference, but since answers the question "Is there an edge from vertex i to vertex j is easiest with an adjacency matrix, the adjacency matrix would be the natural choice. For larger matrices the edge count would be a consideration. If n is large and the number of edges is relatively small, it might use less memory to maintain a list of edges instead of building an $n \times n$ matrix. Most software for working with graphs will make the decision for you.

Mathematica Note

First, a short history of graphs in *Mathematica*. Until *Mathematica* 6.0, all graph related functions were part of a package called *Combinatorica*. A few graph related functions, notably **`GraphPlot`**, were introduced in version 6.0. The output from GraphPlot was (and still is) a Graphics object. Starting in *Mathematica* 8.0, graphs became native *Mathematica* objects. Graph expressions are backwards compatible in that *Combinatorica* is still available. In addition, **`GraphPlot`** is still a good way to fine-tune the way a graph appears.

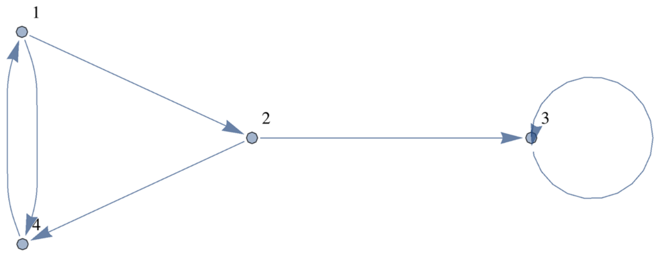
The graph in Example 9.2.1 was drawn by evaluating the following expression.

```
G1 = GraphPlot[{1 → 2, 2 → 3, 2 → 4, 4 → 1, 1 → 4, 3 → 3},
  VertexLabeling → True, DirectedEdges → True]
```



The same graph, with a different embedding and style of displaying vertices can be produced using **Graph**.

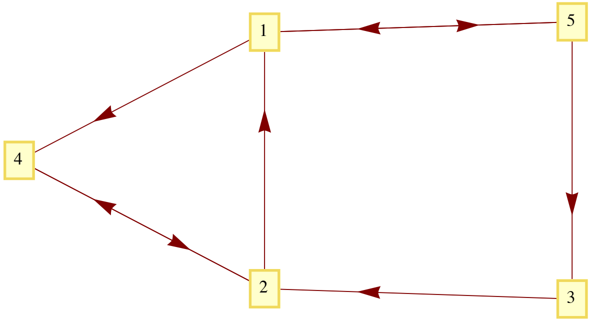
```
G1 = Graph[{1, 2, 3, 4}, {1 → 2, 2 → 3, 2 → 4, 4 → 1, 1 → 4, 3 → 3},
  VertexLabels → "Name", ImagePadding → 5]
```



From both expressions one sees that an edge list in the form of *Mathematica* rules is used to specify the edges. Using **GraphPlot**, the vertices are implicit from the numbers that appear among the edges. This has the drawback of not allowing for an isolated vertex without any edges connected to it. A second acceptable way to specify edges is using **GraphPlot** is with an adjacency matrix:

$$G_2 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix};$$

```
GraphPlot[G2, VertexLabeling → True, DirectedEdges → True]
```



Notice that in these examples, the placement of the vertices is determined by *Mathematica*. Both functions have options that do allow for placement.

An example of a system graph function is **GraphDistance**. For example, we can ask for the distance from vertex 1 to vertex 3 in G_1 and find that one needs to travel along two edges to go from 1 to 3.

```
GraphDistance[G1, 1, 3]
```

```
2
```

In G_1, you can't get from vertex 3 to vertex 4, so the distance is infinite:

```
GraphDistance[G1, 3, 4]
```

```
∞
```

We can get the adjacency matrix of G_1 or the edge list of G_2 with package function

```
AdjacencyMatrix[G1]
```

```
SparseArray[<6>, {4, 4}]
```

In practice, graphs are often quite large, so *Mathematica* automatically uses a sparse array data structure to store the adjacency matrix. To see the actual matrix you can use the `Normal` function:

```
Normal[AdjacencyMatrix[G1]]
```

$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

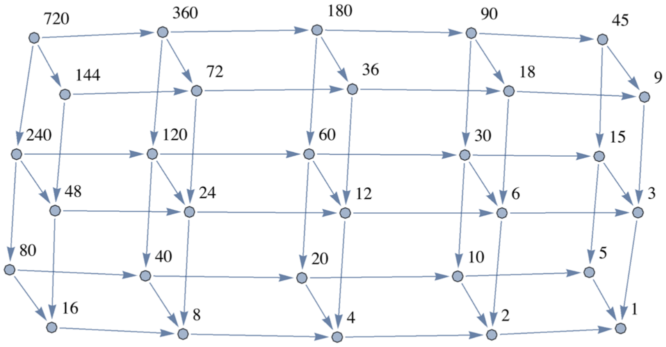
Larger graphs can be generated by creating lists of edges using rules. For example, here is graph of all divisors of $6\,! = 720$ with an edge connecting j to k if $\frac{j}{k}$ is a prime. For example, there is an edge connecting 72 to 24 because $\frac{72}{24} = 3$ is prime. The code for creating $\boldsymbol{G_3}$ may look daunting, but essentially the set of ordered pairs in the set

$$\text{Divisors}[6\,!] = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 30, 36, 40, 45, 48, 60, 72, 80, 90, 120, 144, 180, 240, 360, 720\}$$

and the relatively few ordered pairs where the first number divided by the second number is prime are selected out. These ordered pairs are then converted to a rule: $\{a, b\}$ is converted to $a \to b$.

```
edges = Map[Rule @@ # &, Select[Tuples[Divisors[6 !], 2], PrimeQ[Divide @@ #] &]];

G3 = Graph[edges, VertexLabels → "Name", ImagePadding → 5]
```



The adjacency matrix of G_3 can certainly be considered sparse since it has relatively few 1's.

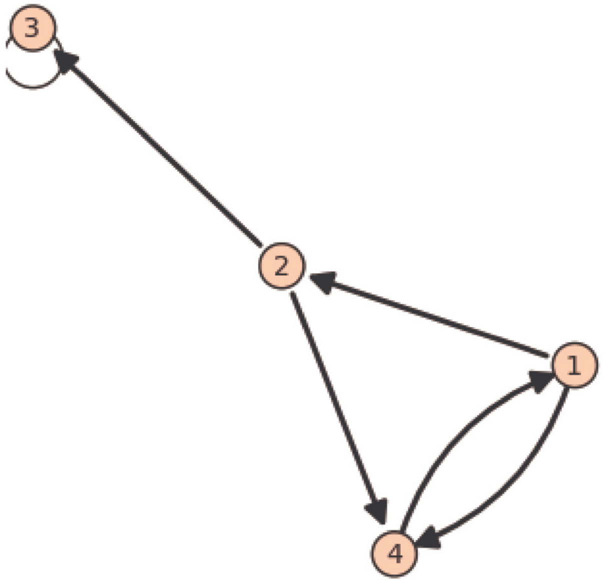
AdjacencyMatrix[G$_3$] // Normal

$$\begin{pmatrix}
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&0
\end{pmatrix}$$

Sage Note

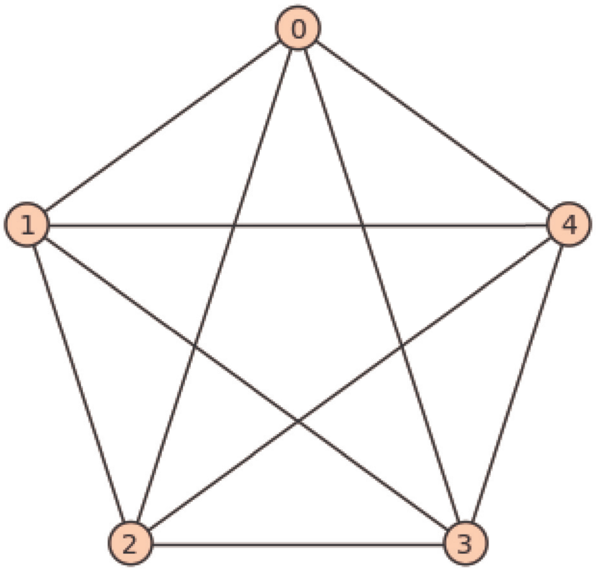
Sage graphs are specified using version 1 of edge lists. Here is how the graph in Example 9.2.1 is generated and then displayed.

```
sage:  G1 = DiGraph( { 1 : [4, 2], 2 : [3, 4], 3 : [3], 4 : [1]})
G1.show()
```



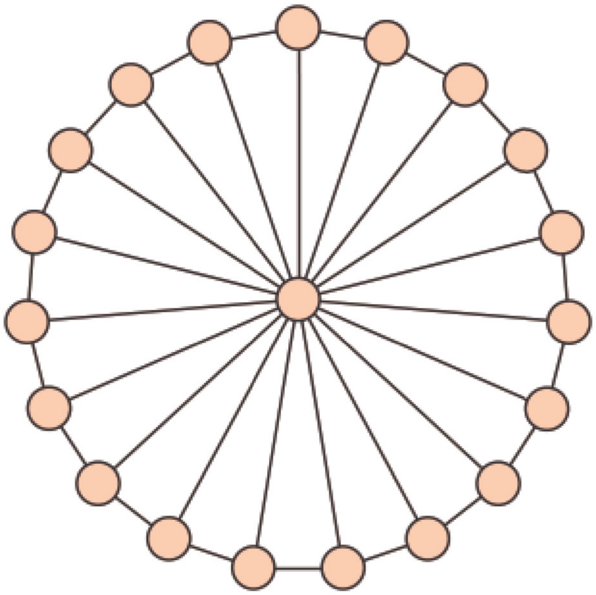
There are many special graphs and graph families that are available in Sage through the `graphs` module. They are referenced with the prefix `graphs.` followed by the name and zero or more paramenters inside parentheses. Here are a couple of them, first a complete graph with five vertices.

```
sage: graphs.CompleteGraph(5).show()
```



Here is a wheel graph, named for an obvious pattern of vertices and edges. We assign a name to it first and then show the graph without labeling the vertices.

```
sage: w=graphs.WheelGraph(20)
sage: w.show(vertex_labels=false)
```



There are dozens of graph methods, one of which determines the degree sequence of a graph.

```
sage:  w.degree_sequence()

[19, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3]
```

The degree sequence method is defined within the graphs module, but the prefix `graphs.` isn't needed because the value of `w` inherits the graphs methods.

Example 9.2.2. Consider an directed graph represented by the Division I NCAA college basketball teams in the United States for a given year. There are approximately 350 teams in Division 1. Suppose we constructed the graph with an edge from team A to team B if A beat B at least once in the season; and we label the edge with the number of wins. Since the average team plays around 30 games in a season, most of which will be against other Division I teams, we could expect around $\frac{30\times 350}{2} = 5250$ edges in the graph (this is somewhat reduced by games with lower division teams and cases where two or more wins over the same team produces one edge). Since 5250 is much smaller than $350^2 = 122\,500$ entries in an adjacency matrix, we would consider this a sparse graph and would expect to find one of the edge list structures most efficient. Even if an adjacency matrix is created, as could be done in *Mathematica*, it would be represented using a sparse matrix data structure.

EXERCISES FOR SECTION 9.2

A Exercises

1. Estimate the number of vertices and edges in each of the following graphs. Would the graph be considered sparse?

(a) Vertices: Cities of the world that are served by at least one airline.

Edges: Pairs of cities that are connected by a regular direct flight.

(b) Vertices: ASCII characters.

Edges: connect characters that differ in their binary code by exactly two bits.

(c) Vertices: All English words.

Edges: An edge connects word x to word y if x is a prefix of y.

2. Each edge of a graph is colored with one of the four colors red, blue, yellow, or green. How could you represent the edges in this graph using a variation of the adjacency matrix structure?

3. Directed graphs $G_1, \ldots, G_6$, each with vertex set {1, 2, 3, 4, 5} are represented by the matrices below. Which graphs are isomorphic?

$$G_1 : \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad G_2 : \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad G_3 : \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$G_4 : \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad G_5 : \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} \qquad G_6 : \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

4. The following Sage command verifies that the wheel graph with four vertices is isomorphic to the complete graph with four vertices.

```
    graphs.WheelGraph(4).is_isomorphic(graphs.CompleteGraph(4))
```

Evaluate the expression `dir(graphs.)` in Sage to get a list of graph names, and then find two more pairs of isomorphic graphs.

9.3 Connectivity

This section is devoted to a question that, when posed in relation to the graphs that we have examined, seems trivial. That question is: Given two vertices, s and t, of a graph, is there a path from s to t? If $s = t$, this question is interpreted as asking whether there is a circuit of positive length starting at s. Of course, for the graphs we have seen up to now, this question can be answered after a brief examination.

There are two situations under which a question of this kind is nontrivial. One is where the graph is very large and an "examination" of the graph could take a considerable amount of time. Anyone who has tried to solve a maze may have run into a similar problem. The second interesting situation is when we want to pose the question to a machine. If only the information on the edges between the vertices is part of the data structure for the graph, how can you put that information together to determine whether two vertices can be connected by a path?

Connectivity Terminology. Let v and w be vertices of a directed graph. Vertex v is *connected* to vertex w if there is a path from v to w. Two vertices are *strongly connected* if they are connected in both directions to one another. A *graph is connected* if, for each pair of distinct vertices, v and w, v is connected to w or w is connected to v. A *graph is strongly connected* if every pair of its vertices is strongly connected. For an undirected graph, in which edges can be used in either direction, the notions of strongly connected and connected are the same.

Theorem 9.3.1*. If a graph has n vertices and vertex u is connected to vertex w, then there exists a path from u to w of length no more than n.*

Proof (Indirect): Suppose u is connected to w, but the shortest path from u to w has length m, where $m > n$. A vertex list for a path of length m will have $m + 1$ vertices. This path can be represented as $(v_0, v_1, \ldots, v_m)$, where $v_0 = u$ and $v_m = w$. Note that since there are only n vertices in the graph and m vertices are listed in the path after v_0, we can apply the pigeonhole principle and be assured that there must be some duplication in the last m vertices of the vertex list, which represents a circuit in the path. This means that our path of minimum length can be reduced, which is a contradiction. ■

Methods for Testing Connectivity

Questions:

Question 1: Given a graph and two vertices in the graph, is there a path from the first vertex to the second?

Question 2: If the answer to Question 1 is "yes" then what is the path?

Some Answers

Method 1: Adjacency Matrix Method. Suppose that the information about edges in a graph is stored in an adjacency matrix, G. The relation, r, that G defines is $v\,r\,w$ if there is an edge connecting v to w. Recall that the composition of r with itself, r^2 , is defined by $v\,r^2\,w$ if there exists a vertex y such that $v\,r\,y$ and $y\,r\,w$; that is, v is connected to w by a path of length 2. We could prove by induction that the relation r^k , $k \geq 1$, is defined by $v\,r^k\,w$ if and only if there is a path of length k from v to w. Since the transitive closure, r^+ , is the union of r, r^2 , r^3, …, we can answer our connectivity question by determining the transitive closure of r, which can be done most easily by keeping our relation in matrix form. Theorem 9.3.1 is significant in our calculations because it tells us that we need only go as far as E^n to determine the matrix of the transitive closure.

The main advantage of the adjacency matrix method is that the transitive closure matrix can answer all questions about the existence of paths between vertices. If $G^+$is the matrix of the transitive closure, v_i, is connected to v_j if $(E^+)_{i\,j} = 1$. A directed graph is connected if $(E^+)_{i\,j} = 1$ or $(E^+)_{j\,i} = 1$ for each $i \neq j$. A directed graph is strongly connected if its transitive closure matrix has no zeros.

A disadvantage of the adjacency matrix method is that the transitive closure matrix tells us whether a path exists, but not what the path is.

Method 2: Broadcasting. We will describe this method first with an example.

Example 9.3.1. The football team at Mediocre State University (MSU) has had a bad year, 2 wins and 9 losses. Thirty days after the end of the football season, the university trustees is meeting to decide whether to rehire the head coach; things look bad for him. However, on the day of the meeting, the coach releases the following list of results from the past year:

Mediocre State defeated Local A&M.

Local A&M defeated City College.

City College defeated Corn State U.

... (25 results later)

Tough Tech defeated Enormous State University (ESU).

And ESU went on to win the national championship!

The trustees were so impressed that they rehired the coach with a raise in pay! How did the coach come up with such a list?

In reality, such lists exist occasionally and appear in newspapers from time to time. Of course they really don't prove anything since each team that defeated MSU in our example above can produce a similar chain of results. Since college football records are readily available, the coach could have found this list by trial and error. All that he needed to start with was that his team won at least one game. Since ESU lost one game, there was some hope of producing the chain.

The problem of finding this list is equivalent to finding a path in the tournament graph for last year's football season that initiates at MSU and ends at ESU. Such a graph is far from complete and would be represented using edge lists. To make the coach's problem interesting, let's imagine that only the winner of a game remembers the result of the game. The coach's problem has now taken on the flavor of a maze. To reach ESU, he must communicate with the various teams along the path. One way that the coach could have discovered his list in time is by sending the following emails to the coaches of the two teams that MSU defeated during the season:

When this example was first written, we commented that ties should be ignored. Most recent NCAA rules call for a tiebreaker in college football and so ties are no longer an issue. Email was also not common and we described the process in terms of letter, not email messages. The coach could also have asked the MSU math department to use *Mathematica* or Sage to get the path!

Dear Football Coach:
Please follow these directions exactly.

(1) If you are the coach at ESU, call the coach at MSU now and tell him who sent you this message.

(2) If you are not the coach at ESU and this is the first message of this type that you have received, then:
   (a) Remember who you received this message from.
   (b) Forward a copy of this message, signed by you, to each of the coaches whose teams you defeated during the past year.

(3) Ignore this message if you have received one like it already.

Signed,

Coach of MSU

Observations: From the conditions of this message, it should be clear that if everyone cooperates and if coaches participate within a day of receiving the message:

(a) If a path of length n exists from MSU to ESU, then the coach will know about it in n days.

(b) By making a series of phone calls, the coach can obtain the path that he wants by first calling the coach who defeated ESU (the person who sent ESU's coach that message). This coach will know who sent him a letter, and so on. Therefore, the vertex list of the desired path is obtained in reverse order.

(c) If a total of M football games were played, no more than M letters will be sent out.

(d) If a day passes without any letter being sent out, no path from MSU to ESU exists.

(e) This method could be extended to obtain a list of all teams that a given team can be connected to. Simply imagine a series of letters like the one above sent by each football coach and targeted at every other coach.

The general problem of finding a path between two vertices in a graph, if one exists, can be solved exactly as we solved the problem above. The following algorithm is commonly called a *breadth-first search*.

Algorithm 9.3.1. A broadcasting algorithm for finding a path between vertex i and vertex j of a graph having n vertices. The each item V_k of a list $V = \{V_1, V_2, \ldots, V_n\}$, consist of a Boolean field V_k.found and an integer field V_k.from. The sets D_1, D_2, …, called *depth sets*, have the property that if k is in D_r , then the shortest path from vertex i to vertex k is of length r. In Step 5, a stack is used to put the vertex list for the path from the vertex i to vertex j in the proper order.

```
1.  Set the value $V_k$.found equal to False, k = 1, 2, … , n
2.  r = 0
3.  $D_0 = \{i\}$
4.  While ($\neg$ $V_j$.found) and ($D_r \neq \emptyset$)
    4.1   $D_{r+1} = \emptyset$
    4.2   For each k in $D_r$ do
            For each edge (k,t) do
                If $V_t$.found == False
                  then  $V_t$.found = True
                        $V_t$.from = $k$
                        $D_{r+1} = D_{r+1} \cup \{t\}$
    4.3   r = r + 1
5. If $V_j$.found = True Then
    5.1   S = Empty Stack
    5.2   k=j
    5.3   While $V_k$.from $\neq$ $i$
            5.3.1 Push k onto S
            5.3.2 $k$ = $V_k$.from
```

Notes on Algorithm 9.3.1:

(a) This algorithm will produce one path from vertex i to vertex j, if one exists, and that path will be as short as possible. If more than one path of this length exists, then the one that is produced depends on the order in which the edges are examined and the order in which the elements of

D_r are examined in Step 4.

(b) The condition $D_r \neq \emptyset$ is analogous to the condition that if no mail is sent in a given stage of the process, in which case MSU cannot be connected to ESU.

(c) This algorithm can be easily revised to find paths to all vertices that can be reached from vertex i. Step 5 would be put off until a specific path to a vertex is needed since the information in V contains an efficient list of all paths. The algorithm can also be extended further to find paths between any two vertices.

Example 9.3.2. Consider the graph in Figure 9.3.1. The existence of a path from vertex 2 to vertex 3 is not difficult to determine by examination. After a few seconds, you should be able to find two paths of length four. Algorithm 9.3.1 will produce one of them.

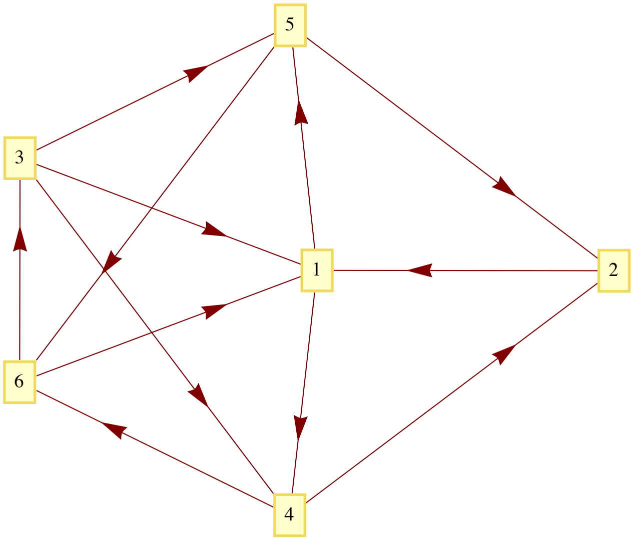


Figure 9.3.1

Suppose that the edges from each vertex are sorted in ascending order by terminal vertex. For example, the edges from vertex 3 would be in the order (3, 1), (3, 4), (3, 5). In addition, assume that in the body of Step 4 of the algorithm, the elements of D_r are used in ascending order. Then at the end of Step 4, the value of V will be

k	1	2	3	4	5	6	
V_k.found	T	T	T	T	T	T	
V_k.from	2	4	6	1	1	4	
Depth set	1	3	4	2	2	3	(value of r for which $k \in D_r$)

Therefore, the path (2, 1, 4, 6, 3) is produced by the algorithm. Note that if we wanted a path from 2 to 5, the information in V produces the path (2, 1, 5) since V_k.from = 1 and V_1.from = 2. A shortest circuit that initiates at vertex 2 is also available by noting that V_2.from = 4, V_4.from = 1 , and V_1.from = 2; thus the circuit (2, 1, 4, 2) is obtained.

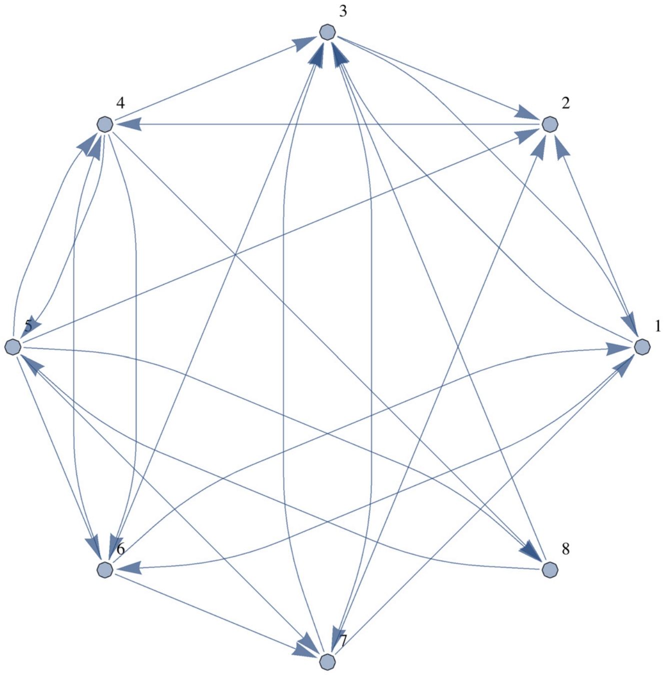
Mathematica Note

Consider the following defined by a adjecency matrix.

```
SeedRandom[2014];
adj = RandomInteger[{0, 1}, {8, 8}] * Table[Boole[i ≠ j], {i, 1, 8}, {j, 1, 8}]
```

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

```
g = AdjacencyGraph[adj, VertexLabels → "Name", ImagePadding → 5]
```



Is 1 is connected to 8 in this graph? The function `FindShortestPath` will give us a shortest:

```
FindShortestPath[g, 1, 8]
```

```
{1, 2, 4, 8}
```

If we are interested in reaching vertex 8 from all vertices, we can do that just as easily.

```
Map[{#, FindShortestPath[g, All, 8][#]} &, Range[8]]
```

```
⎛1  {1, 6, 4, 8}⎞
⎜2    {2, 4, 8} ⎟
⎜3  {3, 2, 4, 8}⎟
⎜4      {4, 8}  ⎟
⎜5      {5, 8}  ⎟
⎜6    {6, 4, 8} ⎟
⎜7  {7, 2, 4, 8}⎟
⎝8       {8}    ⎠
```

Finally, here is a matrix of shortest paths between any two vertices in the graph.

```
Map[Apply[FindShortestPath[g, All, All], #] &, Outer[List, Range[1, 8], Range[1, 8]], {2}]
```

```
⎛    {1}         {1, 2}      {1, 3}    {1, 2, 4}  {1, 2, 4, 5}   {1, 6}      {1, 6, 7}   {1, 2, 4, 8}⎞
⎜{2, 4, 3, 1}     {2}      {2, 4, 3}    {2, 4}     {2, 4, 5}   {2, 4, 6}  {2, 4, 3, 7}   {2, 4, 8}  ⎟
⎜   {3, 1}       {3, 2}       {3}     {3, 2, 4}  {3, 2, 4, 5}  {3, 1, 6}     {3, 7}    {3, 2, 4, 8}⎟
⎜ {4, 3, 1}    {4, 3, 2}    {4, 3}       {4}        {4, 5}      {4, 6}     {4, 3, 7}     {4, 8}    ⎟
⎜ {5, 7, 1}      {5, 2}    {5, 8, 3}    {5, 4}        {5}        {5, 6}      {5, 7}       {5, 8}    ⎟
⎜   {6, 1}     {6, 1, 2}    {6, 3}      {6, 4}     {6, 4, 5}      {6}        {6, 7}     {6, 4, 8}   ⎟
⎜   {7, 1}       {7, 2}      {7, 3}    {7, 2, 4}  {7, 2, 4, 5}  {7, 1, 6}      {7}     {7, 2, 4, 8}⎟
⎝ {8, 3, 1}    {8, 3, 2}    {8, 3}    {8, 5, 4}     {8, 5}     {8, 5, 6}   {8, 3, 7}      {8}      ⎠
```

If no path exists between two vertices, the result is an empty list, as illustrated by this simple example.

```
h = Graph[{1 → 2, 2 → 3, 3 → 4}];
FindShortestPath[h, 4, 1]
```

```
{}
```

Sage Note

Here is some sage code that

1. Generates a random undireced graph with 18 vertices. For each pair of vertices, an edge is included between them with probability 0.2. Since there are $\binom{18}{2} = 153$ potential edges, we expect that there will be approximately $0.2 \times 153 \approx 31$ edges.

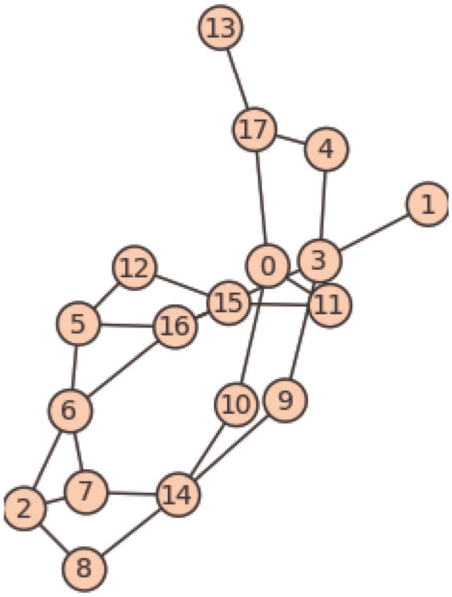
2. Counts the number of edges. In this case the number is a bit less than expected.

3. Finds a shortest path from vertex 0 to vertex 8.

4. Generates a list of vertices that would be reached in a breadth-first search. The expression `Gr.depth_first_search(0)` creates an iterator that is convenient for programming. Wrapping list( ) around the expression shows the order in which the vertices are visited.

5. Generates a list of vertices that would be reached in a depth-first search. In this type of search you travel in one direction away from the starting point until no further new vertices. We will discuss this search later.

```
sage:  Gr=graphs.RandomGNP(18,0.2);
          Gr.show()
```



```
sage:   len(Gr.edges(labels=False))
    25
sage:   Gr.shortest_path(0, 8)
    [0, 10, 14, 8]
sage:   list(Gr.breadth_first_search(0))
    [0, 17, 10, 11, 4, 13, 14, 3, 15, 7, 8, 9, 16, 1, 12, 2, 6, 5]
sage:   list(Gr.depth_first_search(0))
    [0, 11, 15, 12, 5, 6, 7, 14, 10, 9, 3, 4, 17, 13, 1, 16, 8, 2]
```

EXERCISES FOR SECTION 9.3

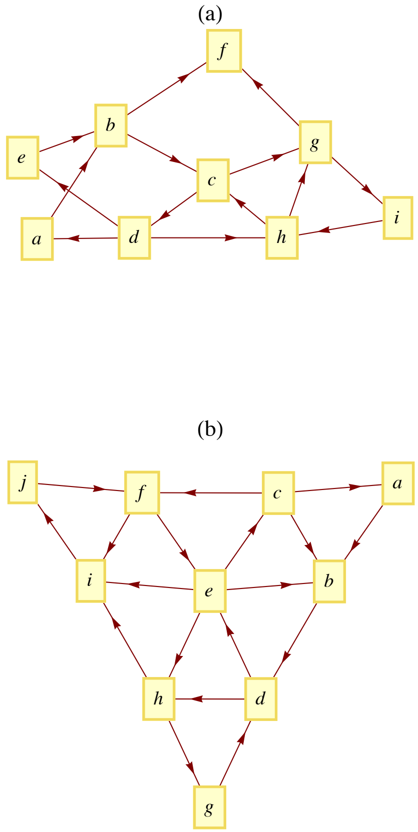
A Exercises

1. Apply Algorithm 9.3.1 to find a path from 5 to 1 in Figure 9.3.1. What would be the final value of V? Assume that the terminal vertices in edge lists and elements of the depth sets are put into ascending order, as we assumed in Example 9.3.1.

2. Apply Algorithm 9.3.1 to find a path from the bedroom to outside using the edge list data structure in Example 9.2.1. Assume that the elements of the depth sets are put into ascending order.

3. In a simple undirected graph with no self-loops, what is the maximum number of edges you can have, keeping the graph unconnected? What is the minimum number of edges that will assure that the graph is connected?

4. Use a broadcasting algorithm to determine the shortest path from vertex a to vertex i in the graphs shown in Figure 9.3.2. List the depth sets and the stack that is obtained.



(a)

(b)

Figure 9.3.2
Exercise 4

B Exercise

5. Prove (by induction on k) that if the relation r on vertices of a graph is defined by $v\, r\, w$ if there is an edge connecting v to w, then r^k , $k \geq 1$, is defined by $v\, r^k\, w$ if there is a path of length k from v to w.

9.4 Traversal: Eulerian and Hamiltonian Graphs

The subject of graph traversals has a long history. In fact, the solution by Leonhard Euler (Switzerland, 1707-83) of the Königsberg Bridge Problem is considered by many to represent the birth of graph theory.

The Königsberg Bridge Problem and Eulerian Graphs

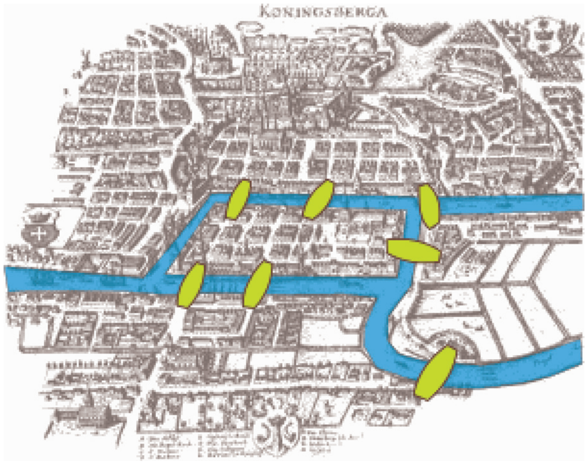


Figure 9.4.1
Map of Königsberg

A map of the Prussian city of Königsberg (circa 1735) in Figure 9.4.1 shows that there were seven bridges connecting the four land masses that made up the city. The legend of this problem states that the citizens of Königsberg searched in vain for a walking tour that passed over each bridge exactly once. No one could design such a tour and the search was abruptly abandoned with the publication of Euler's Theorem.

Theorem 9.4.1: Euler' s Theorem—Königsberg Case. *No walking tour of Königsberg can be designed so that each bridge is used exactly once.*

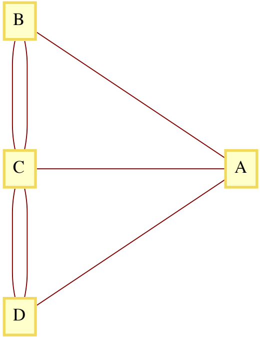


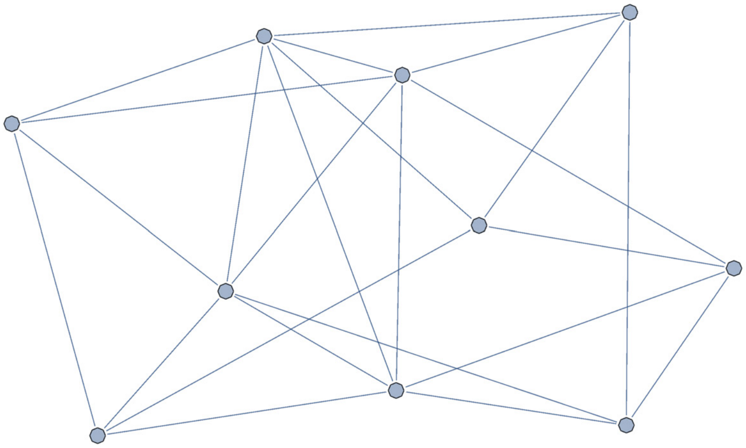
Figure 9.4.2
Multigraph representation of Königsberg

Proof: The map of Königsberg can be represented as an undirected multigraph, as in Figure 9.4.2. The four land masses are the vertices and each edge represents a bridge. The desired tour is then a path that uses each edge once and only once. Since the path can start and end at two different vertices, there are two remaining vertices that must be intermediate vertices in the path. If x is an intermediate vertex, then every time that you visit x, you must use two of its incident edges, one to enter and one to exit. Therefore, there must be an even number of edges connecting x to the other vertices. Since every vertex in the Königsberg graph has an odd number of edges, no tour of the type that is desired is possible. ■

As is typical of most mathematicians, Euler wasn't satisfied with solving only the Königsberg problem. His original theorem, which is paraphrased below, concerned the existence of paths and circuits like those sought in Königsberg. These paths and circuits have become associated with Euler's name.

Definitions: Eulerian Paths, Circuits, Graphs. *A Eulerian path through a graph is a path whose edge list contains each edge of the graph exactly once. If the path is a circuit, then it is called a Eulerian circuit. A Eulerian graph is a graph that possesses a Eulerian path.*

Example 9.4.1. Without tracing any paths, we can be sure that the graph below has an Eulerian circuit because all vertices have an even degree. This follows from the following theorem.



Theorem 9.4.2: Euler's Theorem—General Case. *An undirected graph is Eulerian if and only if it is connected and has either zero or two vertices with an odd degree. If no vertex has an odd degree, then the graph has a Eulerian circuit.*

Proof: It can be proven by induction that the number of vertices in an undirected graph that have an odd degree must be even. We will leave the proof of this fact to the reader as an exercise. The necessity of having either zero or two vertices of odd degree is clear from the proof of the Königsberg case of this theorem. Therefore, we will concentrate on proving that this condition is sufficient to ensure that a graph is Eulerian. Let k be the number of vertices with odd degree.

Phase 1. If $k = 0$, start at any vertex, v_0, and travel along any path, not using any edge twice. Since each vertex has an even degree, this path can always be continued past each vertex that you reach except v_0. The result is a circuit that includes v_0. If $k = 2$, let v_0 be either one of the vertices of odd degree. Trace any path starting at v_0 using up edges until you can go no further, as in the $k = 0$ case. This time, the path that you obtain must end at the other vertex of odd degree that we will call v_1. At the end of Phase 1, we have an initial path that may or may not be Eulerian. If it is not Eulerian, Phase 2 can be repeated until all of the edges have been used. Since the number of unused edges is decreased in any use of Phase 2, a Eulerian path must be obtained in a finite number of steps.

Phase 2. As we enter this phase, we have constructed a path that uses a proper subset of the edges in our graph. We will refer to this path as the current path. Let V be the vertices of our graph, E the edges, and E_u the edges that have been used in the current path. Consider the graph $G' = (V, E - E_u)$. Note that every vertex in G' has an even degree. Select any edge, e, from G'. Let v_a and v_b be the vertices that e connects. Trace a new path starting at v_a whose first edge is e. We can be sure that at least one vertex of the new path is also in the current path since (V, E) is connected. Starting at v_a, there exists a path in (V, E) to any vertex in the current path. At some point along this path, which we can consider the start of the new path, we will have intersected the current path. Since the degree of each vertex in G' is even, any path that we start at v_a can be continued until it is a circuit. Now, we simply augment the current path with this circuit. As we travel along the current path, the first time that we intersect the new path, we travel along it (see Figure 9.4.3). Once we complete the circuit that is the new path, we resume the traversal of the current path.

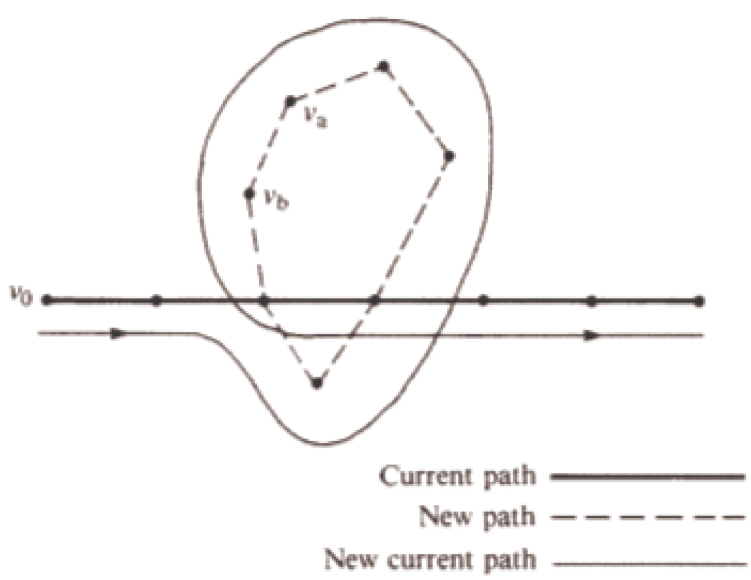


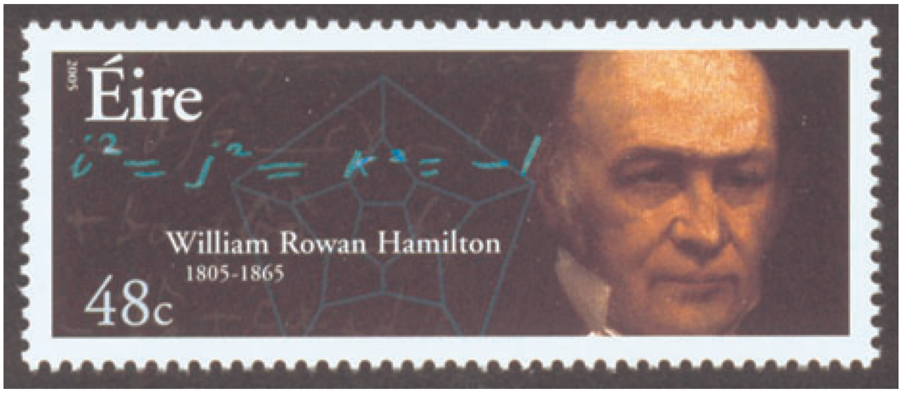
Figure 9.4.3
Augmenting the current path in the proof of Theorem 9.4.2

If the result of this phase is a Eulerian path, then we are finished; otherwise, repeat this phase. #

Example 9.4.2. The complete undirected graphs K_2 and K_{2n+1}, $n = 1, 2, 3, \ldots..,$ are Eulerian. If $n > 1$, then K_{2n} is not Eulerian.

HAMILTONIAN GRAPHS

To search for a path that uses every vertex of a graph exactly once seems to be a natural next problem after you have considered Eulerian graphs. The Irish mathematician Sir William Hamilton (1805-65) is given credit for first defining such paths. He is also credited with discovering the quaternions, for which he was honored by the Irish government with a postage stamp in 2004.



Definition: Hamiltonian Paths, Circuits, and Graphs. *A Hamiltonian path through a graph is a path whose vertex list contains each vertex of the graph exactly once, except if the path is a circuit, in which case the initial vertex appears a second time as the terminal vertex. If the path is a circuit, then it is called a Hamiltonian circuit. A Hamiltonian graph is a graph that possesses a Hamiltonian path.*

Example 9.4.3. Figure 9.4.4 shows a graph that is Hamiltonian. In fact, it is the graph that Hamilton used as an example to pose the question of existence of Hamiltonian paths in 1859. In its original form, the puzzle that was posed to readers was called "Around the World." The vertices were labeled with names of major cities of the world and the object was to complete a tour of these cities. The graph is also referred to as the dodecahedron graph, where vertices correspond with the corners of a dodecahedron and the edges are the edges of the solid that connect the corners.

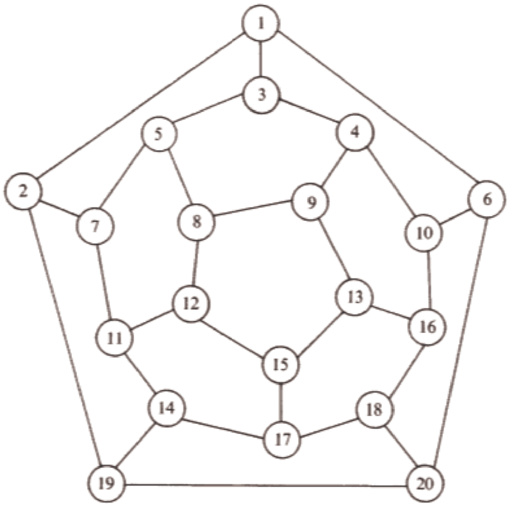


Figure 9.4.4
The dodecahedron graph, a Hamiltonian graph.

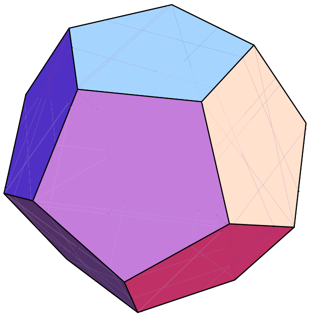


Figure 9.4.5
The regular dodecahedron

Unfortunately, a simple condition doesn't exist that characterizes a Hamiltonian graph. An obvious necessary condition is that the graph be connected; however, there is a connected undirected graph with four vertices that is not Hamiltonian. Can you draw such a graph?

A Note on What Is Possible and What Is Impossible. The search for a Hamiltonian path in a graph is typical of many simple-sounding problems in graph theory that have proven to be very difficult to solve. Although there are simple algorithms for conducting the search, they are impractical for large problems because they take such a long time to complete as graph size increases. Currently, every algorithm to search for a Hamiltonian path in a graph takes exponential time to complete. That is, if $T(n)$ is the time it takes to search a graph of n vertices, then there is a positive real number a, $a > 1$, such that $T(n) > a^n$ for all but possibly a finite number of positive values for n. No matter how close to 1 we can make a, a^n will grow at such a fast rate that the algorithm will not be feasible for large values of n. For a given algorithm, the value of a depends on the relative times that are assigned to the steps, but in the search for Hamiltonian paths, the actual execution time for known algorithms is large with 20 vertices. For 1,000 vertices, no algorithm is likely to be practical, and for 10,000 vertices, no currently known algorithm could be executed.

It is an unproven but widely held belief that no faster algorithm exists to search for Hamiltonian paths. A faster algorithm would have to be one that takes only, for example, polynomial time; that is, $T(n) < p(n)$, for some polynomial sequence p. To sum up, the problem of determining whether a graph is Hamiltonian is theoretically possible; however, for large graphs we consider it a practical impossibility. Many of the problems we will discuss in the next section, particularly the Traveling Salesman Problem, are thought to be impossible in the same sense.

Note: There are so-called subexponential algorithms with time complexities that lie between exponential and polynomial. These speeds are also thought to be generally unattainable in finding Hamiltonian paths.

Definition: The n-cube. *Let $n \geq 1$, and let B^n be the set of strings of 0's and 1's with length n. The n-cube is the undirected graph with a vertex for each string in B^n and an edge connecting each pair of strings that differ in exactly one position.*

The 1-cube, 2-cube, 3-cube, and 4-cube are shown in Figure 9.4.6.

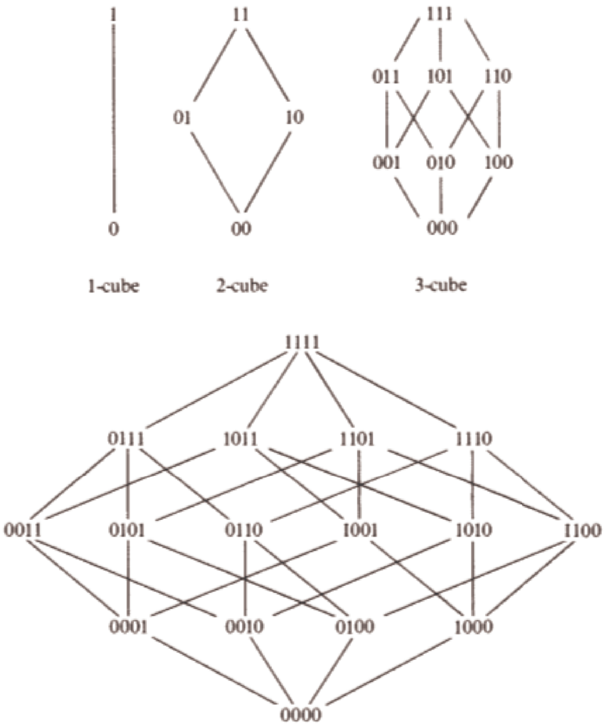


Figure 9.4.6
n-cubes, $n = 1, 2, 3, 4$

The Gray Code. A Hamiltonian circuit of the *n*-cube can be described recursively. The circuit itself, called the Gray Code, is not the only Hamiltonian circuit of the *n*-cube, but it is the easiest to describe. The standard way to write the Gray Code is as a column of strings, where the last string is followed by the first string to complete the circuit.

Basis ($n = 1$): The Gray Code for the 1-cube is $G_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Note that the edge between 0 and 1 is used twice in this circuit. That doesn't violate any rules for Hamiltonian circuits, but can only happen if a graph as two vertices.

Recursion: Given the Gray Code for the *n*-cube, $n > 1$, then G_{n+1} is obtained by (1) listing G_n with each string prefixed with 0, and then (2) reversing the list of strings in G_n with each string prefixed with 1. Symbolically, the recursion can be expressed as

$$G_{n+1} = \begin{pmatrix} 0\,G_n \\ 1\,{G_n}^r \end{pmatrix}$$

where ${G_n}^r$ is the reverse of list G_n. The Gray Codes for the 2-cube and 3-cube are

$$G_2 = \begin{pmatrix} 00 \\ 01 \\ 11 \\ 10 \end{pmatrix} \quad \text{and} \quad G_3 = \begin{pmatrix} 000 \\ 001 \\ 011 \\ 010 \\ 110 \\ 111 \\ 101 \\ 100 \end{pmatrix}$$

Applications of the Gray Code. One application of the Gray code was discussed in the Introduction to this book. An other application is in statistics. In a statistical analysis, there is often a variable that depends on several factors, but exactly which factors are significant may not be obvious. For each subset of factors, there would be certain quantities to be calculated. One such quantity is the multiple correlation coefficient for a subset. If the correlation coefficient for a given subset, *A*, is known, then the value for any subset that is obtained by either deleting or adding an element to *A* can be obtained quickly. To calculate the correlation coefficient for each set, we simply travel along G_n, where *n* is the number of factors being studied. The first vertex will always be the string of 0's, which represents the empty set. For each vertex that you visit, the set that it corresponds to contains the k^{th} factor if the k^{th} character is a 1.

EXERCISES FOR SECTION 9.4

A Exercises

1. Locate a map of New York City and draw a graph that represents its land masses, bridges and tunnels. Is there a Eulerian path through New York City? You can do the same with any other city that has at least two land masses.

2. Which of the drawings in Figure 9.4.7 can be drawn without removing your pencil from the paper and without drawing any line twice?

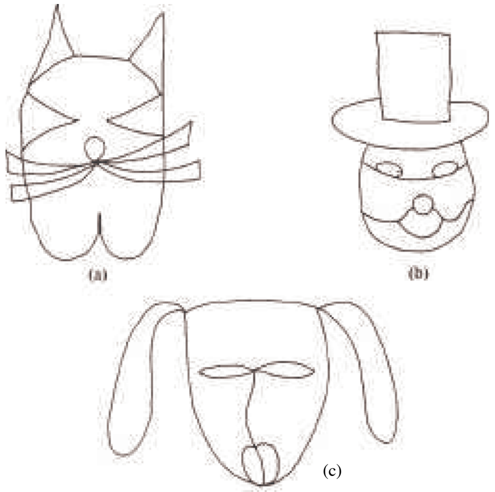


Figure 9.4.7
Exercise 2

3. Write out the Gray Code for the 4-cube.

4. Find a Hamiltonian circuit for the dodecahedron graph in Figure 9.4.4.

5. The Euler Construction Company has been contracted to construct an extra bridge in Königsberg so that a Eulerian path through the town exists. Can this be done, and if so, where should the bridge be built?

6. (a) Determine which of the graphs in Figure 9.4.8 has a Eulerian path?

   (b) Find a Eulerian path for the graphs that have one.

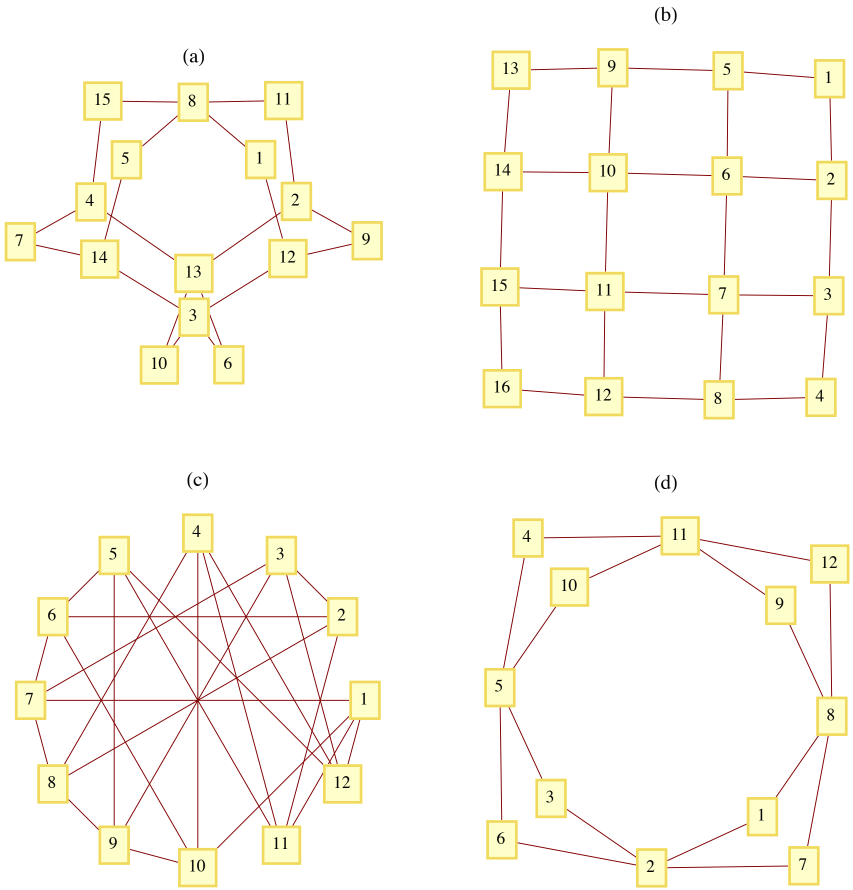


Figure 9.4.8
Exercise 6

B Exercises

7. Formulate Euler's theorem for directed graphs.

8. Prove that the number of vertices in an undirected graph with odd degree must be even. (Hint: Prove by induction on the number of edges.)

9. (a) Under what conditions will a round-robin tournament graph be Eulerian?

(b) Prove that every round-robin tournament graph is Hamiltonian.

10. For what values of *n* is *n*-cube Eulerian.

9.5 Graph Optimization

The common thread that connects all of the problems in this section is the desire to optimize (maximize or minimize) a quantity that is associated with a graph. We will concentrate most of our attention on two of these problems, the Traveling Salesman Problem and the Maximum Flow Problem. At the close of this section, we will discuss some other common optimization problems.

Definition: Weighted Graph. *A weighted graph, (V, E, w), is a graph (V, E) together with a weight function $w : E \to \mathbb{R}$. If $e \in E$, $w(e)$ is the weight on edge e.*

As you will see in our examples, $w(e)$ is usually a cost associated with the edge e; therefore, most weights will be positive.

Example 9.5.1. Let V be the set of six capital cities in New England: Boston, Augusta, Hartford, Providence, Concord, and Montpelier. Let E be $\{\{a, b\} \in V \times V \mid a \neq b\}$; that is, (V, E) is a complete unordered graph. An example of a weight function on this graph is

$$w(c_1, c_2) = \text{the distance from } c_1 \text{ to } c_2 .$$

Many road maps define distance functions as in Figure 9.5.1.

	ME	MA	NH	CT	VT	RI
Augusta, ME	–	165	148	266	190	208
Boston, MA	165	–	75	103	192	43
Concord, NH	148	75	–	142	117	109
Hartford, CT	266	103	142	–	204	70
Montpelier, VT	190	192	117	204	–	223
Providence, RI	208	43	109	70	223	–

FIGURE 9.5.1
Distances between capital cities of New England

The Traveling Salesman Problem

The Traveling Salesman Problem is, given a weighted graph, to find a circuit $(e_1, e_2, \ldots, e_n)$ that visits every vertex at least once and minimizes the sum of the weights,

$$\sum_{i=1}^{n} w(e_i)$$

Any such circuit is called an *optimal path*.

Notes. (a) Some statements of the Traveling Salesman Problem require that the circuit be Hamiltonian. In many applications, the graph in question will be complete and this restriction presents no problem.

(b) If the weight on each edge is constant, for example, $w(e) = 1$, then the solution to the Traveling Salesman Problem will be any Hamiltonian circuit, if one exists.

Example 9.5.2. The Traveling Salesman Problem gets its name from the situation of a salesman who wants to minimize the number of miles that he travels in visiting his customers. For example, if a salesman from Boston must visit the other capital cities of New England, then the problem is to find a circuit in the weighted graph of Example 9.5.1. Note that distance and cost are clearly related in this case. In addition, tolls and traffic congestion might also be taken into account in this case.

The search for an efficient algorithm that solves the Traveling Salesman has occupied researchers for years. If the graph in question is complete, there are $(n-1)!$ different circuits. As n gets large, it is impossible to check every possible circuit. The most efficient algorithms for solving the Traveling Salesman Problem take an amount of time that is proportional to $n\,2^n$. Since this quantity grows so quickly, we can't expect to have the time to solve the Traveling Salesman Problem for large values of n. Most of the useful algorithms that have been developed have to be heuristic; that is, they find a circuit that should be close to the optimal one. One such algorithm is the "closest neighbor" algorithm, one of the earliest attempts at solving the Traveling Salesman Problem. The general idea behind this algorithm is, starting at any vertex, to visit the closest neighbor to the starting point. At each vertex, the next vertex that is visited is the closest one that has not been reached. This shortsighted approach typifies heuristic algorithms called *greedy algorithms*, which attempt to solve a minimization (maximization) problem by minimizing (maximizing) the quantity associated with only the first step.

Algorithm 9.5.1. The Closest Neighbor Algorithm. *Let $G = (V, E, w)$ be a complete weighted graph with $|V| = n$. The closest neighbor circuit through G starting at v_1 is $(v_1, v_2, \ldots, v_n)$, defined by the steps:*

```
1. $V_1 = V - \{v_1\}$.
2. For $k = 2$ to $n - 1$
      2.1 $v_k$ = the closest vertex in $V_{k-1}$ to $v_{k-1}$
            (* $w(v_{k-1}, v_k) = min(w(v_{k-1}, v) \mid v \in V_{k-1})$ *)
            In case of a tie for closest, $v_k$ may be chosen arbitrarily.
      2.2 $V_k = V_{k-1} - \{v_k\}$
3. $v_n$ = the only element of $V_n$.
```

The cost of the closest neighbor circuit is

$$\sum_{k=1}^{n-1} w(v_k, v_{k+1}) \ + w(v_n, v_1)$$

Example 9.5.3. The closest neighbor circuit starting at A in Figure 9.5.2 is (1, 3, 2, 4, 1), with a cost of 29. The optimal path is (1, 2, 3, 4, 1), with a cost of 27.

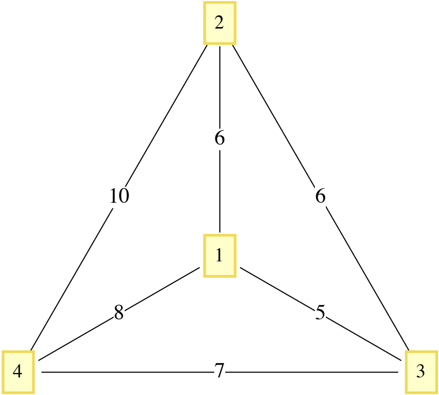


FIGURE 9.5.2
Example 9.5.3

Although the closest neighbor circuit is often not optimal, we may be satisfied if it is close to optimal. If C_{opt} and C_{cn} are the costs of optimal and closest neighbor circuits in a graph, then it is always the case that $C_{\text{opt}} \leq C_{\text{cn}}$ or $\frac{C_{\text{cn}}}{C_{\text{opt}}} \geq 1$. We can assess how good the closest neighbor algorithm is by determining how small the quantity $\frac{C_{\text{cn}}}{C_{\text{opt}}}$ gets. If it is always near 1, then the algorithm is good. However, if there are graphs for which it is large, then the algorithm may be discarded. Note that in Example 9.5.3, $\frac{C_{\text{cn}}}{C_{\text{opt}}} = \frac{29}{27} \approx 1.074$. A 7% increase in cost may or may not be considered significant, depending on the situation.

Example 9.5.4. A salesman must make stops at vertices A, B, and C, which are all on the same one-way street. The graph in Figure 9.5.3 is weighted by the function

$w(i, \ j) \ = \$ the time it takes to drive from vertex i to vertex j.

Note that if j is down the one-way street from i, then $w(i, \ j) \ < \ w(j, \ i)$. The values of C_{opt} , and C_{cn} are 20 and 32, respectively. Verify that C_{cn} is 32 by using the closest neighbor algorithm. The value of $\frac{C_{\text{cn}}}{C_{\text{opt}}} \ = \ 1.6$ is significant in this case since our salesman would spend 60% more time on the road if he used the closest neighbor algorithm.

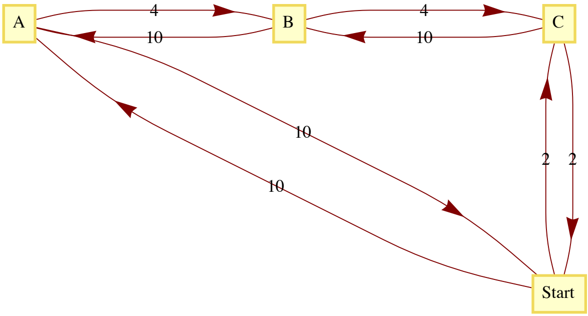


FIGURE 9.5.3
Example 9.5.4

A more general result relating to the closest neighbor algorithm presumes that the graph in question is complete and that the weight function satisfies the conditions

(1) $w(x, \ v) \ = \ w(y, \ x)$ for all x, y in the vertex set, and

(2) $w(x, \ y) \ + \ w(y, \ z) \ \geq \ w(x, \ z)$ for all x, y, z in the vertex set.

The first condition is called the *symmetry condition* and the second is the *triangle inequality*.

The following theorem's reference needs to be updated:

Theorem 9.5.1. If $(V,\ E,\ w)$ is a complete weighted graph that satisfies the symmetry and triangle inequality conditions, then

$$\frac{C_{cn}}{C_{opt}} \leq \frac{\lceil log_2(2\,n)\rceil}{2} \qquad (9.5a)$$

Proof: See Liu, pages 105-109.

Notes: (a) If $|\,V\,| = 8$, then this theorem says that C_{cn} can be no larger than twice the size of C_{opt}; however, it doesn't say that the closest neighbor circuit will necessarily be that far from an optimal circuit. The quantity $\frac{\lceil \log_2(2\,n)\rceil}{2}$ is called an upper bound for the ratio $\frac{C_{\text{cn}}}{C_{\text{opt}}}$. It tells us only that things can't be any worse than the upper bound. Certainly, there are many graphs with eight vertices such that the optimal and closest neighbor circuits are the same. What is left unstated in this theorem is whether there are graphs for which the quantities in 9.5a are equal. If there are such graphs, we say that the upper bound is *sharp*.

(b) The value of $\frac{C_{\text{cn}}}{C_{\text{opt}}}$ in Example 9.5.4 is 1.6, which is greater than $\frac{\lceil \log_2(2\times 4)\rceil}{2} = 1.5$; however, the weight function in this example does not satisfy the conditions of the theorem.

The Traveling Salesman Problem—Unit Square Version

Example 9.5.5. A robot is programmed to weld joints on square metal plates. Each plate must be welded at prescribed points on the square. To minimize the time it takes to complete the job, the total distance that a robot's arm moves should be minimized. Let $d(P,\ Q)$ be the distance between P and Q. Assume that before each plate can be welded, the arm must be positioned at a certain point P_0 . Given a list of n points, we want to put them in order so that

$$d(P_0, P_1) + d(P_1, P_2) + \cdots + d(P_{n-1}, P_n) + d(P_n, P_0)$$

is as small as possible.

The type of problem that is outlined in Example 9.5.5 is of such importance that it is probably the most studied version of the Traveling Salesman Problem. What follows is the usual statement of the problem. Let $[0,\ 1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$, and let $S = [0,\ 1]^2$, the unit square. Given n pairs of real numbers $(x_1,\ y_1), (x_2, y_2), \ldots, (x_n, y_n)$ in S that represent the n vertices of a K_n , find a circuit of the graph that minimizes the sum of the distances traveled in traversing the circuit.

Since the problem calls for a circuit, it doesn't matter which vertex we start at; assume that we will start at (x_1, y_1). Once the problem is solved, we can always change our starting position. A function can most efficiently describe a circuit in this problem. Every bijection $f: \{1,\ \ldots,\ n\} \to \{1,\ \ldots,\ n\}$ with $f(1) = 1$ describes a circuit

$$(x_1,\ y_1), \left(x_{f(2)}, y_{f(2)}\right), \ldots, \left(x_{f(n)}, y_{f(n)}\right)$$

Since there are $(n - 1)!$ such bijections, an examination of all possible circuits is not feasible for large values of n.

One popular heuristic algorithm is the strip algorithm:

Algorithm 9.5.2: The Strip Algorithm. *Given n points in the unit square:*

Phase 1:

(1.1) Divide the square into $\left\lceil \sqrt{n/2}\,\right\rceil$ vertical strips, as in Figure 9.5.4. Let d be the width of each strip. If a point lies on a boundary between two strips, consider it part of the left-hand strip.

(1.2) Starting from the left, find the first strip that contains one of the points. Locate the starting point by selecting the first point that is encountered in that strip as you travel from bottom to top. We will assume that the first point is (x_1, y_1)

(1.3) Alternate traveling up and down the strips that contain vertices until all of the vertices have been reached.

(1.4) Return to the starting point.

Phase 2:

(2.1) Shift all strips $d/2$ units to the right (creating a small strip on the left).

(2.2) Repeat Steps 1.2 through 1.4 of Phase 1 with the new strips.

When the two phases are complete, choose the shorter of the two circuits obtained.

Step 1.3 needs a bit more explanation. How do you travel up or down a strip? In most cases, the vertices in a strip will be vertically distributed so that the order in which they are visited is obvious. In some cases, however, the order might not be clear, as in the third strip in Phase I of Figure 9.5.4. Within a strip, the order in which you visit the points (if you are going up the strip) is determined thusly: (x_i, y_i) precedes $\left(x_j, y_j\right)$

if $y_i < y_j$ or if $y_i = y_j$ and $x_i < x_j$. In traveling down a strip, replace $y_i < y_j$ with $y_i > y_j$.

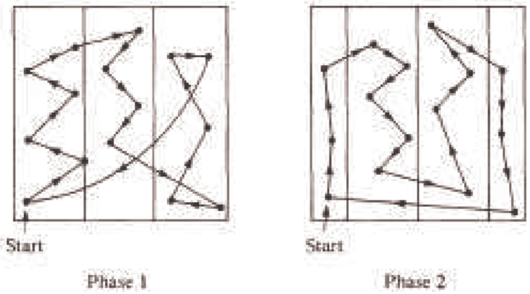


FIGURE 9.5.4
The Strip Algorithm

The selection of $\left\lceil\sqrt{n/2}\right\rceil$ strips was made in a 1959 paper by Beardwood, Halton, and Hammersley. It balances the problems that arise if the number of strips is too small or too large. If the square is divided into too few strips, some strips may be packed with vertices so that visiting them would require excessive horizontal motion. If too many strips are used, excessive vertical motion tends to be the result. An update on what is known about this algorithm is contained in the paper by K. J. Supowit, E. M. Reingold, and D. A. Plaisted.

Since the construction of a circuit in the square consists of sorting the given points, it should come as no surprise that the strip algorithm requires a time that is roughly a multiple of $n \log n$ time units when n points are to be visited.

The worst case that has been encountered with this algorithm is one in which the circuit obtained has a total distance of approximately $\sqrt{2\,n}$ (see Sopowit et al.).

NETWORKS AND THE MAXIMUM FLOW PROBLEM

Definition: Network. *A network is a simple weighted directed graph that contains two distinguished vertices called the source and the sink with the property that the indegree of the source and outdegree of the sink are both zero. The weight function on a network is the capacity function.*

An example of a real situation that can be represented by a network is a city's water system. A reservoir would be the source, while a distribution point in the city to all of the users would be the sink. The system of pumps and pipes that carries the water from source to sink makes up the remaining network. We can assume that the water that passes through a pipe in one minute is controlled by a pump and the maximum rate is determined by the size of the pipe and the strength of the pump. This maximum rate of flow through a pipe is called its capacity and is the information that the weight function of a network contains.

Example 9.5.6. Consider the system that is illustrated in Figure 9.5.5. The numbers that appear next to each pipe indicate the capacity of that pipe in thousands of gallons per minute. This map can be drawn in the form of a network, as in Figure 9.5.6.

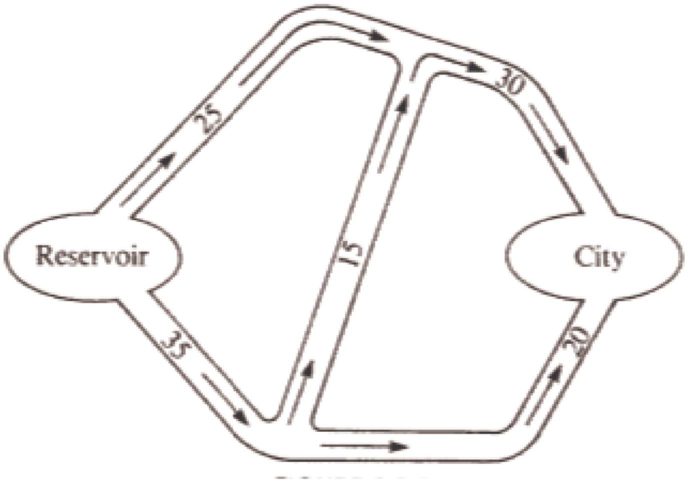


FIGURE 9.5.5
Diagram of a city's water system

Although the material passing through this network is water, networks can also represent the flow of other materials, such as automobiles, electricity, telephone calls or patients in a health system.

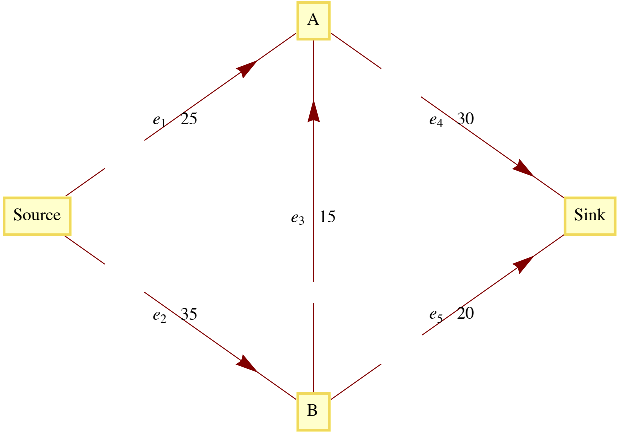


FIGURE 9.5.6
Flow diagram for a city's water system

The Maximum Flow Problem is derived from the objective of moving the maximum amount of water or other material from the source to the sink. To measure this amount, we define a flow as a function $f : E \to \mathbb{R}$ such that (1) the flow of material through any edge is nonnegative and no larger than its capacity: $0 \leq f(e) \leq w(e)$, for all $e \in E$; and (2) for each vertex other than the source and sink, the total amount of material that is directed into a vertex is equal to the total amount that is directed out:

$$\begin{aligned} \sum_{(x,v)\in E} f(x, v) &= \sum_{(v,y)\in E} f(v, y) \\ \text{Flow into } v &= \text{Flow out of } v \end{aligned} \qquad (9.5b)$$

The summation notation on the left of 9.5b represents the sum of the flows through each edge in E that has v as a terminal vertex. The right-hand side indicates that you should add all of the flows through edges that initiate at v.

Theorem 9.5.2. *If f is a flow, then*

$$\sum_{(source,v)\in E} f(source, v) = \sum_{(v,sink)\in E} f(v, sink)$$

This common value is called the value of the flow. We will denote the value of a flow by $V(f)$. The value of a flow represents the amount of material that passes through the network with that flow.

Proof. Subtract the right-hand side of 9.5b from the left-hand side. The result is:

$$\text{Flow into } v - \text{Flow out of } v = 0$$

Now sum up these differences for each vertex in $V' = V - \{\text{source}, \text{sink}\}$. The result is

$$\sum_{v\in V'} \left(\sum_{(x,v)\in E} f(x, v) - \sum_{(v,y)\in E} f(v, y) \right) = 0 \qquad (9.5c)$$

Now observe that if an edge connects two vertices in V, its flow appears as both a positive and a negative term in 9.5c. This means that the only positive terms that are not cancelled out are the flows into the sink. In addition, the only negative terms that remain are the flows out of the source. Therefore,

$$\sum_{(v,\text{sink})\in E} f(v, \text{sink}) - \sum_{(\text{source},v)\in E} f(\text{source}, v) = 0 \qquad \blacksquare$$

MAXIMAL FLOWS

Since the Maximum Flow Problem consists of maximizing the amount of material that passes through a given network, it is equivalent to finding a flow with the largest possible value. Any such flow is called a maximal flow.

For the network in Figure 9.5.6, one flow is f_1, defined by $f_1(e_1) = 25$, $f_1(e_2) = 20$, $f_1(e_3) = 0$, $f_1(e_4) = 25$, and $f_1(e_5) = 20$. The value of f_1, $V(f_1)$, is 45. Since the total flow into the sink can be no larger than 50 ($w(e_4) + w(e_5) = 30 + 20$), we can tell that f_1 is not very far from the solution. Can you improve on f_1 at all? The sum of the capacities into the sink can't always be obtained by a flow. The same is true for the sum of the capacities out of the source. In this case, the sum of the capacities out of the source is 60, which obviously can't be reached in this network.

A solution of the Maximum Flow Problem for this network is the maximal flow f_2, where $f_2(e_1) = 25$, $f_2(e_2) = 25$, $f_2(e_3) = 5$, $f_2(e_4) = 30$, and $f_2(e_5) = 20$, with $V(f_2) = 50$. This solution is not unique. In fact, there is an infinite number of maximal flows for this problem.

There have been several algorithms developed to solve the Maximal Flow Problem. One of these is the Ford and Fulkerson Algorithm (FFA).

The FFA consists of repeatedly finding paths in a network called flow augmenting paths until no improvement can be made in the flow that has been obtained.

Definition: Flow Augmenting Path. *Given a flow f in a network (V, E), a flow augmenting path with respect to f is a simple path from the source to the sink using edges both in their forward and their reverse directions such that for each edge e in the path, $w(e) - f(e) > 0$ if e is used in its forward direction and $f(e) > 0$ if e is used in the reverse direction.*

Example 9.5.7. For f_1 in Example 9.5.6, a flow augmenting path would be (e_2, e_3, e_4) since

$$w(e_2) - f_1(e_2) = 15,\ w(e_3) - f_1(e_3) = 5, \text{and } w(e_4) - f_1(e_4) = 5.$$

These positive differences represent unused capacities, and the smallest value represents the amount of flow that can be added to each edge in the path. Note that by adding 5 to each edge in our path, we obtain f_2, which is maximal. If an edge with a positive flow is used in its reverse direction, it is contributing a movement of material that is counterproductive to the objective of maximizing flow. This is why the algorithm directs us to decrease the flow through that edge.

Algorithm 9.5.3: The Ford and Fulkerson Algorithm.

```
(1) Define the flow function $f_0$ by $f_0(e) = 0$ for each edge $e \in E$.
(2) $i = 0$.
(3) Repeat:
    (3.1) If possible, find a flow augmenting path with respect to $f_i$.
    (3.2) If a flow augmenting path exists, then:
        (3.2.1) Determine
            $d = min\{\{w(e) - f_i(e) \mid e$ is used in the forward direction$\}$,
                    $\{f_i(e) \mid e$ is used in the reverse direction$\}\}$
        (3.2.2) Define $f_{i+1}$ by
            $f_{i+1}(e) = f_i(e)$      if e is not part of the flow augmenting path
            $f_{i+1}(e) = f_i(e) + d$  if e is used in the forward direction
            $f_{i+1}(e) = f_i(e) - d$  if e is used in the reverse direction
        (3.2.3) $i = i + 1$.
  until no flow augmenting path exists.
(4) Terminate with a maximal flow $f_i$
```

Notes:

(a) It should be clear that every flow augmenting path leads to a flow of increased value and that none of the capacities of the network can be violated.

(b) The depth-first search should be used to find flow augmenting paths since it is far more efficient than the breadth-first search in this situation. The depth-first search differs from the broadcasting algorithm (a variation of the breadth-first search) in that you sequentially visit vertices until you reach a "dead end" and then backtrack.

(c) There have been networks discovered for which the FFA does not terminate in a finite number of steps. These examples all have irrational capacities. It has been proven that if all capacities are positive integers, the FFA terminates in a finite number of steps. See Ford and Fulkerson, Even, or Berge for details.

(d) When you use the FFA to solve the Maximum Flow Problem by hand it is convenient to label each edge of the network with the fraction $f_i(e)/w(e)$.

A Depth-First Search for the Sink Initiating at the Source. *Let E' be the set of directed edges that can be used in producing a flow augmenting path. Add to the network a vertex called start and the edge (start, source).*

```
(1)    S = vertex set of the network.
(2)    p = start.
(3)    p = source   (*Move p along the edge (start, source) *)
(4) **While** p is not equal to start or sink **do**.
       **If** an edge in E' exists that takes you from p to another vertex in S
           **then** set p to be that next vertex and delete the edge from E'.
           **else** reassign p to be the vertex that p was reached from (i.e., backtrack).
(5) **If** p = start,
       **then** no flow augmenting path exists.
       **else** p = sink, you have found a flow augmenting path.
```

Example 9.5.8. Consider the network in Figure 9.5.7, where the current flow, f, is indicated by a labeling of the edges. The path $(Source, v_2, v_1, v_3, Sink)$ is a flow augmenting path that allows us to increase the flow by one unit. Note that (v_1, v_3) is used in the reverse direction, which is allowed because $f(v_1, v_3) > 0$. The value of the new flow that we obtain is 8. This flow must be maximal since the capacities out of the source add up to 8. This maximal flow is defined by the labeling of Figure 9.5.8.

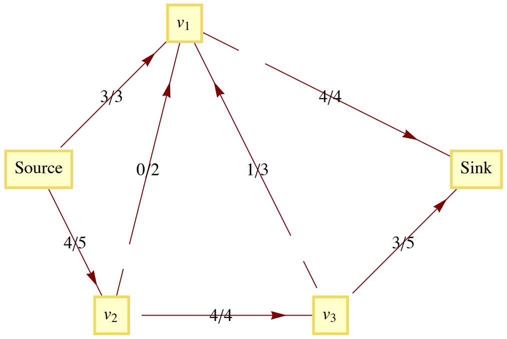


FIGURE 9.5.7
Current flow in Example 9.5.8

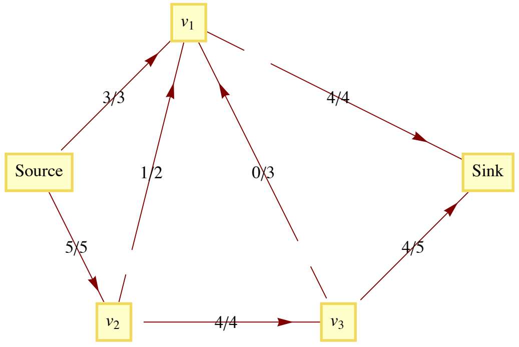


FIGURE 9.5.8
Augmented, optimal flow in Example 9.5.8

OTHER GRAPH-OPTIMIZATION PROBLEMS

(a) *The Minimum Spanning Tree Problem*: Given a weighted graph, (V, E, w), find a subset E' of E with the properties that (V, E') is connected and the sum of the weights of edges in E' are as small as possible. We will discuss this problem in Chapter 10.

(b) *The Minimum Matching Problem*: Given an undirected weighted graph, $(K E, w)$, with an even number of vertices, pair up the vertices so that each pair is connected by an edge and the sum of these edges is as small as possible. A unit square version of this problem has been studied extensively. See References: [Sopowit001] for details on what is known about this version of the problem.

(c) *The Graph Center Problem*: Given a connected, undirected, weighted graph, find a vertex (the center) in the graph with the property that the distance from the center to every other vertex is as small as possible. "As small as possible" could be interpreted either as minimizing the sum of the distances to each vertex or as minimizing the maximum distance from the center to a vertex.

EXERCISES FOR SECTION 9.5

A Exercises

1. Find the closest neighbor circuit through the six capitals of New England starting at Boston. If you start at a different city, will you get a different circuit?

2. Is Theorem 9.5.1 sharp for $n = 3$? For $n = 4$?

3. Given the following sets of points in the unit square, find the shortest circuit that visits all the points and find the circuit that is obtained with the strip algorithm.

(a) $\{(0.1 k, 0.1 k) : k = 0, 1, 2, \ldots, 10\}$

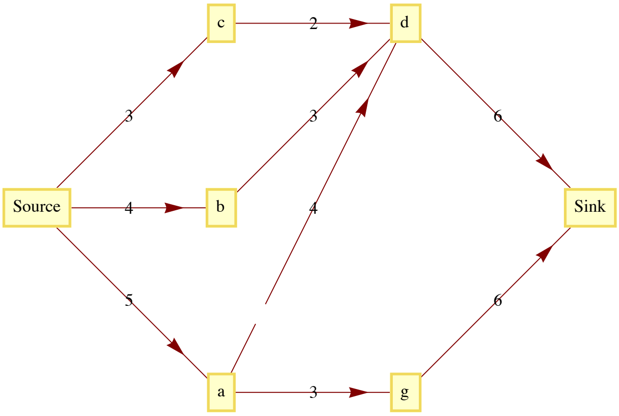
(b) $\{(0.1, 0.3), (0.3, 0.8), (0.5, 0.3), (0.7, 0.9), (0.9, 0.1)\}$

(c) $\{(0.0, 0.5), (0.5, 0.0), (0.5, 1.0), (1.0, 0.5)\}$

(d) $\{(0, 0), (0.2, 0.6), (0.4, 0.1), (0.6, 0.8), (0.7, 0.5)\}$

4. For $n = 4, 5,$ and 6, locate n points in the unit square for which the strip algorithm works poorly.

5. Consider the network whose maximum capacities are shown on the following graph.



(a) A function f is partially defined on the edges of this network by:

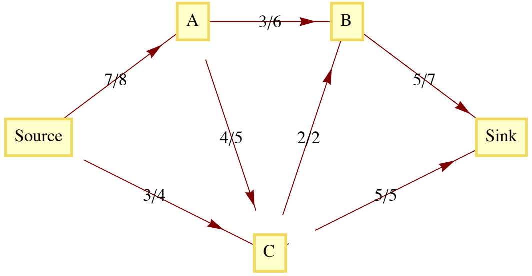
$$f(\text{Source}, c) = f(\text{Source}, b) = f(\text{Source}, a) = 2, \text{ and } f(a, d) = 1.$$

Define f on the rest of the other edges so that f is a flow. What is the value of f?

(b) Find a flow augmenting path with respect to f for this network. What is the value of the augmented flow?

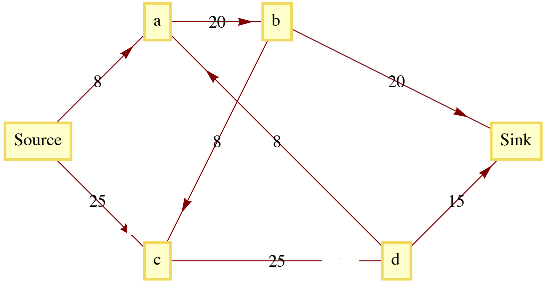
(c) Is the augmented flow a maximum flow? Explain.

6. Given the following network with capacity function c and flow function f, find a maximal flow function. The labels on the edges of the network are of the form $f(e)/c(e)$, where $c(e)$ is the capacity of edge e and $f(e)$ is the used capacity for flow f.

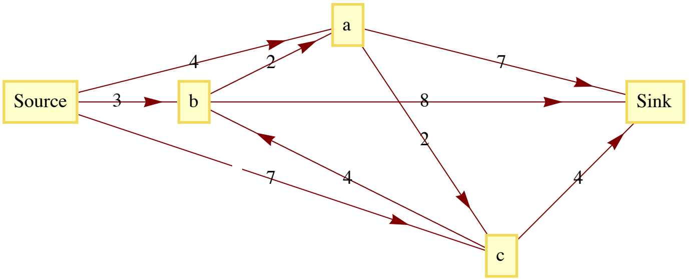


7. Find maximal flows for the following networks.

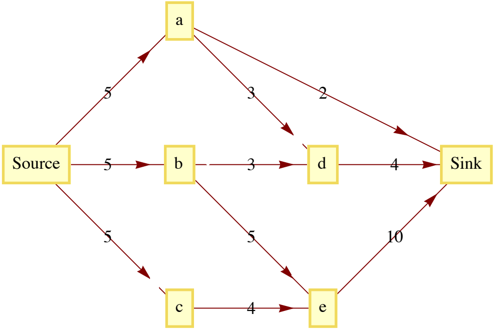
(a)



(b)



(c)



B Exercises

8. (a) [Easy] Find two maximal flows for the network in Figure 9.5.6 other than the one found in the text.

(b) [Harder] Describe the set of all maximal flows for the same network.

(c) [Hardest] Prove that if a network has two maximal flows, then it has an infinite number of maximal flows.

9. Discuss reasons that the closest neighbor algorithm is not used in the unit square version of the Traveling Salesman Problem. (Hint: Count the number of comparisons of distances that must be done.)

C Exercises

10. Explore the possibility of solving the Traveling Salesman Problem in the "unit box": $[0,\ 1]^3$.

11. Devise a "closest neighbor" algorithm for matching points in the unit square.

9.6 Planarity and Colorings

The topics in this section are related to how graphs are drawn.

Planarity: Can a given graph be drawn in a plane so that no edges intersect? Certainly, it is natural to avoid intersections, but up to now we haven't gone out of our way to do so.

Colorings: Suppose that each vertex in an undirected graph is to be colored so that no two vertices that are connected by an edge have the same color. How many colors are needed? This question is motivated by the problem of drawing a map so that no two bordering countries are colored the same. A similar question can be asked for coloring edges.

Definition: Planar Graph/ Plane Graph/Planar Embedding. *A graph is planar if it can be drawn in a plane so that no edges cross. If a graph is drawn so that no edges intersect, it is a plane graph, and such a drawing is a planar embedding of the graph.*

Example 9.6.1. The graph in Figure 9.6.1(a) is planar but not a plane graph. The same graph is drawn as a plane graph in Figure 9.6.1(b)

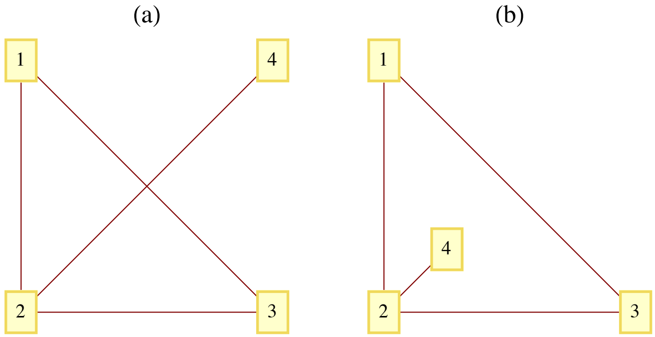


Figure 9.6.1
A planar graph and a planar embedding

Notes:

(a) In discussing planarity, we need only consider simple undirected graphs with no self-loops. All other graphs can be treated as such since all of the edges that relate any two vertices can be considered as one "package" that clearly can be drawn in a plane.

(b) Can you think of a graph that is not planar? How would you prove that it isn't planar? Proving the nonexistence of something is usually more difficult than proving its existence. This case is no exception. Intuitively, we would expect that sparse graphs would be planar and dense graphs would be nonplanar. Theorem 9.6.2 will verify that dense graphs are indeed nonplanar.

(c) The topic of planarity is a result of trying to restrict a graph to two dimensions. Is there an analogous topic for three dimensions? What graphs can be drawn in one dimension?

Answer to Note c: If a graph has only a finite number of vertices, it can always be drawn in three dimensions. This is not true for all graphs with an infinite number of vertices. The only "one-dimensional" graphs are the ones that consist of a finite number of chains, as in Figure 9.6.2, with one or more vertices in each chain.

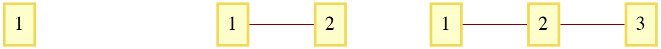


Figure 9.6.2
Chains of length one, two and three

Example 9.6.2. A discussion of planarity is not complete without mentioning the famous Three Utilities Puzzle. The object of the puzzle is to supply three houses, A, B, and C, with the three utilities, gas, electric, and water. The constraint that makes this puzzle impossible to solve is that no utility lines may intersect i. e., a planar embedding of the graph in Figure 9.6.3, which is commonly denoted $K_{3,3}$. This graph is one of two fundamental nonplanar graphs. The Kuratowski Reduction Theorem states that if a graph is nonplanar then "contains" either a $K_{3,3}$ or a K_5. Containment is in the sense that if you start with a nonplanar graph you can always perform a sequence of edge deletions and contractions (shrinking an edge so that the two vertices connecting it coincide) to produce one of the two graphs.

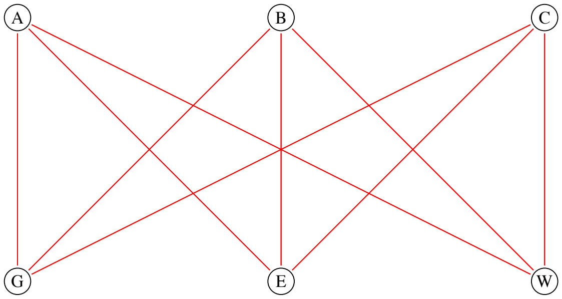


Figure 9.6.3
The Three Utilities Puzzle.

A planar graph divides the plane into one or more regions. Two points on the plane lie in the same region if you can draw a curve connecting the two points that does not pass through an edge. One of these regions will be of infinite area. Each point on the plane is either a vertex, a point on an edge, or a point in a region. A remarkable fact about the geography of planar graphs is the following theorem that is attributed to Euler.

Theorem 9.6.1: Euler's Formula. *If G = (V, E) is a connected planar graph with r regions, v vertices and e edges, then*

$$v + r - e = 2 \qquad (9.6a)$$

Experiment: Jot down a graph right now and count the number of vertices, regions, and edges that you have. If $v + r - e$ is not 2, then your graph is either nonplanar or not connected.

Proof: We prove Euler's Formula by Induction on e, for $e \geq 0$.

Basis: If $e = 0$, then G must be a graph with one vertex, $v = 1$; and there is one infinite region, $r = 1$.

Therefore, $v + r - e = 1 + 1 - 0 = 2$, and the basis is true.

Induction: Suppose that G has k edges, $k \geq 1$, and that all connected planar graphs with less than k edges satisfy 9.6a. Select any edge that is part of the boundary of the infinite region and call it e_1. Let G' be the graph obtained from G by deleting e_1. Figure 9.6.4 illustrates the two different possibilities we need to consider: either G' is connected or it has two connected components, G_1 and G_2.

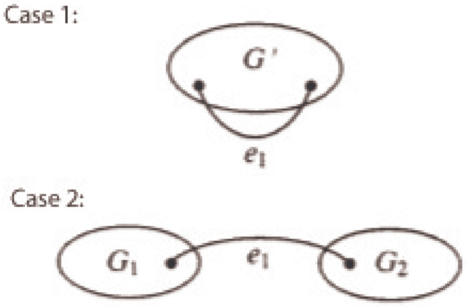


Figure 9.6.4
Two case in the proof of Euler's Formula

If G' is connected, the induction hypothesis can be applied to it. If G' has v' vertices, r' edges and e' edges, then $v' + r' - e' = 2$ and in terms of the corresponding numbers for G,

$v' = v$	No vertices were removed to form G'
$r' = r - 1$	One region of G merged with the infinite region when e_1 is removed
$e' = k - 1$	We assumed that G had k edges.

For the case where G' is connected,

$$\begin{aligned} v + r - e &= v + r - k \\ &= v' + (r' + 1) - (e' + 1) \\ &= v' + r' - e' \\ &= 2 \end{aligned}$$

If G' is not connected, it must consist of two connected components, G_1 and G_2 since we started with a connected graph, G. We can apply the induction hypothesis to each of the two components to complete the proof. We leave it to the students to do this, with the reminder that in counting regions, G_1 and G_2 will share the same infinite region. ■

Theorem 9.6.2. *If* $G = (V, E)$ *is a connected planar graph with v vertices,* $v \geq 3$, *and e edges, then*

$$e \leq 3v - 6. \qquad (9.6b)$$

Remark: One implication of 9.6b is that the number of edges in a connected planar graph will never be larger than three times its number.of vertices (as long as it has at least three vertices). Since the maximum number of edges in a graph with v vertices is a quadratic function of v, as v increases, planar graphs are more and more sparse.

Outline of a Proof of Theorem 9.6.2.

(a) Let r be the number of regions in G. For each region, count the number of edges that comprise its border. The sum of these counts must be at least $3r$. Recall that we are working with simple graphs here, so a region made by two edges connecting the same two vertices is not possible.

(b) Based on (a), infer that the number of edges in G must be at least $\frac{3r}{2}$.

(c) $e \geq \frac{3r}{2} \Rightarrow r \leq \frac{2e}{3}$

(d) Substitute $\frac{2e}{3}$ for r in Euler's Formula to obtain an inequality that is equivalent to 9.6.b. ■

The following theorem will be useful as we turn to graph coloring.

Theorem 9.6.3. *If G is a connected planar graph, then it has a vertex with degree 5 or less.*

Proof (by contradiction): We can assume that G has at least seven vertices, for otherwise the degree of any vertex is at most 5. Suppose that G is a connected planar graph and each vertex has a degree of 6 or more. Then, since each edge contributes to the degree of two vertices, $e \geq \frac{6v}{2} = 3v$. However, Theorem 9.6.2 states that the $e \leq 3v - 6 < 3v$, which is a contradiction. ■

GRAPH COLORING

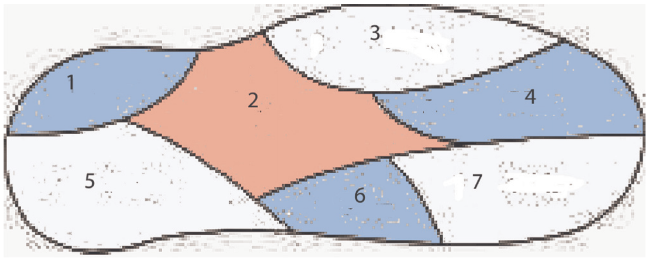


Figure 9.6.5
A 3-coloring of Euler Island

The map of Euler Island in Figure 9.6.5 shows that there are seven towns on the island. Suppose that a cartographer must produce a colored map in which no two towns that share a boundary have the same color. To keep costs down, she wants to minimize the number of different colors that appear on the map. How many colors are sufficient? For Euler Island, the answer is three. This problem motivates a more general problem.

The Graph Coloring Problem. Given an undirected graph $G = (V, E)$, find a "coloring function" f from V into a set of colors H such that $(v_i, v_j) \in E \Rightarrow f(v_i) \neq f(v_j)$ and H has the smallest possible cardinality. The cardinality of H is called the *chromatic number of* G, $\chi(G)$.

Notes:

(a) A coloring function onto an n element set is called an n-coloring.

(b) In terms of this general problem, the chromatic number of the graph of Euler Island is three. To see that no more than three colors are needed, we need only display a 3-coloring: $f(1) = f(4) = f(6) =$ blue, $f(2) =$ red, and $f(3) = f(5) = f(7) =$ white. This coloring is not unique. The next smallest set of colors would be of two colors, and you should be able to convince yourself that no 2-coloring exists for this graph.

In the mid-nineteenth century, it became clear that the typical planar graph had a chromatic number of no more than 4. At that point, mathematicians attacked the Four-Color Conjecture, which is that if G is any planar graph, then its chromatic number is no more than 4. Although the conjecture is quite easy to state, it took over 100 years, until 1976, to prove the conjecture in the affirmative.

Theorem 9.6.4: The Four-Color Theorem. *If G is a planar graph, then $\chi(G) \leq 4$.*

A proof of the Four-Color Theorem is beyond the scope of this text, but we can prove a theorem that is only 25 percent inferior.

Theorem 9.6.5: The Five-Color Theorem. *If G is a planar graph, then $\chi(G) \leq 5$.*

The number 5 is not a sharp upper bound for $\chi(G)$ because of the Four-Color Theorem.

Proof, by Induction on the Number of Vertices in the Graph:

Basis: Clearly, a graph with one vertex has a chromatic number of 1.

Induction: Assume that all planar graphs with $n - 1$ vertices have a chromatic number of 5 or less. Let G be a planar graph. By Theorem 9.6.2, there exists a vertex v with $\deg v \leq 5$. Let $G - v$ be the planar graph obtained by deleting v and all edges that connect v to other vertices in G. By the induction hypothesis, $G - v$ has a 5-coloring. Assume that the colors used are red, white, blue, green, and yellow.

If $\deg v < 5$, then we can produce a 5-coloring of G by selecting a color that is not used in coloring the vertices that are connected to v with an edge in G.

If $\deg v = 5$, then we can use the same approach if the five vertices that are adjacent to v are not all colored differently. We are now left with the possibility that v_1, v_2, v_3, v_4, and v_5 are all connected to v by an edge and they are all colored differently. Assume that they are colored red, white blue, yellow, and green, respectively, as in Figure 9.6.6.

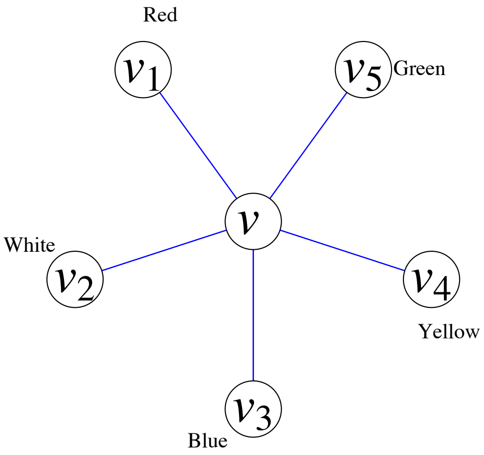


Figure 9.6.6

Starting at v_1 in $G-v$, suppose we try to construct a path v_3 that passes through only red and blue vertices. This can either be accomplished or it can't be accomplished. If it can't be done, consider all paths that start at v_1, and go through only red and blue vertices. If we exchange the colors of the vertices in these paths, including v_1 we still have a 5-coloring of $G - v$. Since v_1 is now blue, we can color the central vertex, v, red.

Finally, suppose that v_1 is connected to v_3 using only red and blue vertices. Then a path from v_1 to v_3 by using red and blue vertices followed by the edges (v_3, v) and (v, v_1) completes a circuit that either encloses v_2 or encloses v_4 and v_5 . Therefore, no path from v_2 to v_4 exists using only white and yellow vertices. We can then repeat the same process as in the previous paragraph with v_2 and v_4 , which will allow us to color v white. ■

Definition: Bipartite Graph. *A bipartite graph is a graph that has a 2-coloring. Equivalently, a graph is bipartite if its vertices can be partitioned into two nonempty subsets so that no edge connects a vertices from the same from each subset.*

Example 9.6.3.

(a) The graph of the Three Utilities Puzzle is bipartite. The vertices are partitioned into the utilities and the homes. Of course a 2-coloring of the graph is to color the utilities red and the homes blue.

(b) For $n \geq 1$, the n-cube is bipartite. A coloring would be to color all strings with an even number of 1's red and the strings with an odd number of 1's blue. By the definition of the n-cube, two strings that have the same color couldn't be connected since they would need to differ in at least two positions.

(c) Let V be a set of 64 vertices, one for each square on a chess board. We can index the elements of V by

$v_{i\,j}$ = the square on the row i, column j.

Connect vertices in V according to whether or not you can move a knight from one square to another. Using our indexing of V,

$$\left(v_{i\,j},\ v_{k\,l}\right) \in E \text{ if and only if } \begin{array}{c} |\,i-k\,|+|\,j-l\,| = 3 \\ \text{and } |\,i-k\,|\cdot|\,j-l\,| = 2 \end{array}$$

$(V,\ E)$ is a bipartite graph. The usual coloring of a chessboard is valid 2-coloring.

How can you recognize whether a graph is bipartite? Unlike planarity, there is a nice equivalent condition for a graph to be bipartite.

Theorem 9.6.6. An undirected graph is bipartite if and only if it has no circuit of odd length.

Proof. (⇒) Let $G = (V,\ E)$ be a bipartite graph that is partitioned into two sets, *R(ed)* and *B(lue)* that define a 2-coloring. Consider any circuit in V. If we specify a direction in the circuit and define f on the vertices of the circuit by

$$f\,(u) = \text{the next vertex in the circuit after } v.$$

Note that *f* is a bijection. Hence the number of red vertices in the circuit equals the number of blue vertices, and so the length of the circuit must be even.

($\Longleftarrow$) Assume that G has no circuit of odd length. For each component of G, select any vertex w and color it red. Then for every other vertex v in the component, find the path of shortest distance from w to v. If the length of the path is odd, color v blue, and if it is even, color v red. We claim that this method defines a 2-coloring of G. Suppose that it does not define a 2-coloring. Then let v_a and v_b be two vertices with identical colors that are connected with an edge. By the way that we colored G, neither v_a nor v_b could equal w. We can now construct a circuit with an odd length in G. First, we start at w and follow the shortest path to v_a . Then follow the edge (v_a, v_b), and finally, follow the reverse of a shortest path from w to v_b. Since v_a and v_b have the same color, the first and third segments of this circuit have lengths that are both odd or even, and the sum of their lengths must be even. The addition of the single edge (v_a, v_b) shows us that this circuit has an odd length. This contradicts our premise. ■

Note: An efficient algorithm for finding a 2-coloring of a graph can be designed using the method that is used in the second part of the proof above.

EXERCISES FOR SECTION 9.6

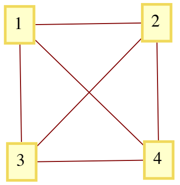
A Exercises

1. Apply Theorem 9.6.2 to prove that once n gets to a certain size, a K_n is nonplanar. What is the largest complete planar graph?

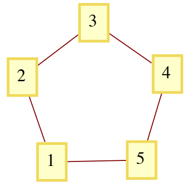
2. Can you apply Theorem 9.6.2 to prove that the Three Utilities Puzzle can't be solved?

3. What are the chromatic numbers of the following graphs?

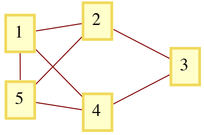
(a)



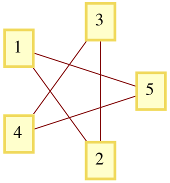
(b)



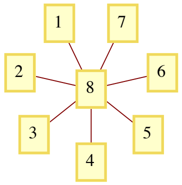
(c)



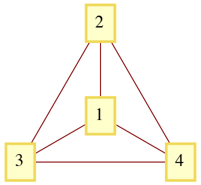
(d)



(e)



(f)



4. Prove that if an undirected graph has a subgraph that is a K_3 it then its chromatic number is at least 3.

5. What is $\chi(K_n)$, $n \geq 1$?

6. What is the chromatic number of the United States?

B Exercises

7. Complete the proof of Theorem 9.6.1.

8. Use the outline of a proof of Theorem 9.6.2 to write a complete proof. Be sure to point out where the premise $v \geq 3$ is essential.

9. Let $G = (V, E)$ with $\lvert V \rvert \geq 11$, and let U be the set of all undirected edges between distinct vertices in V. Prove that either G or $G' = (V, E^c)$ is nonplanar.

10. Design an algorithm to determine whether a graph is bipartite.

11. Prove that a bipartite graph with an odd number of vertices greater than or equal to 3 has no Hamiltonian circuit.

C Exercises

12. Prove that any graph with a finite number of vertices can be drawn in three dimensions so that no edges intersect.

13. Suppose you had to color the edges of an undirected graph so that for each vertex, the edges that it is connected to have different colors. How can this problem be transformed into a vertex coloring problem?

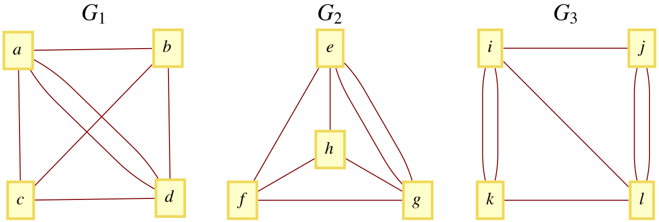
14. (a) Suppose the edges of a K_6 are colored either red or blue. Prove that there will be either a "red K_3" (a subset of the vertex set with three vertices connected by red edges) or a "blue K_3."

(b) Suppose six people are selected at random. Prove that either there exists a subset of three of them with the property that any two people in the subset can communicate in a common language, or there exist three people, no two of whom can communicate in a common language.

SUPPLEMENTARY EXERCISES FOR CHAPTER 9

Section 9.1

1. Determine which two of the graphs below are isomorphic and give an explicit isomorphism between those two graphs.



2. Teams 1, 2, 3, and 4 compete in a round-robin tournament. Draw a round-robin tournament graph that represents one of the possible out comes of the tournament. In terms of your graph, what was the outcome of the tournament (in wins and losses)?

3. Let $G = (V, E)$ be an undirected graph. An *independent set*, W, is a subset of V having the property that no two vertices in W are connected by an edge in E. That is,

$$v, w \in W \Rightarrow \{v, w\} \notin E.$$

Finding a maximal independent set (an independent set that is as large as possible) is often of interest.

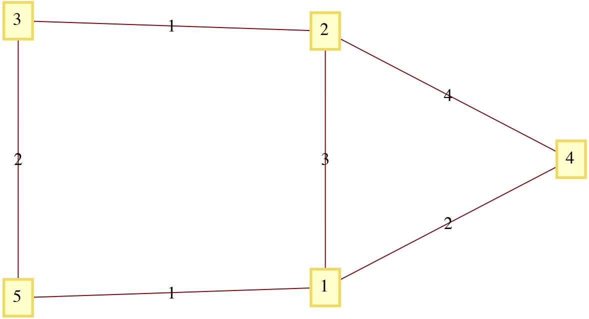
(a) Find a maximal independent set in the graph of Figure 9.1.2.

(b) Prove that if W is a maximal independent set in G, then every vertex in G is connected by an edge to at least one vertex in W.

(c) How large can a maximal independent set in a K_n be?

4. Let $S = \{1, 2, \ldots, n\}$ be a set of n cities. Define a matrix $A = \left[a_{ij}\right]$ of order $n \times n$ by $a_{ij} = 0$ if $i = j$; otherwise a_{ij} is the *number* of distinct ways of traveling directly from city i to city j by car, without visiting any other cities belonging to S en route.

In the following diagram, the points represent five cities, 1, 2, 3, 4, and 5, and a line is drawn between two cities and labeled with a positive integer giving the number of *direct* routes (by car) between the respective cities.

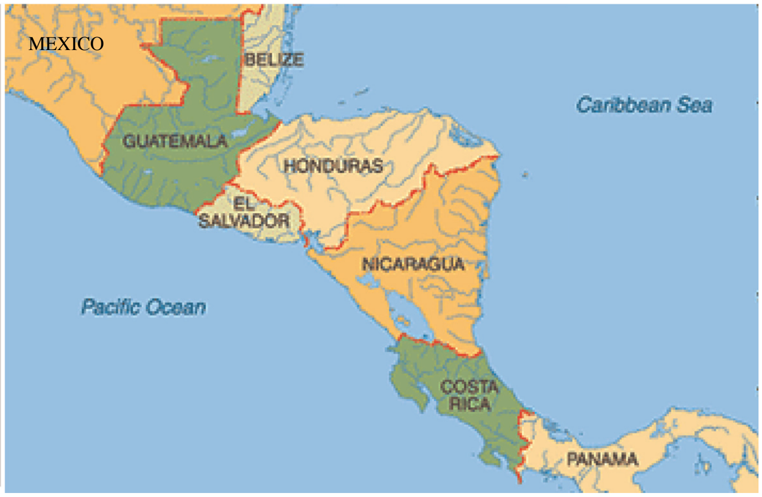


(a) Determine the 5×5 matrix A going with the above diagram.

(b) Calculate A^2.

(c) Interpret the meaning of the entries in A^2, both for the result in part b, and for the general set $S = \{1, 2, \ldots, n\}$.

5. An undirected graph can be used to model a map of states or countries, where there is a vertex for each country and an edge between two vertices if the two countries share a boundary. For example, the undirected graph of Central America (mainland only) would have eight vertices. {Honduras, Nicaragua} would be an edge of the graph, but {Mexico, Nicaragua} would not be an edge.



(a) Draw the graph of Central America.

(b) Find a path from Mexico to Panama.

(c) What significance would this path have if you intended to drive from Mexico to Panama?

6. Show that the graph of the states of Washington, Oregon, Idaho, Montana, Wyoming, and Colorado is isomorphic to the graph of New England.

7. The outdegree of a vertex in a directed graph is the number of vertices in the graph that start at that vertex, and the indegree of the vertex is the number of vertices in the graph that terminate at that vertex. A vertex v in a tournament graph is a source if the indegree of that vertex is zero. A sink is a vertex in a tournament graph that has outdegree of zero.

(a) Prove that a round-robin tournament graph can have at most one source and at most one sink. Interpret these facts in terms of the results of the tournament.

(b) What is the outdegree of a source in a round-robin tournament graph? What is the indegree of a sink in a round-robin tournament graph?

(c) Let $G = (V, E)$ be a round-robin tournament graph with $|V| > 2$. If p is "G has a sink," and q is "G has a source," prove that any one of the propositions $\neg p \wedge \neg q$, $\neg p \wedge q$, $p \wedge \neg q$ and $p \wedge q$ could be true.

Section 9.2

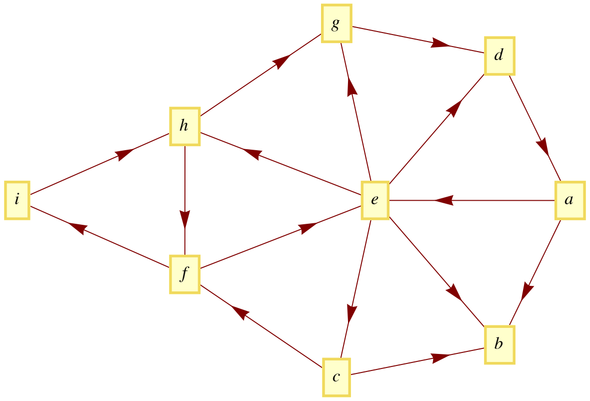
8. Let $G = (V, E)$ be a round-robin tournament graph with $|V| = n$. If M is the matrix of G,

(a) For $i = 1, 2, \ldots, n$, explain why the number of 1's in column i of M plus the number of 1s in row i is always equal to $n - 1$.

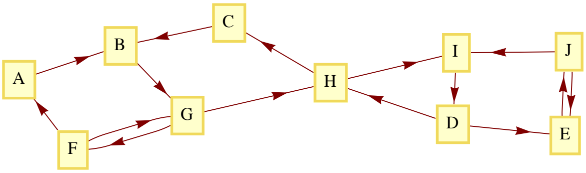
(b) How many 1s are there in M?

Section 9.3

9. Use the broadcasting algorithm to determine a shortest path from vertex a to vertex i in the following graph. List the depth sets.



10. In a breadth-first (broadcasting) search for a path from vertex A to vertex J, what would the depth sets $(D_1, D_2, \ldots)$ be?



Section 9.4

Definition: Randomly Eulerian. *Graph G is randomly Eulerian from vertex v if every path in G that initiates at v and uses edges at random is a Eulerian circuit*.

11. Give examples of undirected graphs that are randomly Eulerian from none, one, two, or all vertices. It can be proven that no graph is randomly Eulerian from more than two vertices unless it is randomly Eulerian from all vertices.

12. Prove that G is randomly Eulerian from v if and only if every circuit in G contains v.

13. Ore's Theorem states that if $G = (V, E)$ is an undirected graph with $|V| = n \geqslant 3$ such that $\{v, w\} \notin E \Rightarrow deg\, u + deg\, v \geqslant n$, then G has a Hamiltonian circuit. Prove Ore's Theorem given the following out line.

Proof by contradiction:

(a) Add edges to E so that G still has no Hamiltonian circuit, but so that the addition of any other edge does produce a Hamiltonian circuit. Now select any $\{v, w\} \notin E$. There must be a path in G:

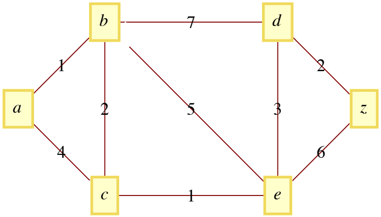
$v = (v_1, v_2, \ldots, v_n) = w$.

(b) Prove that for $2 \leqslant i \leqslant n$, $\{v_1, v_i\} \in E \Rightarrow \{v_{i-1}, v_n\} \notin E$.

(c) Conclude that $deg\, v + deg\, w < n$.

Section 9.5

14. Given:

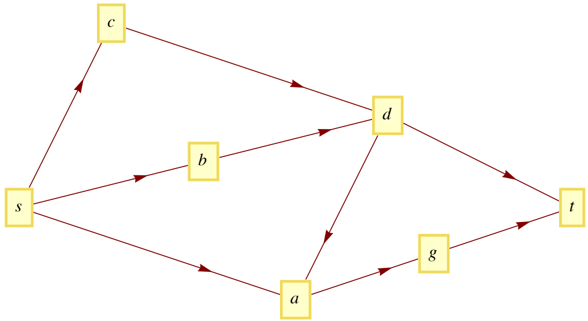


(a) Determine the optimal path from the vertex a to the vertex z.

(b) Use the broadcasting algorithm to find a path from a to z.

(c) Find the "costs" of both paths and discuss whether the algorithm in part b gives a "good result."

15. Consider the network



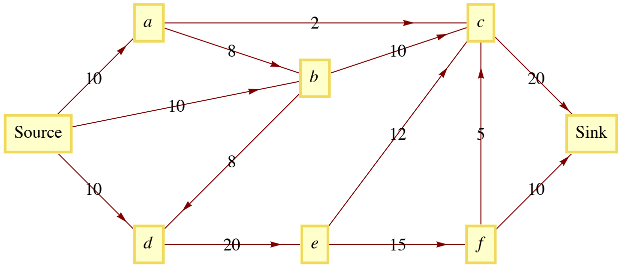
We start with a flow *f* on this network partially defined by $f(s, c) = f(s, b) = f(s, a) = 1$ and $f(d, a) = 0$.

(a) Define *f* for each of the other edges in this network so as to achieve a flow.

(b) Assume that the maximum capacity of each edge is 2. Determine a flow augmenting path with respect to the flow given in part a. (Use the Ford and Fulkerson Algorithm.)

(c) Is the flow obtained in part b a maximal flow? Explain.

16. Find a maximal flow for the following network:



17. (a) Given the mileage chart below, what is the closest neighbor circuit starting at city *A*?

	A	*B*	*C*	*D*	*E*	*F*
A	_	34	50	12	51	37
B	34	_	40	27	70	60
C	50	40	_	30	33	41
D	12	27	30	_	39	20
E	51	70	33	39	_	15
F	37	60	41	20	15	_

(b) Suppose it takes $(k - 1)$ seconds to determine which of *k* cities is closest to any given city. Estimate how long it would take to find a closest neighbor circuit through *n* cities.

Section 9.6

18. Draw three connected graphs, G_2, G_3, and G_4, with four vertices, each having chromatic numbers 2, 3, and 4 (i.e. $c(G_i) = i$.

19. (a) Prove that although a K_5 is not planar, it can be drawn on a *torus* (a doughnut-shaped surface).

(b) Can the Three Utilities Puzzle be solved on a torus?

20. Draw examples of the following graphs, if possible. Clearly indicate which of the graphs are impossible and why they are impossible. You may cite any theorem that justifies your claim.

(a) An undirected Hamiltonian graph that is not Eulerian. Explain why your graph is not Eulerian.

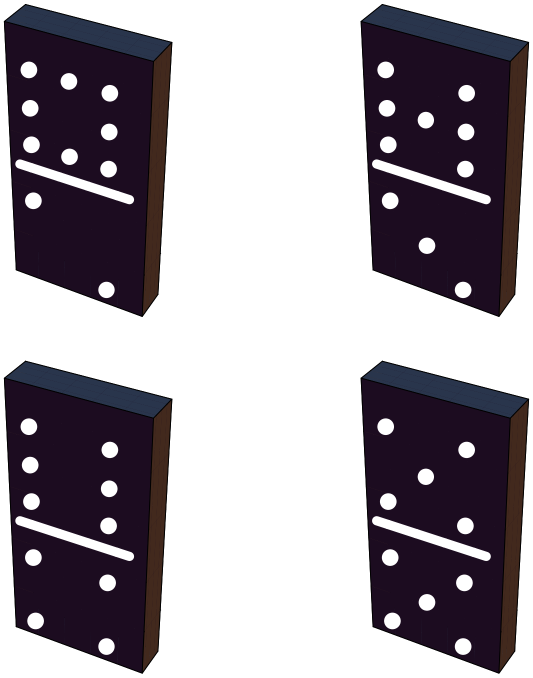
(b) A bipartite Hamiltonian graph with five vertices.

(c) A round-robin tournament graph with four vertices.

(d) A connected planar graph with four vertices, three regions, and six edges.

(e) An undirected graph with chromatic number five.

chapter 10



TREES

GOALS

In this chapter we will study the class of graphs called trees. Trees are frequently used in both mathematics and the sciences. Our solution of Example 2.1 is one simple instance. Since they are often used to illustrate or prove other concepts, a poor background in trees can be a serious handicap. For this reason, our ultimate goals are to: (1) define the various common types of trees, (2) identify some basic properties of trees, and (3) discuss some of the common applications of trees.

10.1 What Is a Tree?

What distinguishes trees from other types of graphs is the absence of certain paths called cycles. Recall that a *path* is a sequence of consecutive edges in a graph; and a *circuit* is a path that begins and ends at the same vertex.

Definition: Cycle. *A cycle is a circuit whose edge list contains no duplicates.*

The simplest example of a cycle in an undirected graph is a pair of vertices with two edges connecting them. Since trees are cycle-free, we can rule out all multigraphs from consideration as trees.

Trees can either be undirected or directed graphs. We will concentrate on the undirected variety in this chapter.

Definition: Tree. *An undirected graph is a tree if it is connected and contains no cycles or self-loops.*

Example 10.1.1.

(a) Graphs i, ii and iii in Figure 10.1.1 are all trees, while graphs iv, v, and vi are not trees.

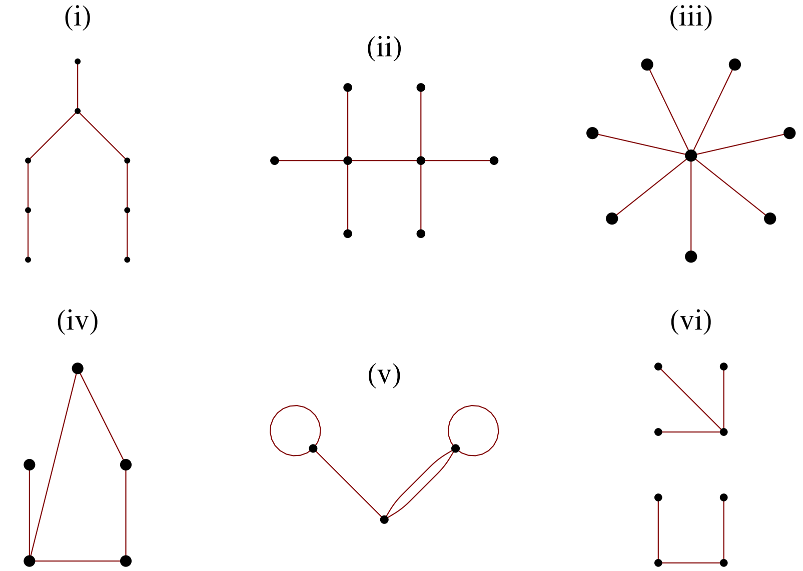


Figure 10.1.1
Some trees and non-trees

(b) A K_2 is a tree. However, if $n \geq 3$, a K_n is not a tree.

(c) In a loose sense, a botanical tree is a mathematical tree. There are usually no cycles in the branch structure of a botanical tree.

(d) The structures of some chemical compounds are modeled by a tree. For example, butane (Figure 10.1.2a) consists of four carbon molecules and ten hydrogen molecules, where an edge between two molecules represents a bond between them. A bond is a force that keeps two molecules together. The same set of molecules can be linked together in a different tree structure to give us the compound isobutane (Figure 10.1.2b). There are some compounds whose graphs are not trees. One example is benzene (Figure 10.1.2c).

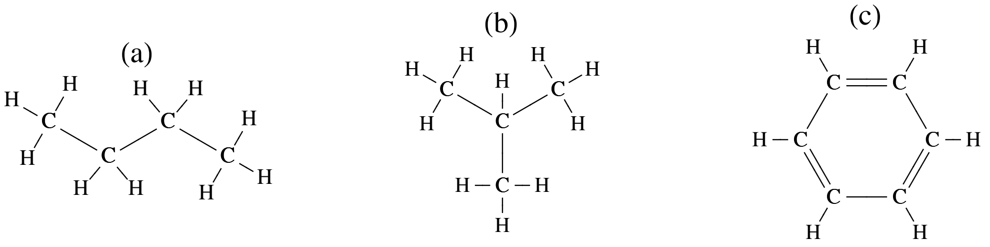


Figure 10.1.2
Simple organic compounds

One type of graph that is not a tree, but is closely related, is a forest.

Definition: Forest. *A forest is an undirected graph whose components are all trees.*

Example 10.1.2. The top half of Figure 10.1.1 can be viewed as a forest of three trees.

We will now examine several conditions that are equivalent to the one that defines a tree. The following theorem will be used as a tool in proving that the conditions are equivalent.

Theorem 10.1.1. *Let $G = (V, E)$ be an undirected graph with no self-loops, and let $v_a, v_b \in V$. If two different simple paths exist between v_a and v_b, then there exists a cycle in G.*

Proof: Let $p_1 = (e_1, e_2, \ldots, e_m)$ and $p_2 = (f_1, f_2, \ldots, f_n)$ be two different simple paths from v_a to v_b. The first step we will take is to delete from p_1 and p_2 the initial edges that are identical. That is, if $e_1 = f_1, e_2 = f_2, \ldots, e_j = f_j$, and $e_{j+1} \neq f_{j+1}$ delete the first j edges of both paths. Once this is done, both paths start at the same vertex, call it v_c, and both still end at v_b. Now we construct a cycle by starting at v_c and following what is left of p_1 until we first meet what is left of p_2. If this first meeting occurs at vertex v_d, then the remainder of the cycle is completed by following the portion of the reverse of p_2 that starts at v_d and ends at v_c. ■

Theorem 10.1.2. Let $G = (V, E)$ be an undirected graph with no self-loops and $|V| = n$. The following are all equivalent:

(1) G is a tree.

(2) For each pair of distinct vertices in V, there exists a unique simple path between them.

(3) G is connected, and if $e \in E$, then $(V, E - \{e\})$ is disconnected.

(4) G contains no cycles, but by adding one edge, you create a cycle.

(5) G is connected and $|E| = n - 1$.

Proof Strategy. Most of this theorem can be proven by proving the following chain of implications: (1) ⇒ (2), (2) ⇒ (3), (3) ⇒ (4), and (4) ⇒ (1). Once these implications have been demonstrated, the transitive closure of ⇒ on $\{1, 2, 3, 4\}$ establishes the equivalence of the first four conditions. The proof that Statement 5 is equivalent to the first four can be done by induction, which we will leave to the reader.

Proof: (1) ⇒ (2) (Indirect). Assume that G is a tree and that there exists a pair of vertices between which there is either no path or there are at least two distinct paths. Both of these possibilities contradict the premise that G is a tree. If no path exists, G is disconnected, and if two paths exist, a cycle can be obtained by Theorem 10.1.1.

(2) ⇒ (3). We now use Statement 2 as a premise. Since each pair of vertices in V are connected by exactly one path, G is connected. Now if we select any edge e in E, it connects two vertices, v_1 and v_2. By (2), there is no simple path connecting v_1 to v_2 other than e. Therefore, no path at all can exist between v_1 and v_2 in $(V, E - \{e\})$. Hence $(V, E - \{e\})$ is disconnected.

(3) ⇒ (4). Now we will assume that Statement 3 is true. We must show that G has no cycles and that adding an edge to G creates a cycle. We will use an indirect proof for this part. Since (4) is a conjunction, by DeMorgan's Law its negation is a disjunction and we must consider two cases. First, suppose that G has a cycle. Then the deletion of any edge in the cycle keeps the graph connected, which contradicts (3). The second case is that the addition of an edge to G does not create a cycle. Then there are two distinct paths between the vertices that the new edge connects. By Theorem 10.1.1, a cycle can then be created, which is a contradiction.

(4) ⇒ (1) Assume that G contains no cycles and that the addition of an edge creates a cycle. All that we need to prove to verify that G is a tree is that G is connected. If it is not connected, then select any two vertices that are not connected. If we add an edge to connect them, the fact that a cycle is created implies that a second path between the two vertices can be found which is in the original graph, which is a contradiction. ■

The usual definition of a directed tree is based on whether the associated undirected graph, which is obtained by "erasing" its directional arrows, is a tree. In Section 10.3 we will introduce the rooted tree, which is a special type of directed tree.

EXERCISES FOR SECTION 10.1

A Exercises

1. Given the following vertex sets, draw all possible undirected trees that connect them.

(a) $V_a = \{\text{right}, \text{left}\}$

(b) $V_b = \{+, -, 0\}$

(c) $V_c = \{\text{north}, \text{south}, \text{east}, \text{west}\}$.

2. Are all trees planar? If they are, can you explain why? If they are not, you should be able to find a nonplanar tree.

3. Prove that if G is a simple undirected graph with no self-loops, then G is a tree if and only if G is connected and $|E| = |V| - 1$.

4. (a) Prove that if $G = (V, E)$ is a tree and $e \in E$, then $(V, E - \{e\})$ is a forest of two trees.

(b) Prove that if(V_1, E_1) and (V_2, E_2) are disjoint trees and e is an edge that connects a vertex in V_1 to a vertex in V_2, then $(V_1 \cup V_2, E_1 \cup E_2 \cup \{e\})$ is a tree.

5. (a) Prove that any tree with at least two vertices has at least two vertices of degree 1.

(b) Prove that if a tree is not a chain, then it has at least three vertices of degree 1.

10.2. Spanning Trees

The topic of spanning trees is motivated by a graph-optimization problem.

Example 10.2.1. A map of Atlantis (Figure 10.2.1) shows that there are four campuses in its university system. A new secure communications system is being installed and the objective is to allow for communication between any two campuses, to achieve this objective, the university must buy direct lines between certain pairs of campuses. Let G be the graph with a vertex for each campus and an edge for each direct line. Total communication is equivalent to G being a connected graph. This is due to the fact that two campuses can communicate over any number of lines. To minimize costs, the university wants to buy a minimum number of lines.

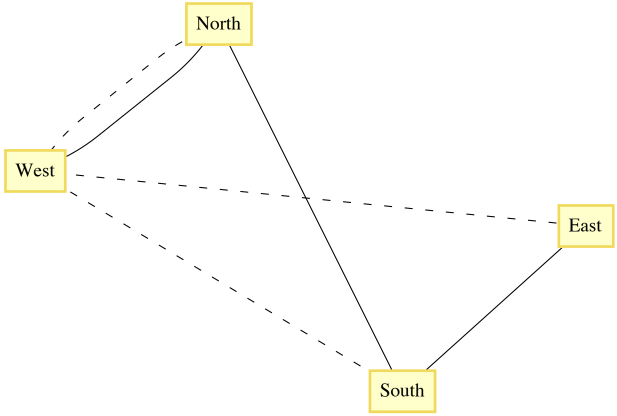


Figure 10.2.1
The Atlantis University System

The solutions to this problem are all trees. Any graph that satisfies the requirements of the university must be connected, and if a cycle does exist, any line in the cycle can be deleted, reducing the cost. Each of the sixteen trees that can be drawn to connect the vertices North, South, East, and West (see Exercise lc of Section 10.1) solves the problem as it is stated. Note that in each case, three direct lines must be purchased. There are two considerations that can help reduce the number of solutions that would be considered.

Objective 1: Given that the cost of each line depends on certain factors, such as the distance between the campuses, select a tree whose cost is as low as possible.

Objective 2: Suppose that communication over multiple lines is noisier as the number of lines increases. Select a tree with the property that the maximum number of lines that any pair of campuses must use to communicate with is as small as possible.

Typically, these objectives are not compatible; that is, you cannot always simultaneously achieve these objectives. In the case of the Atlantis university system, the solution with respect to Objective 1 is indicated with solid lines in Figure 10.2.1. There are four solutions to the problem with respect to Objective 2: any tree in which one campus is directly connected to the other three. One solution with respect to Objective 2 is indicated with dotted lines in Figure 10.2.1. After satisfying the conditions of Objective 2, it would seem reasonable to select the cheapest of the four trees.

Definition: Spanning Set, Spanning Tree.

(a) *Let $G = (V, E)$ be a connected undirected graph. A spanning set for G is a subset E' of E such that (V, E') is connected.*
(b) *If E' is a spanning set for G and $T = (V, E')$ is a tree, then T is called a spanning tree for G.*

Notes

(a) If (V, E') is a spanning tree, $|E'| = |V| - 1$.

(b) The significance of a spanning tree is that it is a minimal spanning set. A smaller set would not span the graph, while a larger set would have a cycle, which has an edge that is superfluous.

For the remainder of this section, we will discuss two of the many topics that relate to spanning trees. The first is the Minimal Spanning Tree Problem, which addresses Objective 1 above. The second is the Minimum Diameter Spanning Tree Problem, which addresses Objective 2.

THE MINIMAL SPANNING TREE PROBLEM

Given a weighted connected undirected graph $G = (V, E, w)$, the *minimal spanning tree problem* is to find a spanning tree (V, E') for which $\sum_{e\in E'} w(e)$ is as small as possible.

Unlike many of the graph-optimization problems that we've examined, a solution to this problem can be obtained efficiently. It is a situation in which a greedy algorithm works.

Definition: Bridge. *Let $G = (V, E)$ be an undirected graph and let $\{L, R\}$ be a partition of V. A bridge between L and R is an edge in E that connects a vertex in L to a vertex in R.*

Theorem 10.2.1. *Let $G = (V, E, w)$ be a weighted connected undirected graph. Let V be partitioned into two sets L and R. If e^* is a bridge of least weight between L and R, then there exists a minimal spanning tree for G that includes e^*.*

Proof (Indirect proof): Suppose that no minimum spanning tree including e^* exists. Let $T = (V, E')$ be a minimum spanning tree. If we add e^* to T, a cycle is created, and this cycle must contain another bridge, e, between L and R. Since $w(e^*) \leq w(e)$, we can delete e and the new tree, which includes e^* must also be a minimum spanning tree. ■

Example 10.2.2. The bridges between the vertex sets $\{a, b, c\}$ and $\{d, e\}$ in Figure 10.2.2 are the edges $\{b, d\}$ and $\{c, e\}$. According to the theorem, a minimal spanning tree that includes $\{b, d\}$ exists. By examination, you should be able to see that this is true. Is it true that only the bridges of minimal weight can be part of a minimal spanning tree? The answer is no.

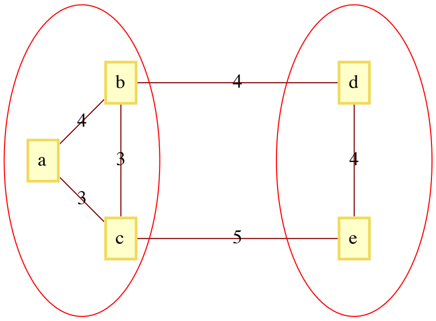


Figure 10.2.2

Theorem 10.2.1 essentially tells us that a minimal spanning tree can be constructed recursively by continually adding minimally weighted bridges to a set of edges.

Algorithm 10.2.1: Prim's Algorithm for Finding a Minimal Spanning Tree. *Let $G = (V, E, w)$ be a connected, weighted, undirected graph, and let v_0 be an arbitrary vertex in V. The following steps lead to a minimal spanning tree for G. L and R will be sets of vertices and E' is a set of edges.*

```
(1) (Initialize) $L = V - \{v_0\}$;   $R = \{v_0\}$; $E' = \emptyset$.
(2) (Build the tree) While $L \neq \emptyset$
        (2.1) Find $e^* = \{v_L, v_R\}$, a bridge of minimum weight between L and R.
        (2.2) $R = R \cup \{v_L\}$; $L = L - \{v_L\}$ ; $E' := E' \cup \{e^*\}$
(3) Terminate with a minimal spanning tree $(V, E')$.
```

Notes:

(a) If more than one minimal spanning tree exists, then the one that is obtained depends on v_0 and the means by which e^* is selected in Step 2.1 if two minimally weighted bridges exist.

(b) Warning: If two minimally weighted bridges exist between L and R, do not try to speed up the algorithm by adding both of them to E'.

(c) That Algorithm 10.2.1 yields a minimal spanning tree can be proven by induction with the use of Theorem 10.2.1.

(d) If it is not known whether G is connected, Algorithm 10.2.1 can be revised to handle this possibility. The key change (in Step 2.1) would be to determine whether any bridge at all exists between L and R. The condition of the while loop in Step 2 must also be changed somewhat.

Example 10.2.3. Consider the graph in Figure 10.2.3. If we apply Algorithm 10.2.1 starting at a, we obtain the following edge list in the order given: $\{a, f\}$, $\{f, e\}$, $\{e, c\}$, $\{c, d\}$, $\{f, b\}$, $\{b, g\}$. The total of the weights of these edges is 20. The method that we have used (in Step 2.1) to select a bridge when more than one minimally weighted bridge exists is to order all bridges alphabetically by the vertex in L and then, if further ties exist, by the vertex in R. The first vertex in that order is selected in Step 2.1 of the algorithm.

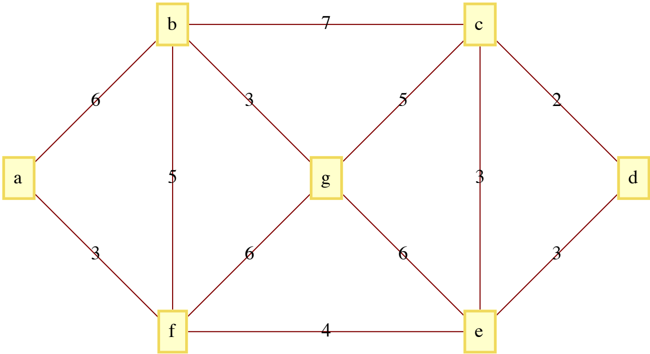
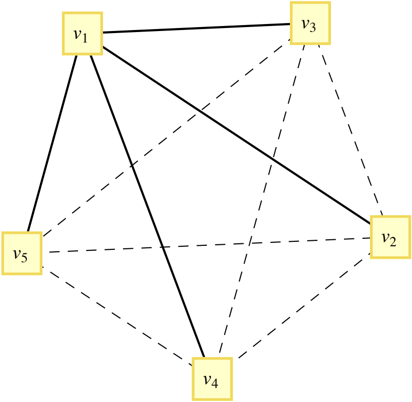


Figure 10.2.3

The Minimum Diameter Spanning Tree Problem

Given a connected undirected graph G = (V, E), find a spanning tree T = (V, E') of G such that the longest path in T is as short as possible.

Example 10.2.4. The Minimum Diameter Spanning Tree Problem is easy to solve in a K_n. Select any vertex v_0 and construct the spanning tree whose edge set is the set of edges that connect v_0 to the other vertices in the K_n . Figure 10.2.4 illustrates a solution for $n = 5$.



Minimum diameter spanning tree for K_5

For incomplete graphs, a two-stage algorithm is needed. In short, the first step is to locate a "center" of the graph. The maximum distance from a center to any other vertex is as small as possible. Once a center is located, a breadth-first search of the graph is used to construct the spanning tree. The breadth-first search is essentially the broadcasting algorithm that we discussed in Section 9.3 applied to undirected graphs.

EXERCISES FOR SECTION 10.2

A Exercises

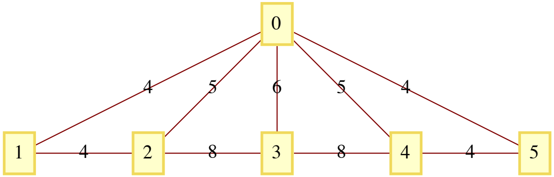
1. Suppose that after Atlantis University's phone system is in place, a fifth campus is established and that a transmission line can be bought to connect the new campus to any old campus. Is this larger system the most economical one possible with respect to Objective 1? Can you always satisfy Objective 2?

2. Construct a minimal spanning tree for the capital cities in New England (see Figure 9.5.1).

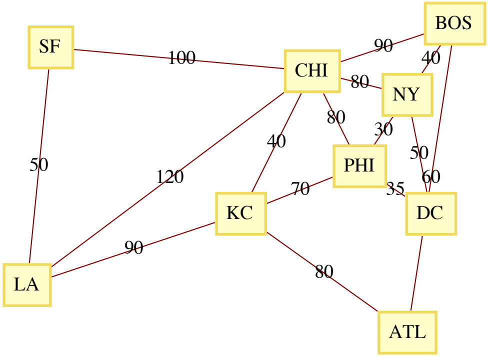
3. Show that the answer to the question posed in Example 10.2.2 is "no."

4. Find a minimal spanning tree for the following graphs.

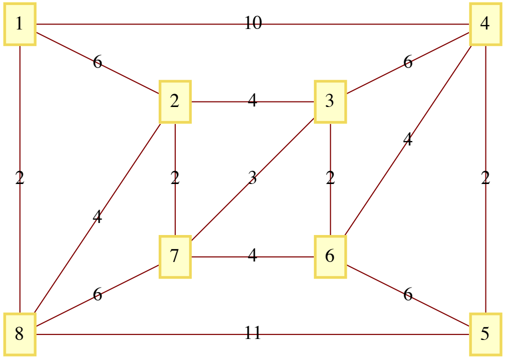
(a)


0
4
5
6
5
4
1
4
2
8
3
8
4
4
5

(b)

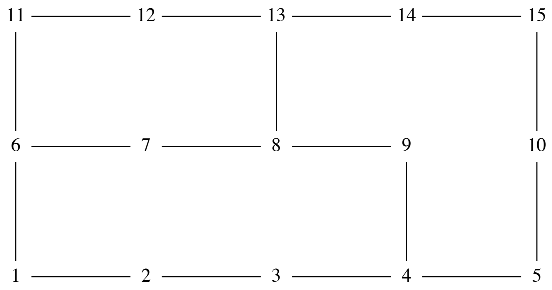

BOS
SF
100
CHI
90
40
80
NY
50
80
30
40
PHI
50
120
70
35
60
KC
DC
90
LA
80
ATL

(c)

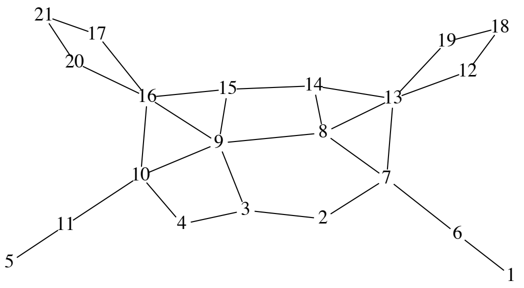

1
10
4
6
6
2
4
3
4
2
2
3
2
2
4
7
4
6
6
6
8
11
5

5. Find a minimum diameter spanning tree for the following graphs.

(a)



(b)



6. In each of the following parts back up your answer with either a proof or an counterexample.

(a) Suppose a weighted undirected graph had distinct edge weights. Is is possible that no minimal spanning tree includes the edge of minimal weight?

(b) Suppose a weighted undirected graph had distinct edge weights. Is is possible that every minimal spanning tree includes the edge of maximal weight?

10.3 Rooted Trees

In the next two sections, we will discuss rooted trees. Our primary focuses will be on general rooted trees and on a special case, ordered binary trees.

Informal Definition and Terminology: What differentiates rooted trees from undirected trees is that a rooted tree contains a distinguished vertex, called the root. Consider the tree in Figure 10.3.1. Vertex A has been designated the root of the tree. If we choose any other vertex in the tree, such as M, we know that there is a unique path from A to M. The vertices on this path, $(A,\ D,\ K,\ M)$, are described in genealogical terms:

M is a child of K (so is L).

K is M's parent.

A, D, and K are M's ancestors.

D, K, and M are descendants of A.

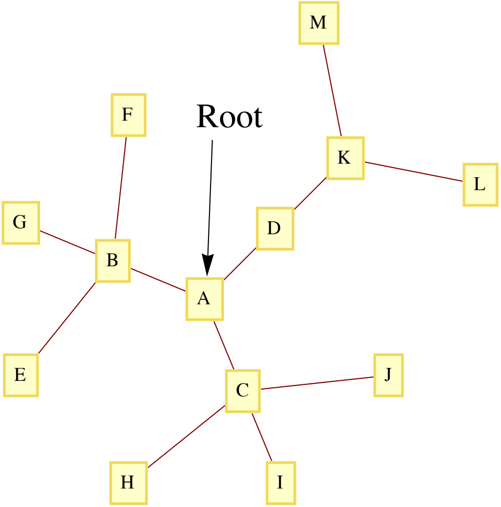


FIGURE 10.3.1
Rooted tree

These genealogical relationships are often easier to visualize if the tree is rewritten so that children are positioned below their parents, as in Figure 10.3.2.

With this format, it is easy to see that each vertex in the tree can be thought of as the root of a tree that contains, in addition to itself, all of its descendants. For example, D is the root of a tree that contains D, K, L, and M. Furthermore, K is the root of a tree that contains K, L, and M. Finally, L and M are roots of trees that contain only themselves. From this observation, we can give a formal definition of a rooted tree.

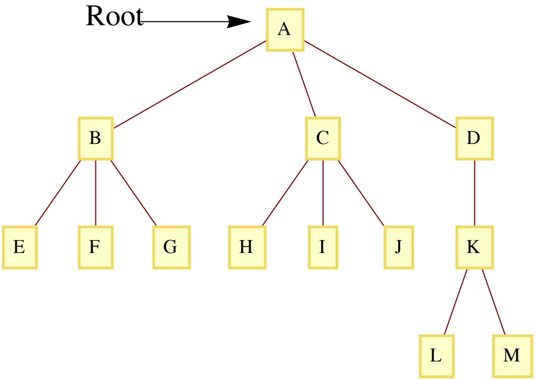


FIGURE 10.3.2
Rooted tree of Figure 10.3.1, redrawn

Definition: Rooted Tree.

(a) Basis:

(i) A tree with no vertices is a rooted tree (the empty tree),

(ii) A single vertex with no children is a rooted tree

(b) Recursion:
Let T_1, T_2, … , T_r, $r \geq 1$, be disjoint rooted trees with roots v_1, v_2, …, v_r, respectively, and let v_0 be a vertex that does not belong to any of these trees. Then a rooted tree, rooted at v_0, is obtained by making v_0 the parent of the vertices v_1, v_2, …, and v_r. We call T_1, T_2, … , T_r, subtrees of the larger tree.

The level of a vertex of a rooted tree is the number of edges that separate the vertex from the root. The level of the root is zero. The depth of a tree is the maximum level of the vertices in the tree. The depth of a tree in Figure 10.3.2 is three, which is the level of the vertices L and M. The vertices E, F, G, H, I, J, and K have level two. B, C, and D are at level one and A has level zero.

Example 10.3.1. Figure 2.1.1, which we reproduce below is a rooted tree with *Start* as the root. It is an example of what is called a decision tree.

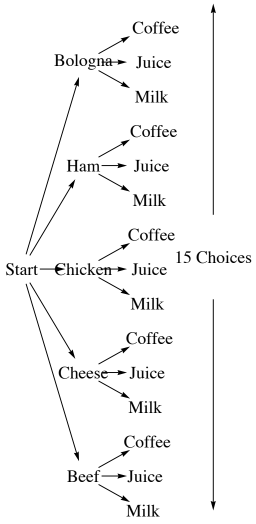


Figure 2.1.1

Example 10.3.2: Data Structures. One of the keys to working with large amounts of information is to organize it in a consistent, logical way. A *data structure* is a scheme for organizing data. A simple example of a data structure might be the information a college admissions department might keep on their applicants. Items in a *flat file* might look something like this:

ApplicantItem = {FirstName, MiddleInitial, LastName, StreetAddress, City, State, Zip, HomePhone, CellPhone, EmailAddress, HighSchool, Major, ApplicationPaid, MathSAT, VerbalSAT, Recommendation1, Recommendation2, Recommendation3}

A spreadsheet can be used to arrange data in this way. Although a flat file structure is often adequate, there are often advantages to clustering some the information. For example the applicant information is broken into four parts: name, contact information, high school, and application data.

ApplicantItem = {{FirstName, MiddleInitial, LastName}, {{StreetAddress, City, State, Zip}, {HomePhone, CellPhone}, EmailAddress}, HighSchool, {Major, ApplicationPaid, {MathSAT, VerbalSAT}, {Recommendation1, Recommendation2, Recommendation3}}}

The first item in the ApplicantItem list is a list {FirstName, MiddleInitial, LastName}, with each item in that list being a single field of the original flat file. The third item is simply the single high school item from the flat file. The application data is a list and one of its items, is itself a list with the recommendation data for each recommendation the applicant has.

The organization of this data can be visualized with a rooted tree such as the one in Figure 10.3.3.

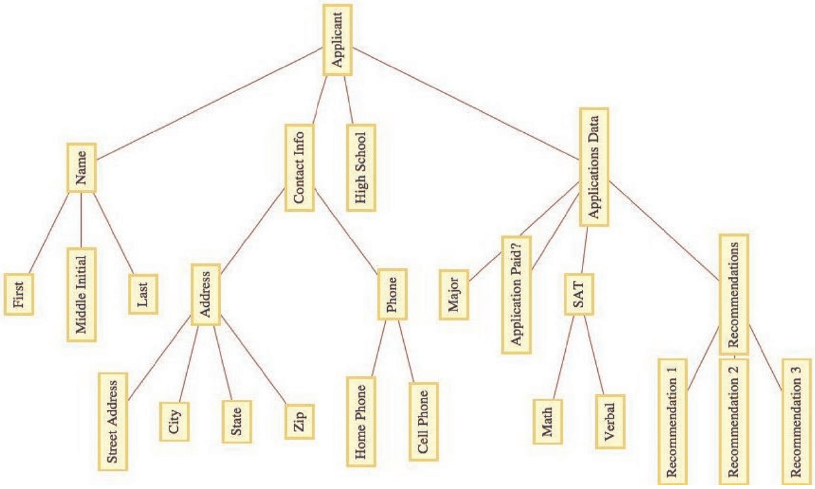


Figure 10.3.3
Structured Data

In general, you can represent a data item, T, as a rooted tree with T as the root and a subtree for each field. Those fields that are more than just one item are roots of further subtrees, while individual items have no further children in the tree.

KRUSKAL'S ALGORITHM

An alternate algorithm for constructing a minimal spanning tree uses a forest of rooted trees. First we will describe the algorithm in its simplest terms. Afterward, we will describe how rooted trees are used to implement the algorithm. Finally, we will describe a simple data structure and operations that make the algorithm quite easy to program. In all versions of this algorithm, assume that $G = (V, E, w)$ is a weighted undirected graph with $|V| = m$ and $|E| = n$.

Kruskal's Algorithm—Version 1.

(1) Sort the edges of G in ascending order according to weight. That is,

$$i \leq j \iff w(e_j) \leq w(e_j).$$

(2) Go down the list obtained in Step 1 and add edges to a set (initially empty) of edges so that the set does not form a cycle. When an edge that would create a cycle is encountered, ignore it. Continue examining edges until either $m - 1$ edges have been selected or you have come to the end of the edge list. If $m - 1$ edges are selected, these edges make up a minimal spanning tree for G. If fewer than $m - 1$ edges are selected, G is not connected.

Note: Step 1 can be accomplished using one of any number of standard sorting routines. Using the most efficient sorting routine, the time required to perform this step is proportional to $n \log n$. The second step of the algorithm, also of $n \log n$ time complexity, is the one that uses a forest of rooted trees to test for whether an edge should be added to the spanning set.

Kruskal's Algorithm—Version 2.

(1) Sort the edges as in Version 1.

(2) (2.1) Initialize each vertex in V to be the root of its own rooted tree.

(2.2) Go down the list of edges until either a spanning tree is completed or the edge list has been exhausted. For each edge $e = \{v_1, v_2\}$, we can determine whether e can be added to the spanning set without forming a cycle by determining whether the root of v_1's tree is equal to the root of v_2's tree. If the two roots are equal, then ignore e. If the roots are different, then we can add e to the spanning set. In addition, we merge the trees that v_1 and v_2 belong to. This is accomplished by either making v_1's root the parent of v_2's root or vice versa.

Notes:

(a) Since we start the algorithm with m trees and each addition of an edge decreases the number of trees by one, we end the algorithm with one rooted tree, provided a spanning tree exists.

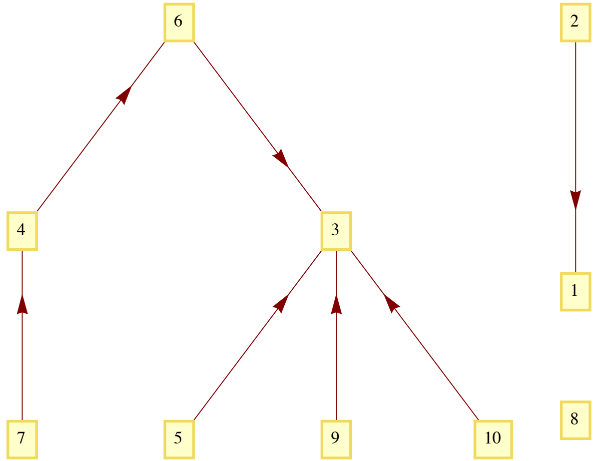
(b) The rooted tree that we develop in the algorithm is not the spanning tree itself.

Mathematica Implementation of Kruskal's Algorithm

We will implement Kruskal's Algorithm with *Mathematica*. First we will describe a very simple data structure for representing the forest of trees that is maintained within the algorithm. All that is needed is a list of integers, one for each of the vertices in the graph. For simplicity we will take the vertices to be the integers 1, 2, …, n and will illustrate with the case of $n = 10$. If **forest** is the list, then

$$\texttt{forest[[k]]} = \begin{cases} \boldsymbol{j} & \text{if } \boldsymbol{j} \text{ is } \boldsymbol{k}'\,s \text{ parent in the forest} \\ \mathbf{0} & \text{if } \boldsymbol{k} \text{ is the root of a tree in the forest} \end{cases}$$

For example, if **forest** is equal to {0, 1, 0, 6, 3, 3, 4, 0, 3, 3}, the vertices 1, 3, and 8 are roots of trees. Figure 10.3.4 shows the forest, where directed edges are used to indicate parent hood. An edge from k to j indicates that j is k's parent. Roots are sinks in this representation of trees.



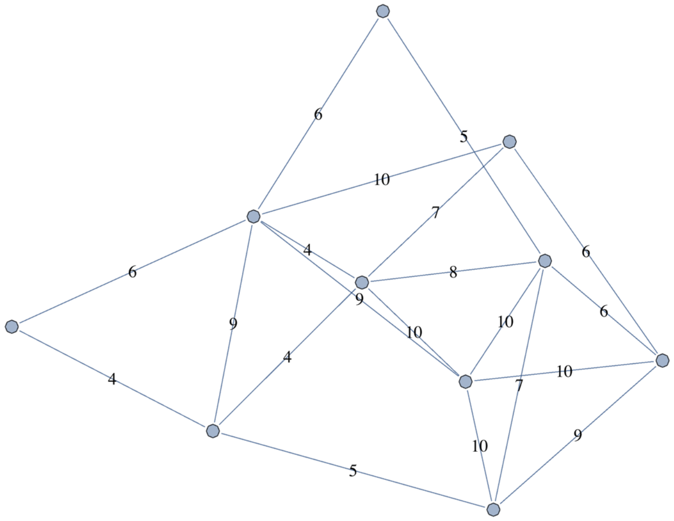
By representing forests in this way, it is easy to program functions that give the root of a tree and merge two trees. Notice the recursive nature of the **root** function. The input cell below has been set to be not evaluatable. These functions will be defined locally within the Kruskal algorithm code.

```
root[k_] := If[forest[[k]] == 0, k, root[forest[[k]]]];
merge[v1_, v2_] := (forest[[root[v2]]] = root[v1]);
```

Example 10.3.3. One way to represent a weighted graph in *Mathematica* is as a list of pairs {edge, weight} where the edge is a rule. For example, **{1 ⟷ 3, 6}** would be a edge connecting vertices 1 and 3 with weight 6. For consistency, we seed the random number generator and then generate a random graph, **wg**, having 10 vertices by "flipping a coin" to determine whether each edge is present. We also assign a assign random weight between 4 and 10 to each edge. These numbers are arbitrary and can be adjusted, if desired.

Here is the *Mathematica* code that generates the graph

```
SeedRandom[2012];
n = 10;
edges =
  Map[UndirectedEdge @@ # &, Subsets[Range[10], {2}] // Select[#, RandomReal[] ≤ 1 / 2 &] &];
e = Length[edges];
weights = RandomInteger[{4, 10}, e];
graph = Graph[MapThread[Labeled[#1, #2] &, {edges, weights}]]
```



```
edgelist = SortBy[Transpose[{edges, weights}], Last]
```

```
⎛ 1 •–• 2    4 ⎞
⎜ 2 •–• 8    4 ⎟
⎜ 3 •–• 8    4 ⎟
⎜ 4 •–• 7    5 ⎟
⎜ 6 •–• 8    5 ⎟
⎜ 1 •–• 3    6 ⎟
⎜ 1 •–• 7    6 ⎟
⎜ 4 •–• 5    6 ⎟
⎜ 5 •–• 10   6 ⎟
⎜ 2 •–• 10   7 ⎟
⎜ 4 •–• 6    7 ⎟
⎜ 2 •–• 4    8 ⎟
⎜ 1 •–• 8    9 ⎟
⎜ 1 •–• 9    9 ⎟
⎜ 5 •–• 6    9 ⎟
⎜ 1 •–• 10  10 ⎟
⎜ 2 •–• 9   10 ⎟
⎜ 4 •–• 9   10 ⎟
⎜ 5 •–• 9   10 ⎟
⎝ 6 •–• 9   10 ⎠
```

The following function presumes that the data from a weighted undirected graph is in the {edge, weight} format described above and called **`edgelist`**. The output is a sublist that comprises a minimal spanning tree for the input.

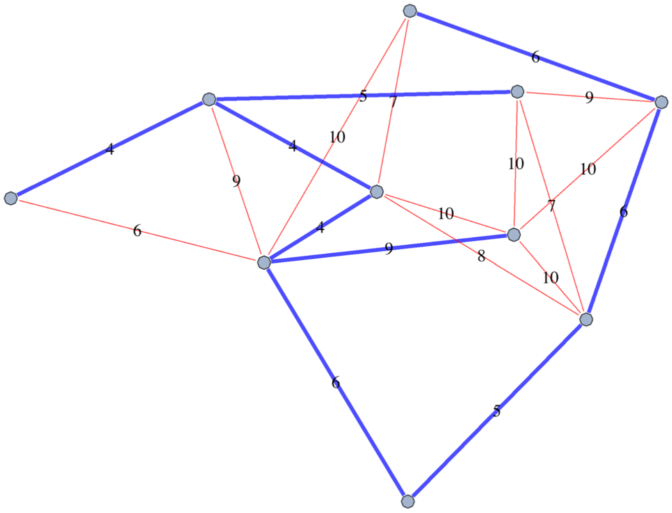
```
Kruskal[g_] :=
 Module[{nV, vertexset, spanset, edgepool, forest, nextedge, root, merge, index},
  root[k_] := If[forest[[k]] == 0, k, root[forest[[k]]]];
  merge[v1_, v2_] := (forest[[root[v2]]] = root[v1]);
  vertexset = Union[Flatten[(List @@ #) & /@ g[[All, 1]]]]; nV = Length[vertexset];
  Map[(index[vertexset[[#]]] = #) &, Range[nV]];
  forest = Table[0, {nV}]; spanset = {}; edgepool = SortBy[g, Last];
  While[(Length[spanset] < nV - 1) && (edgepool ≠ {}),
   nextedge = First[edgepool]; edgepool = Rest[edgepool];
   If[root[index[nextedge[[1, 1]]]] ≠ root[index[nextedge[[1, 2]]]], AppendTo[
     spanset, nextedge]; merge[index[nextedge[[1, 1]]], index[nextedge[[1, 2]]]]]];
  If[Length[spanset] == nV - 1, spanset, "Graph not connected - no spanning tree exists."]]
```

We use the function to generate a spanning tree for our example:

```
st = Kruskal[edgelist]
```

```
 1 ⟷ 2    4
 2 ⟷ 8    4
 3 ⟷ 8    4
 4 ⟷ 7    5
 6 ⟷ 8    5
 1 ⟷ 7    6
 4 ⟷ 5    6
 5 ⟷ 10   6
 1 ⟷ 9    9
```

Lets take a look at the spanning tree, with tree edges colored blue and the unused edges colored red.



Note: The *Mathematica* code to that displays this and other spanning trees is not so instructive to the general reader. If you are interested in seeing the code, it is available as part of the package ADS2.m. See the text’s web page for download information. The function name is **KruskalGraph**.

Example 10.3.4. Lets look at how long it take to complete the algorithm for a graph with 200 edges. Drawing the graph isn't of interest, it's mostly the time to generate the spanning tree we are interested in.

```
SeedRandom[2010];
largegraph = Map[{UndirectedEdge @@ #, RandomInteger[{4, 10}]} &,
   RandomGraph[BernoulliGraphDistribution[200, 0.5]] // EdgeList //
    Select[#, (First[#] < Last[#]) &] &];
```

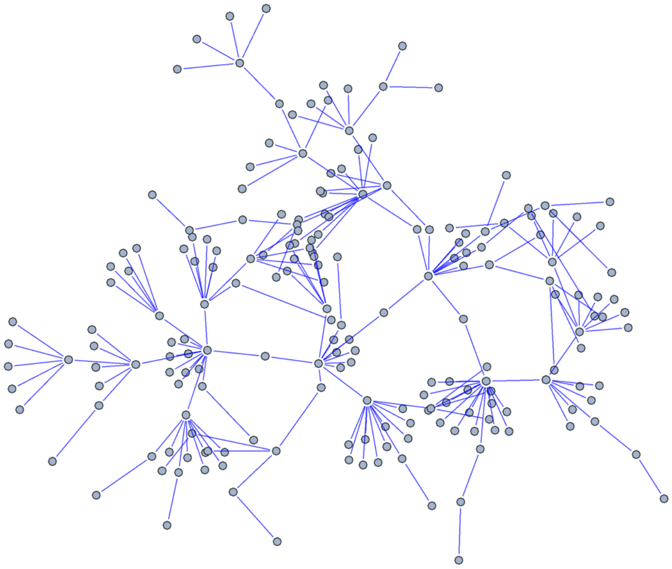
The time will vary depending on the computer you are using. The expression **First[Timing[calculation;]]** will perform a calculation and just display the CPU time needed, in seconds, to complete the calculation.

```
{First[Timing[largetree = Kruskal[largegraph];]], $System}
```

```
{0.564645, Mac OS X x86 (64−bit)}
```

Just for fun, here is what the spanning tree looks like.

```
KruskalGraph[largetree, Blue]
```



Example 10.3.5. Lets conclude with an example that is based on some real data, using Wolfram's Computable database of city data. We will build a minimal spanning tree for the large cities of France, where "large" is taken to mean a population of 100,000 or more. The weights of edges between cities will the distance between them. First here is that list of cities. By the way, you can change "France" to any other country or region and get similar results.

```
citylist = CityData[{Large, "France"}]
```

```
Paris                  IleDeFrance               France
Marseille              ProvenceAlpesCoteDAzur    France
Lyon                   RhoneAlpes                France
Toulouse               MidiPyrenees              France
Nice                   ProvenceAlpesCoteDAzur    France
Nantes                 PaysDeLaLoire             France
Strasbourg             Alsace                    France
Montpellier            LanguedocRoussillon       France
Bordeaux               Aquitaine                 France
Lille                  NordPasDeCalais           France
Rennes                 Bretagne                  France
LeHavre                HauteNormandie            France
Reims                  ChampagneArdenne          France
SaintEtienne           RhoneAlpes                France
Toulon                 ProvenceAlpesCoteDAzur    France
Grenoble               RhoneAlpes                France
Angers                 PaysDeLaLoire             France
Dijon                  Bourgogne                 France
Brest                  Bretagne                  France
LeMans                 PaysDeLaLoire             France
Nimes                  LanguedocRoussillon       France
AixEnProvence          ProvenceAlpesCoteDAzur    France
Limoges                Limousin                  France
ClermontFerrand        Auvergne                  France
Tours                  Centre                    France
Amiens                 Picardie                  France
Villeurbanne           RhoneAlpes                France
Metz                   Lorraine                  France
Besancon               FrancheComte              France
Perpignan              LanguedocRoussillon       France
Orleans                Centre                    France
Rouen                  HauteNormandie            France
Mulhouse               Alsace                    France
Caen                   BasseNormandie            France
BoulogneBillancourt    IleDeFrance               France
Nancy                  Lorraine                  France
Montreuil              IleDeFrance               France
Argenteuil             IleDeFrance               France
```

As part of the geographic database, there is a functional called GeoDistance that we will use to define a function that tells us how many kilometers separate any two cities.

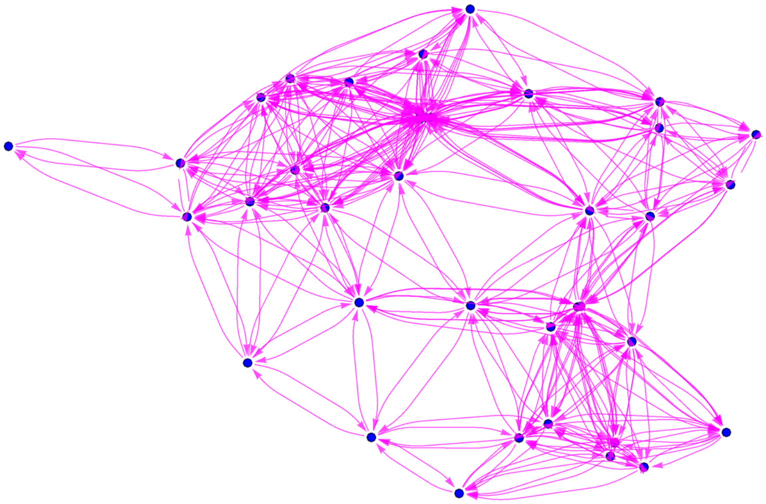
```
CityDistance[city1_, city2_] :=
 GeoDistance[CityData[city1, "Coordinates"], CityData[city2, "Coordinates"]] / 1000
```

Next, we generate the weighted graph.

```
g = Map[{First[#[[1]]] → First[#[[2]]], CityDistance @@ #} &, Tuples[citylist, 2]] //
   Select[#, Last[#] > 0 &] &;
```

In France there are large cities and drawing the K_{38} produces a largely uninteresting figure. By drawing only the edges for cities within 300 km of one another, the figure is a little more interesting. The cluster in the north central part of France is greater-Paris, where several other adjacent cities are also large. We use the longitude and latitude of each city to plot a location on the plane.

```
Graph[g // Select[#, Last[#] < 300 &] & // #[[All, 1]] &,
 VertexCoordinates → Map[(First[#] → Reverse[CityData[#, "Coordinates"]]) &, citylist],
 EdgeStyle → {Darker, Magenta}, VertexStyle → Blue]
```



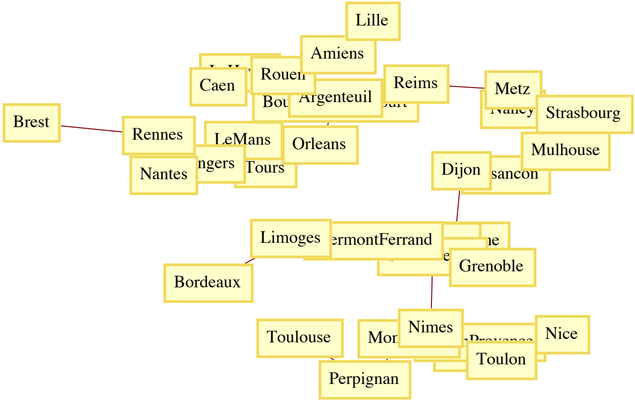
Now we use our **Kruskal** function to generate a spanning tree. Notice the first few edges in the list are of very close cites.

```
span = Kruskal[g]
```

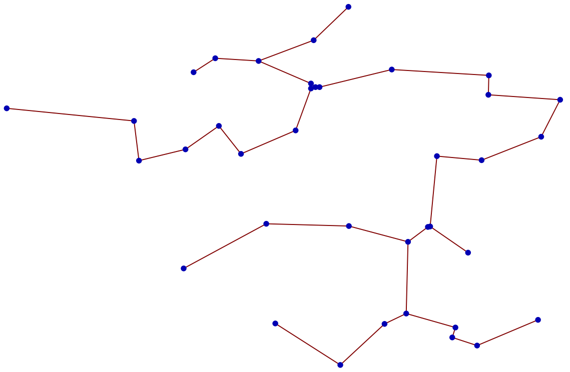
```
⎛ Villeurbanne → Lyon                4.04522 ⎞
  Montreuil → Paris                  6.6039
  BoulogneBillancourt → Paris        8.06249
  Argenteuil → Paris                 11.5285
  Marseille → AixEnProvence          25.091
  Montpellier → Nimes                46.3561
  Nancy → Metz                       47.825
  Marseille → Toulon                 48.9574
  LeHavre → Caen                     49.043
  Lyon → SaintEtienne                50.2382
  Rouen → LeHavre                    69.9004
  Besancon → Dijon                   75.559
  Tours → LeMans                     78.1345
  LeMans → Angers                    80.1425
  Angers → Nantes                    82.6313
  Villeurbanne → Grenoble            92.0243
  Nimes → AixEnProvence              94.3932
  Mulhouse → Strasbourg              96.3815
  Rennes → Nantes                    98.1899
  Amiens → Lille                     98.9384
  Argenteuil → Rouen                 101.2
  Rouen → Amiens                     101.847
  Orleans → BoulogneBillancourt      106.438
  Tours → Orleans                    107.746
  SaintEtienne → ClermontFerrand     109.348
  Besancon → Mulhouse                115.034
  Strasbourg → Nancy                 117.825
  Reims → Montreuil                  124.727
  Toulon → Nice                      126.35
  Montpellier → Perpignan            128.738
  ClermontFerrand → Limoges          142.36
  Toulouse → Perpignan               155.437
  Metz → Reims                       157.396
  Villeurbanne → Dijon               173.794
  SaintEtienne → Nimes               176.717
  Bordeaux → Limoges                 180.776
⎝ Brest → Rennes                     211.714 ⎠
```

Here are a couple of graphs of the spanning tree. The first shows city names, but would need to be blown up to see them all.

```
GraphPlot[span, EdgeLabeling → False, VertexLabeling → True,
 VertexCoordinateRules → Map[(First[#] → Reverse[CityData[#, "Coordinates"]]) &, citylist]]
```



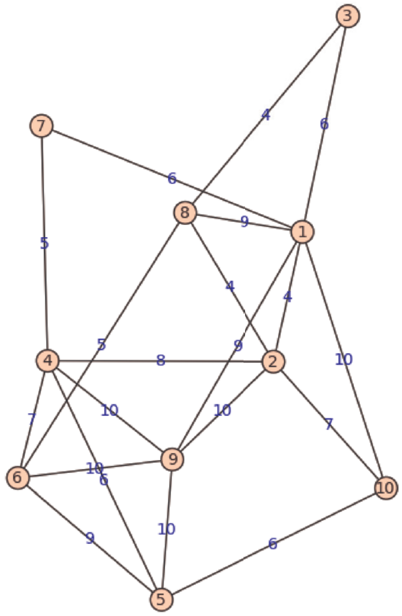
The same graph with VertexLabeling shut off shows the tree's structure.



Sage Note

Kruskal's algorithm has been implemented in Sage. Here we illustrate how the spanning tree for the graph in Example 10.3.3 can be generated. We start with graph data consisting of a list of triples of the form (vertex, vertex, label). The weighted method tells Sage to consider the labels as weights.

```
edges=[(1, 2, 4), (2, 8, 4), (3, 8, 4), (4, 7, 5), (6, 8, 5), (1, 3, 6), (1, 7, 6), (4, 5, 6),
(5, 10, 6), (2, 10, 7), (4, 6, 7), (2, 4, 8), (1, 8, 9), (1, 9, 9), (5, 6, 9), (1, 10, 10), (2,
9, 10), (4, 9, 10), (5, 9, 10), (6, 9, 10)]
G=Graph(edges)
G.weighted(True)
G.graphplot(edge_labels=True,save_pos=True).show()
```

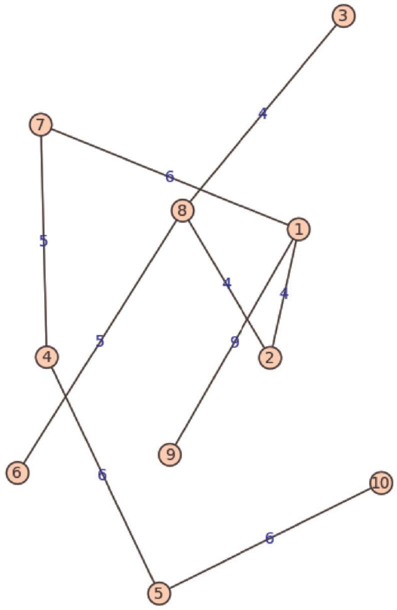


Next, we load the kruskal function and use it to generate the list of edges in a spanning tree of G.

```
from sage.graphs.spanning_tree import kruskal
E = kruskal(G, check=True);E
  [(1, 2, 4), (2, 8, 4), (3, 8, 4), (4, 7, 5), (6, 8, 5), (1, 7, 6), (4, 5, 6), (5, 10, 6), (1, 9, 9)]
```

To see the resulting tree with the same embedding as G, we generate a graph from the spanning tree edges. Next, we set the positions of the vertices to be the same as in the graph. Finally, we plot the tree.

```
T=Graph(E)
T.set_pos(G.get_pos())
T.graphplot(edge_labels=True).show()
```

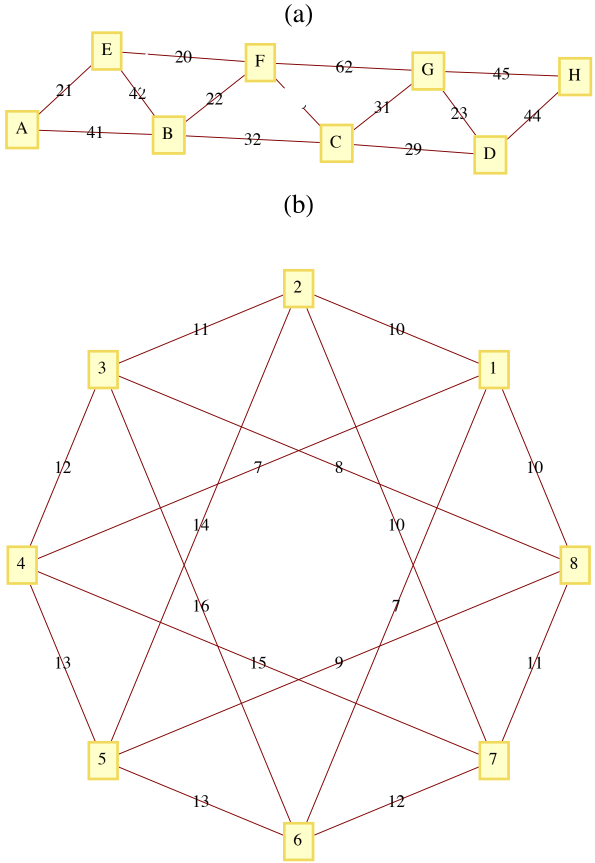


EXERCISES FOR SECTION 10.3

A Exercises

1. Suppose that an undirected tree has diameter d and that you would like to select a vertex of the tree as a root so that the resulting rooted tree has the smallest depth possible. How would such a root be selected and what would be the depth of the tree (in terms of d)?

2. Use Kruskal's algorithm to find a minimal spanning tree for the following graphs. In addition to the spanning tree, find the final rooted tree in the algorithm. When you merge two trees in the algorithm, make the root with the lower number the root of the new tree.


(a)

(b)

C Exercises

3. Suppose that information on buildings is arranged in records with five fields: the name of the building, its location, its owner, its height, and its floor space. The location and owner fields are records that include all of the information that you would expect, such as street, city, and state, together with the owner's name (first, middle, last) in the owner field. Draw a rooted tree to describe this type of record,

4. (Requires *Mathematica*) Given a country with n large cities evenly distributed in an area of A square kilometers, one would expect that the total length of the spanning tree for the cities would roughly depend on n and A. In the case of France, $n = 37$ cities, $A = 547\,030\text{ km}^2$, and the length of the spanning tree is 3501.59 km. Look for such a relationship by collecting similar data for other countries or generating random data. To get areas of countries you can use the **CountryData** function.

```
CountryData["France", "Area"]
```

```
547030.
```

Caution: Oddly shaped countries such as Chile, or countries that have large uninhabited areas such as Brazil will probably not fit any proposed model.

10.4 Binary Trees

An ordered rooted tree is a rooted tree whose subtrees are put into a definite order and are, themselves, ordered rooted trees. An empty tree and a single vertex with no descendants (no subtrees) are ordered rooted trees.

Example 10.4.1. The trees in Figure 10.4.1 are identical rooted trees, with root 1, but as ordered trees, they are different.

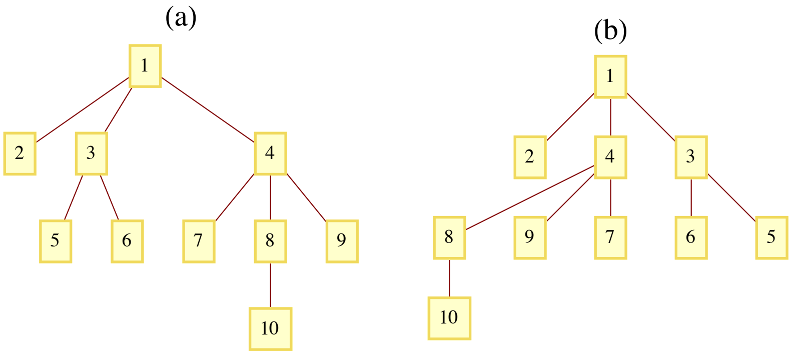
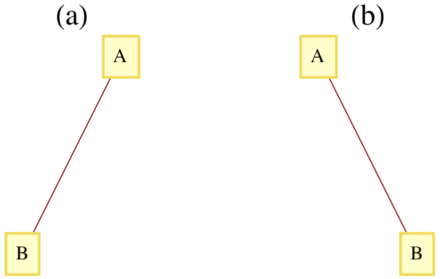


Figure 10.4.1
Two different ordered rooted trees

If a tree rooted at v has p subtrees, we would refer to them as the first, second, ..., p^{th} subtrees. If we restrict the number of subtrees of each vertex to be less than or equal to two, we have a binary (ordered) tree.

Definition: Binary Tree. *A binary tree is*
(a) a tree consisting of no vertices (the empty tree), or
(b) a vertex with two subtrees that are both binary trees. The subtrees are called the left and right subtrees.

The difference between binary trees and ordered trees is that every vertex of a binary tree has exactly two subtrees (one or both of which may be empty), while a vertex of an ordered tree may have any number of subtrees. The two trees in Figure 10.4.2 would be considered identical as ordered trees; however, they are different binary trees. Tree (a) has an empty right subtree and Tree (b) has an empty left subtree.



Terminology and General Facts:

(a) A vertex of a binary tree with two empty subtrees is called a *leaf*. All other vertices are called *internal vertices*.

(b) The number of leaves in a binary tree can vary from one up to roughly half the number of vertices in the tree (see Exercise 4 of this section).

(c) The maximum number of vertices at level k of a binary tree is 2^k , $k \geq 0$ (see Exercise 6 of this section).

(d) A *full binary tree* is a tree in which each vertex has either zero or two empty subtrees. In other words, each vertex has either two or zero children. See Exercise 7 of this section for a general fact about full binary trees.

TRAVERSALS OF BINARY TREES

The traversal of a binary tree consists of visiting each vertex of the tree in some prescribed order. Unlike graph traversals, the consecutive vertices that are visited are not always connected with an edge. The most common binary tree traversals are differentiated by the order in which the root and its subtrees are visited. The three traversals are best described recursively and are:

(1) **Preorder Traversal**:
 (a) Visit the root of the tree.
 (b) Preorder traverse the left subtree.
 (c) Preorder traverse the right subtree.

(2) **Inorder Traversal**:
 (a) Inorder traverse the left subtree.
 (b) Visit the root of the tree.
 (c) Inorder traverse the right subtree.

(3) **Postorder Traversal**:

(a) Postorder traverse the left subtree.
(b) Postorder traverse the right subtree.
(c) Visit the root of the tree.

Any traversal of an empty tree consists of doing nothing.

Example 10.4.2. For the tree in Figure 10.4.3, the orders in which the vertices are visited are:

A-B-D-E-C-F-G, for the preorder traversal

D-B-E-A-F-C-G, for the inorder traversal and

D-E-B-F-G-C-A, for the preorder traversal.

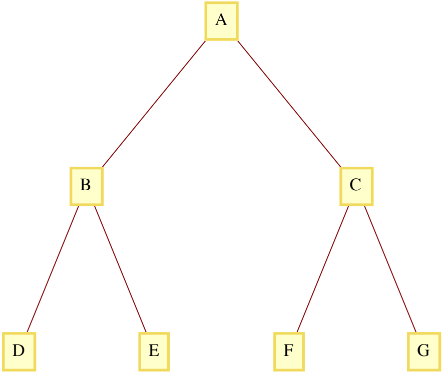


Figure 10.4.3

Example 10.4.3: Binary Tree Sort. Given a collection of integers (or other objects than can be ordered), one technique for sorting is a binary tree sort. If the integers are $a_1, a_2, \ldots, a_n,\ n \geq 1$, we first execute the following algorithm that creates a binary tree:

```
(1) Insert $a_1$ into the root of the tree.
(2) For k := 2 to n        //insert $a_k$ into the tree
    (2.1) r = $a_1$ ,
    (2.2) inserted = false
    (2.3) While Not(inserted) Do
        If $a_k < r$ then
                if r has a left child
                    then r = left child of r
                    else make $a_k$ the left child of r; inserted = true
            else  // $a_k \geq r$
                if r has a right child
                    then r = right child of r
                    else make $a_k$ the right child of r; inserted = true
```

If the integers to be sorted are 25, 17, 9, 20, 33, 13, and 30, then the tree that is created is the one in Figure 10.4.4. The inorder traversal of this tree is 9, 13, 17, 20, 25, 30, 33, the integers in ascending order. In general, the inorder traversal of the tree that is constructed in the algorithm above will produce a sorted list. The preorder and postorder traversals of the tree have no meaning here.

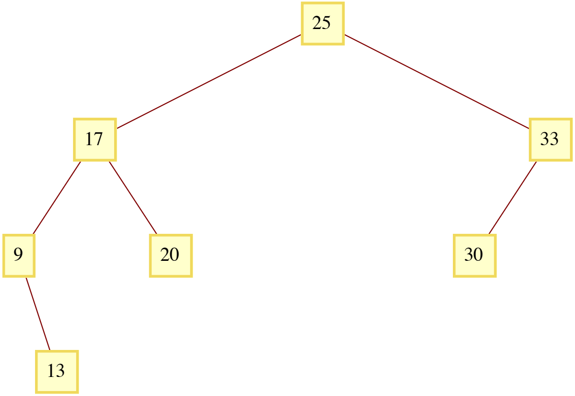


Figure 10.4.4

EXPRESSION TREES

A convenient way to represent an algebraic expression is by its expression tree. Consider the expression

$$X = a*b - c/d + e.$$

Since it is customary to put a precedence on multiplication/divisions, X is evaluated as $((a*b) - (c/d)) + e$. Consecutive multiplication/divisions or addition/subtractions are evaluated from left to right. We can analyze X further by noting that it is the sum of two simpler expressions $(a*b) - (c/d)$ and e?. The first of these expressions can be broken down further into the difference of the expressions $a*b$ and c/d. When we decompose any expression into

(left expression) (operation) (right expression),

the expression tree of that expression is the binary tree whose root contains the operation and whose left and right subtrees are the trees of the left and right expressions, respectively. Additionally, a simple variable or a number has an expression tree that is a single vertex containing the variable or number. The evolution of the expression tree for expression X appears in Figure 10.4.5.

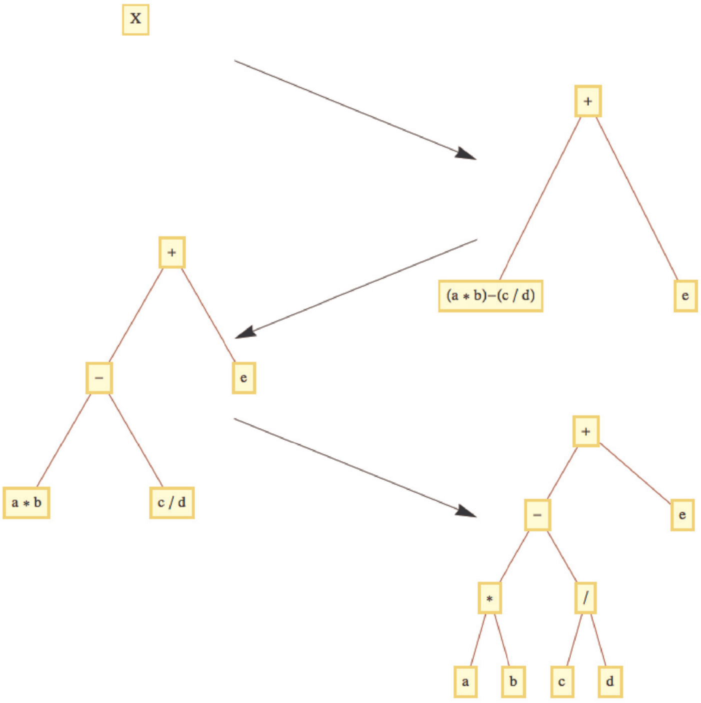


Figure 10.4.5

Example 10.4.4.

(a) If we intend to apply the addition and subtraction operations in X first, we would parenthesize the expression to $a*(b - c)/(d + e)$. Its expression tree appears in Figure 10.4.6a.

(b) The expression trees for $a^2 - b^2$ and for $(a + b)*(a - b)$ appear in Figures 10.4.6(b) and 10.4.6(c).

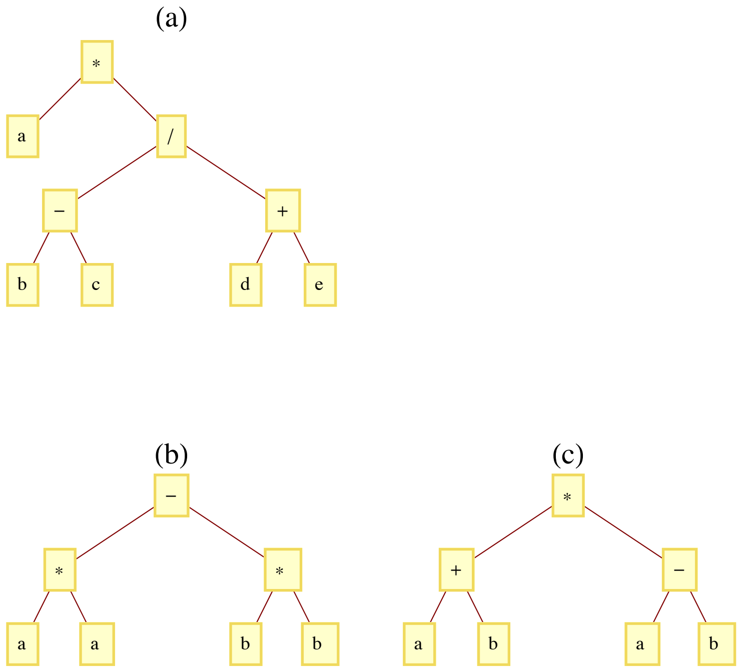


Figure 10.4.6

The three traversals of an operation tree are all significant. A binary operation applied to a pair of numbers can be written in three ways. One is the familiar infix form, such as $a + b$ for the sum of a and b. Another form is prefix, in which the same sum is written $+a\,b$. The final form is postfix, in which the sum is written $a\,b\,+$. Algebraic expressions involving the four standard arithmetic operations ($+$, $-$, $*$, and $/$) in prefix and postfix form are defined as follows:

Prefix: (a) A variable or number is a prefix expression, (b) Any operation followed by a pair of prefix expressions is a prefix expression.

Postfix: (a) A variable or number is a postfix expression, (b) Any pair of postfix expressions followed by an operation is a postfix expression.

The connection between traversals of an expression tree and these forms is simple:

(a) The preorder traversal of an expression tree will result in the prefix form of the expression.

(b) The postorder traversal of an expression tree will result in the postfix form of the expression.

(c) The inorder traversal of an operation tree will not, in general, yield the proper infix form of the expression. If an expression requires parentheses in infix form, an inorder traversal of its expression tree has the effect of removing the parentheses.

Example 10.4.5. The preorder traversal of the tree in Figure 10.4.5 is $+-*a\,b/c\,d\,e$, which is the prefix version of expression X. The postfix traversal is $a\,b*c\,d/-e\,+$. Note that since the original form of X needed no parentheses, the inorder traversal, $a*b - c/d + e$, is the correct infix version.

COUNTING BINARY TREES

We close this section with a formula for the number of different binary trees with n vertices. The formula is derived using generating functions. Although the complete details are beyond the scope of this text, we will supply an overview of the derivation in order to illustrate how generating functions are used in advanced combinatorics.

Let $B(n)$ be the number of different binary trees of size n (n vertices), $n \geq 0$. By our definition of a binary tree, $B(0) = 1$. Now consider any positive integer $n + 1$, $n \geq 0$. A binary tree of size $n + 1$ has two subtrees, the sizes of which add up to n. The possibilities can be broken down into $n + 1$ cases:

Case 0: Left subtree has size 0; right subtree has size n.

Case 1: Left subtree has size 1; right subtree has size $n - 1$.

$\vdots$

Case k: Left subtree has size k; right subtree has size $n - k$.

$\vdots$

Case n: Left subtree has size n; right subtree has size 0.

In the general Case k, we can count the number of possibilities by multiplying the number of ways that the left subtree can be filled, $B(k)$, by the number of ways that the right subtree can be filled. $B(n-k)$. Since the sum of these products equals $B(n+1)$, we obtain a recurrence relation for $n \geq 0$:

$$\begin{aligned} B(n+1) &= B(0)\,B(n) + B(1)\,B(n-1) + \cdots + B(n)\,B(0) \\ &= \sum_{k=0}^{n} B(k)\,B(n-k) \end{aligned}$$

Now take the generating function of both sides of this recurrence relation:

$$\sum_{n=0}^{\infty} B(n+1)\,z^n = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} B(k)\,B(n-k)\right)z^n$$

or

$$G(B\uparrow;\ z) = G(B * B;\ z) = G(B;\ z)^2.$$

Recall that $G(B\uparrow; z) = \frac{G(B;z)-B(0)}{z} = \frac{G(B;z)-1}{z}$ If we abbreviate $G(B;\ z)$ to G, we get

$$\frac{G-1}{z} = G^2 \ \Rightarrow\ z\,G^2 - G + 1 = 0$$

Using the quadratic equation we get two solutions:

$$G_1 = \frac{1+\sqrt{1-4z}}{2z} \text{ and } G_2 = \frac{1-\sqrt{1-4z}}{2z}$$

The gap in our deviation occurs here since we don't presume calculus. If we expand G_1 as an extended series, we find

$$G_1 = \frac{1+\sqrt{1-4z}}{2z} = \frac{1}{z} - 1 - z - 2z^2 - 5z^3 - 14z^4 - 42z^5 + \cdots$$

The coefficients after the first one are all negative and there is *singularity* at 0 because of the $\frac{1}{z}$ term. However if we do the same with G_2 we get

$$G_2 = \frac{1-\sqrt{1-4z}}{2z} = 1 + z + 2z^2 + 5z^3 + 14z^4 + 42z^5 + \cdots$$

Further analysis leads to a closed form expression for $B(n)$, which is

$$B(n) = \frac{1}{n+1}\binom{2n}{n}.$$

This sequence of numbers is often called the *Catalan numbers*. For more information on the Catalan numbers, see the entry A000108 in The On-Line Encyclopedia of Integer Sequences.

Mathematica Note

It may be of interest to note how the extended power series expansions of G_1 and G_2 are determined using *Mathematica*. The function **`Series`** will generate a finite number of terms. For example for G_1 we evaluate the expression

$$\mathtt{Series}\left[\frac{\mathtt{1+\sqrt{1-4\,z}}}{\mathtt{2\,z}},\ \mathtt{\{z,\ 0,\ 5\}}\right]$$

$$\frac{1}{z} - 1 - z - 2z^2 - 5z^3 - 14z^4 - 42z^5 + O\left(z^6\right)$$

The first argument is the closed form expression for G_1. The second argument has three parts. The first part is the variable. The second part is the center of the expansion, 0, since we want a sum in powers of z to get the coefficients of those powers. The third part is the maximum power of the variable. Notice that the output also include the term $O(z^6)$ to indicate that the remaining terms are all multiples of z^6. If we wanted the first three terms of the expansion around -1, which is a sum of powers of $z+1$, we would get

$$\mathbf{Series}\left[\frac{\mathbf{1+\sqrt{1-4\,z}}}{\mathbf{2\,z}},\ \{\mathbf{z,\ -1,\ 3}\}\right]$$

$$\left(-\frac{1}{2}-\frac{\sqrt{5}}{2}\right)+\left(-\frac{1}{2}-\frac{3}{2\sqrt{5}}\right)(z+1)+\left(-\frac{1}{2}-\frac{13}{10\sqrt{5}}\right)(z+1)^2+\left(-\frac{1}{2}-\frac{61}{50\sqrt{5}}\right)(z+1)^3+O\!\left((z+1)^4\right)$$

Sage Note

In Sage, one has the capability of being very specific about how algebraic expressions should be interpreted. This also makes working with various algebraic expressions a bit more confusing to the beginner. Here, without getting into a lot of detail, is how to get a Laurent expansion for G_1 above.

```
sage: R.<z>=PowerSeriesRing(ZZ,'z')
sage: G=(1+sqrt(1-4*z))/(2*z)
sage: G
z^-1 - 1 - z - 2*z^2 - 5*z^3 - 14*z^4 - 42*z^5 - 132*z^6 - 429*z^7 - 1430*z^8 - 4862*z^9 -
16796*z^10 - 58786*z^11 - 208012*z^12 - 742900*z^13 - 2674440*z^14 - 9694845*z^15 -
35357670*z^16 - 129644790*z^17 - 477638700*z^18 + O(z^19)
```

The first output above declares a structure called a *ring* that contains power series. Here we are not using that structure, just a specific element, **G**. So the important thing about this first input is that it establishes **z** as being a variable associated with power series. When the second expression defines the value of **G** in terms of **z**, it is automatically converted to a power series. Notice that the final output does match the *Mathematica* result, but with more terms displayed. In Chapter 16 we will introduce rings and will be able to take advantage of Sage's capabilities in this area and this will probably make more sense.

EXERCISES FOR SECTION 10.4

A Exercises

1. Draw the expression trees for the following expressions:

(a) $a\,(b + c)$

(b) $a\,b + c$

(c) $a\,b + a\,c$

(d) $b\,b - 4\,a\,c$

(e) $((a_3\,x + a_2)\,x + a_1)\,x + a_0$

2. Draw the expression trees for

(a) $\frac{x^2-1}{x-1}$

(b) $x\,y + x\,z + y\,z$

3. Write out the preorder, inorder, and postorder traversals of the trees in Exercise 1 above.

4. Verify the formula for $B(k)$, $0 \leq k \leq 3$ by drawing all binary trees with three or fewer vertices.

5. (a) Draw a binary tree with seven vertices and only one leaf.

(b) Draw a binary tree with seven vertices and as many leaves as possible.

B Exercises

6. Prove that the maximum number of vertices at level k of a binary tree is 2^k and that a tree with that many vertices at level k must have at least $2^{k+1} - 1$ vertices.

7. Prove that if T is a full binary tree, then the number of leaves of T is one more than the number of internal vertices (non-leaves).

8. Use *Mathematica* to determine the sequence whose generating function is $G(z) = \frac{1}{(1-z)^3}$

SUPPLEMENTARY EXERCISES FOR CHAPTER 10

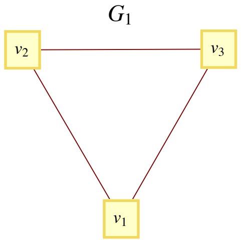
Section 10.1

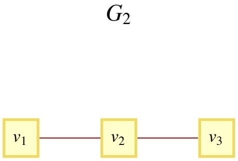
1. Show that in a tree with n vertices, the sum of the degrees of all vertices is $2n-2$.

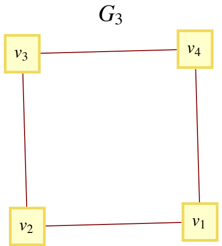
2. (a) Show that there exists a tree with ten vertices and the property that each vertex has degree either 1 or 5.

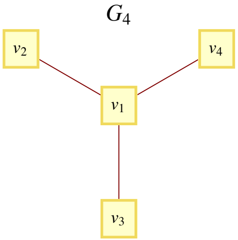
(b) Prove that no such tree exists with an odd number of vertices.

3. Given $G=(V,E)$ with $|V|=v$ and $|E|=e$, G is *graceful* if the elements in V can be labeled with v distinct positive integers such that for each positive integer k, $1 \leq k \leq e$, there is an edge connecting vertices i and j such that $|i-j|=k$.
(a) Which of the following graphs are graceful?





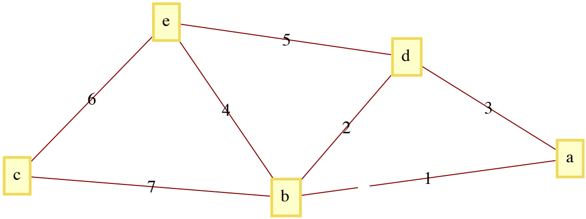




(b) Prove that every chain (see Figure 9.6.1) is graceful. It has been conjectured that every tree is graceful.

Section 10.2

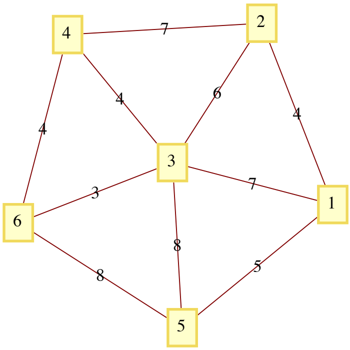
4. Let G be the graph



Find a minimal spanning tree for G using the method of left and right sets. Start with $R=\{a\}$ and $L=\{b,c,d,e\}$. At each step show what L and R are and indicate what edge you added to the tree.

Section 10.3

5. Find a minimal spanning tree for the graph below. Use Kruskal's algorithm and draw the forest of rooted trees after you have added the third edge to the spanning set.



6. If a rooted tree has the properties that each vertex has no more than m children and its depth is less than or equal to n, how many vertices could it have?

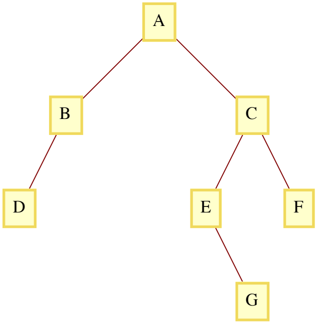
Section 10.4

7. Represent the algebraic expression $(((a - b) * c) + 7) * ((d + 4) / x)$ by a tree. Determine the depth of the tree.

8. (a) Write out the post order traversal for the graph below.

(b) Write out the inorder traversal for the graph below.

(c) Write out the preorder traversal for the graph below.



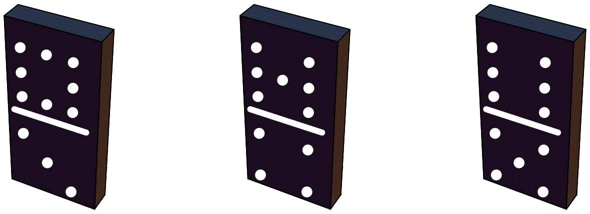
9. (a) Draw the operation tree for the expression $a^2 + 2$ ab $+ b$, where all multiplications are done first, $x^2 = xx$, and additions are done from left to right (as usual).

(b) List the postorder traversal of the tree that you obtained in part a. What is the significance of this traversal?

10. (a) Draw the binary tree that would be constructed by the binary sort algorithm for sorting the integers 5, 55, 34, 38, 11, 3, 71, 23, and 18 in descending order. Afterwards, list the preorder traversal of the tree and then build a sorting tree from that order. Repeat the process above, but do an inorder traversal instead of preorder.

(b) Based on the results of part a, what can you say about the process of building a binary sorting tree, storing it in preorder (or inorder), and then building a tree from that new list?

chapter 11



ALGEBRAIC SYSTEMS

GOALS

The primary goal of this chapter is to make the reader aware of what an algebraic system is and how algebraic systems can be studied at different levels of abstraction. After describing the concrete, axiomatic, and universal levels, we will introduce one of the most important algebraic systems at the axiomatic level, the group. In this chapter, group theory will be a vehicle for introducing the universal concepts of isomorphism, direct product, subsystem, and generating set. These concepts can be applied to all algebraic systems. The simplicity of group theory will help the reader obtain a good intuitive understanding of these concepts. In Chapter 15, we will introduce some additional concepts and applications of group theory. We will close the chapter with a discussion of how some computer hardware and software systems use the concept of an algebraic system.

11.1 Operations

One of the first mathematical skills that we all learn is how to add a pair of positive integers. A young child soon recognizes that something is wrong if a sum has two values, particularly if his or her sum is different from the teacher's. In addition, it is unlikely that a child would consider assigning a non-positive value to the sum of two positive integers. In other words, at an early age we probably know that the sum of two positive integers is unique and belongs to the set of positive integers. This is what characterizes all binary operations on a set.

Definition: Binary Operation. *Let S be a nonempty set. A binary operation on S is a rule that assigns to each ordered pair of elements of S a unique element of S. In other words, a binary operation is a function from $S \times S$ into S.*

Example 11.1.1. Union and intersection are both binary operations on the power set of any universe. Addition and multiplication are binary operators on the natural numbers. Addition and multiplication are binary operations on the set of 2 by 2 real matrices, $M_{2\times 2}(\mathbb{R})$. Division is a binary operation on some sets of numbers, such as the positive reals. But on the integers ($1/2 \notin \mathbb{Z}$) and even on the real numbers ($1/0$ is not defined), division is not a binary operation.

Notes:

(a) We stress that the image of each ordered pair must be in S. This requirement disqualifies subtraction on the natural numbers from consideration as a binary operation, since $1 - 2$ is not a natural number. Subtraction *is* a binary operation on the integers.

(b) On Notation. Despite the fact that a binary operation is a function, symbols, not letters, are used to name them. The most commonly used symbol for a binary operation is an asterisk, *. We will also use a diamond, $\diamond$, when a second symbol is needed.

(c) If * is a binary operation on S and $a, b \in S$, there are three common ways of denoting the image of the pair (a, b). They are:

$*a\,b$	$a*b$	$a\,b\,*$
Prefix Form	Infix Form	Postfix FOrm

We are all familiar with infix form. For example, $2 + 3$ is how everyone is taught to write the sum of 2 and 3. But notice how $2 + 3$ was just described in the previous sentence! The word *sum* preceded 2 and 3. Orally, prefix form is quite natural to us. The prefix and postfix forms are superior to infix form in some respects. In Chapter 10, we saw that algebraic expressions with more than one operation didn't need parentheses if they were in prefix or postfix form. However, due to our familiarity with infix form, we will use it throughout most of the remainder of this book.

Some operations, such as negation of numbers and complementation of sets, are not binary, but unary operators.

Definition: Unary Operation. *Let S be a nonempty set. A unary operator on S is a rule that assigns to each element of S a unique element of S. In other words, a unary operator is a function from S into S.*

COMMON PROPERTIES OF OPERATIONS

Whenever an operation on a set is encountered, there are several properties that should immediately come to mind. To effectively make use of an operation, you should know which of these properties it has. By now, you should be familiar with most of these properties. We will list the most common ones here to refresh your memory and define them for the first time in a general setting. Let S be any set and * a binary operation on S.

Properties that apply to a single binary operation:

*Let * be a binary operation on a set S*

** is **commutative** if $a * b = b * a$ for all $a, b \in S$.*

** is **associative** if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.*

** **has an identity** if there exists an element, e, in S such that $a * e = e * a = a$ for all $a \in S$.*

** has the **inverse property** if for each $a \in S$, there exists $b \in S$ such that $a * b = b * a = e$.*

We call b an inverse of a.

** is **idempotent** if a * a = a for all $a \in S$. Properties that apply to two binary operations:*

Let $\diamond$ be a second binary operation on S.

*$\diamond$ is left distributive over * if $a \diamond (b * c) = (a \diamond b) * (a \diamond c)$ for all $a, b, c \in S$.*

*$\diamond$ is right distributive over * if $(b * c) \diamond a = (b \diamond a) * (c \diamond a)$ for all $a, b, c \in S$.*

*$\diamond$ is distributive over * if $\diamond$ is both left and right distributive over *.*

Let $-$ be a unary operation.

A unary operation — on S has the involution property if $-(-a) = a$ for all $a \in S$.

Finally, a property of sets, as they relate to operations.

*If T is a subset of S, we say that T is closed under * if $a, b \in T$ implies that $a * b \in T$. In other words, by operating on elements of T with *, you can't obtain new elements that are outside of T.*

Example 11.1.2.

(a) The odd integers are closed under multiplication, but not under addition.

(b) Let p be a proposition over U and let A be the set of propositions over U that imply p. That is; $q \in A$ if $q \Rightarrow p$. Then A is closed under both conjunction and disjunction.

(c) The set positive integers that are multiples of 5 is closed under both addition and multiplication.

Note: It is important to realize that the properties listed above depend on both the set and the operation(s).

OPERATION TABLES

If the set on which an operation is defined is small, a table is often a good way of describing the operation. For example, we might want to define $\oplus$ on $\{0,\ 1,\ 2\}$ by

$$a \oplus b = \begin{cases} a+b & \text{if } a+b<3 \\ a+b-3 & \text{if } a+b \geq 3 \end{cases}$$

The table for $\oplus$ is

"

⊕	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

The top row and left column are the column and row headings, respectively. To determine $a \oplus b$, find the entry in Row a and Column b. The following operation table serves to define * on $\{i,\ j,\ k\}$.

"

*	i	j	k
i	i	i	i
j	j	j	j
k	k	k	k

Note that; $j * k = j$, yet $k * j = k$. Thus, * is not commutative. Commutivity is easy to identify in a table: the table must be symmetric with respect to the diagonal going from the top left to lower right.

EXERCISES FOR SECTION 11.1

A Exercises

1. Determine the properties that the following operations have on the positive integers.

   (a) addition

   (b) multiplication

   (c) M defined by $a\,M\,b$ = larger of a and b

   (d) m defined by $a\,m\,b$ = smaller of a and b

   (e) @ defined by a @ $b = a^b$

2. Which pairs of operations in Exercise 1 are distributive over one another?

3. Let * be an operation on a set S and $A,\ B \subseteq S$. Prove that if A and B are both closed under *, then $A \cap B$ is also closed under *, but $A \cup B$ need not be.

4. How can you pick out the identity of an operation from its table?

5. Define a * b by $\mid a - b \mid$, the absolute value of a - b. Which properties does * have on the set of natural numbers, ℕ?

11.2 Algebraic Systems

An algebraic system is a mathematical system consisting of a set called the domain and one or more operations on the domain. If V is the domain and $*_1, *_2, \ldots, *_n$ are the operations, $[V; *_1, *_2, \ldots, *_n]$ denotes the mathematical system. If the context is clear, this notation is abbreviated to V.

Example 11.2.1.

(a) Let B^* be the set of all finite strings of 0's and 1's including the null (or empty) string, λ. An algebraic system is obtained by adding the operation of concatenation. The concatenation of two strings is simply the linking of the two strings together in the order indicated. The concatenation of strings a with b is denoted $a <> b$. For example, "01101" <> "101" = "01101101" and λ <> "100" = "100". Note that concatenation is an associative operation and that λ is the identity for concatenation.

Note on Notation: There isn't a standard symbol for concatenation. We have chosen <> to be consistant with the notation used in *Mathematica* for the **StringJoin** function, which does concatenation. Many programming languages use the plus sign for concatenation, but others use & or ||.

(b) Let M be any nonempty set and let * be any operation on M that is associative and has in identity in M. Our second example might seem strange, but we include it to illustrate a point. The algebraic system $[B^*; <>]$ is a special case of $[M; *]$. Most of us are much more comfortable with B^* than with M. No doubt, the reason is that the elements in B^* are more concrete. We know what they look like and exactly how they are combined. The description of M is so vague that we don't even know what the elements are, much less how they are combined. Why would anyone want to study M? The reason is related to this question: What theorems are of interest in an algebraic system? Answering this question is one of our main objectives in this chapter. Certain properties of algebraic systems are called algebraic properties, and any theorem that says something about the algebraic properties of a system would be of interest. The ability to identify what is algebraic and what isn't is one of the skills that you should learn from this chapter.

Now, back to the question of why we study M. Our answer is to illustrate the usefulness of M with a theorem about M.

Theorem 11.2.1. *If a, b are elements of M and $a * b = b * a$, then $(a * b) * (a * b) = (a * a) * (b * b)$.*

Proof:

$$\begin{aligned}(a*b)*(a*b) &= a*(b*(a*b)) && \text{Why?}\\ &= a*((b*a)*b) && \text{Why?}\\ &= a*((a*b)*b) && \text{Why?}\\ &= a*(a*(b*b)) && \text{Why?}\\ &= (a*a)*(b*b) && \text{Why?}\end{aligned}$$

The power of this theorem is that it can be applied to any algebraic system that M describes. Since B^* is one such system, we can apply Theorem 11.2.1 to any two strings that commute—for example, 01 and 0101. Although a special case of this theorem could have been proven for B^*, it would not have been any easier to prove, and it would not have given us any insight into other special cases of M .

Example 11.2.2. Consider the set of 2×2 real matrices, $M_{2\times 2}(\mathbb{R})$, with the operation of matrix multiplication. In this context, Theorem 11.2.1 can be interpreted as saying that if $A B = B A$, then $(A B)^2 = A^2 B^2$. One pair of matrices that this theorem applies to is $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ and $\begin{pmatrix} 3 & -4 \\ -4 & 3 \end{pmatrix}$.

LEVELS OF ABSTRACTION

One of the fundamental tools in mathematics is abstraction. There are three levels of abstraction that we will identify for algebraic systems: concrete, axiomatic, and universal.

Concrete Level. Almost all of the mathematics that you have done in the past was at the concrete level. As a rule, if you can give examples of a few typical elements of the domain and describe how the operations act on them, you are describing a concrete algebraic system. Two examples of concrete systems are B^* and $M_{2\times 2}(\mathbb{R})$. A few others are:

(a) The integers with addition. Of course, addition isn't the only standard operation that we could include. Technically, if we were to add multiplication, we would have a different system.

(b) The subsets of the natural numbers, with union, intersection, and complementation.

(c) The complex numbers with addition and multiplication.

Axiomatic Level. The next level of abstraction is the axiomatic level. At this level, the elements of the domain are not specified, but certain axioms are stated about the number of operations and their properties. The system that we called M is an axiomatic system. Some combinations of axioms are so common that a name is given to any algebraic system to which they apply. Any system with the properties of M is called a *monoid*. The study of M would be called monoid theory. The assumptions that we made about M, associativity and the existence of an identity, are called the monoid axioms. One of your few brushes with the axiomatic level may have been in your elementary algebra course. Many algebra texts identify the properties of the real numbers with addition and multiplication as the field axioms. As we will see in Chapter 16, "Rings and Fields," the real numbers share these axioms with other concrete systems, all of which are called fields.

Universal Level. The final level of abstraction is the universal level. There are certain concepts, called universal algebra concepts, that can be applied to the study of all algebraic systems. Although a purely universal approach to algebra would be much too abstract for our purposes, defining concepts at this level should make it easier to organize the various algebraic theories in your own mind. In this chapter, we will consider the concepts of isomorphism, subsystem, and direct product.

GROUPS

To illustrate the axiomatic level and the universal concepts, we will consider yet another kind of axiomatic system, the group. In Chapter 5 we noted that the simplest equation in matrix algebra that we are often called upon to solve is $A X = B$, where A and B are known square matrices and X is an unknown matrix. To solve this equation, we need the associative, identity, and inverse laws. We call the systems that have these properties groups.

Definition: Group. *A group consists of a nonempty set G and an operation $*$ on G satisfying the properties*

(a) $*$ is associative on G: $(a*b)*c = a*(b*c)$ for all $a, b, c \in G$.

(b) There exists an identity element, $e \in G$ such that $a*e = e*a = a$ for all $a \in G$.

(c) For all $a \in G$, there exists an inverse, there exist $b \in G$ such that $a*b = b*a = e$.

A group is usually denoted by its set's name, G, or occasionally by $[G; *]$ to emphasize the operation. At the concrete level, most sets have a standard operation associated with them that will form a group. As we will see below, the integers with addition is a group. Therefore, in group theory $\mathbb{Z}$ always stands for $[\mathbb{Z}; +]$.

Generic Symbols. At the axiomatic and universal levels, there are often symbols that have a special meaning attached to them. In group theory, the letter e is used to denote the identity element of whatever group is being discussed. A little later, we will prove that the inverse of a group element, a, is unique and it is inverse is usually denoted a^{-1} and is read "a inverse." When a concrete group is discussed, these symbols are dropped in favor of concrete symbols. These concrete symbols may or may not be similar to the generic symbols. For example, the identity element of the group of integers is 0, and the inverse of n is denoted by $-n$, the additive inverse of n.

The asterisk could also be considered a generic symbol since it is used to denote operations on the axiomatic level.

Example 11.2.3.

(a) The integers with addition is a group. We know that addition is associative. Zero is the identity for addition: $0 + n = n + 0 = n$ for all integers n. The additive inverse of any integer is obtained by negating it. Thus the inverse of n is $-n$.

(b) The integers with multiplication is not a group. Although multiplication is associative and 1 is the identity for multiplication, not all integers have a multiplicative inverse in $\mathbb{Z}$. For example, the multiplicative inverse of 10 is $\frac{1}{10}$, but $\frac{1}{10}$ is not an integer.

(c) The power set of any set U with the operation of symmetric difference, $\oplus$, is a group. If A and B are sets, then $A \oplus B = (A \bigcup B) - (A \bigcap B)$. We will leave it to the reader to prove that $\oplus$ is associative over $\mathcal{P}(U)$. The identity of the group is the empty set: $A \oplus \emptyset = A$. Every set is its own inverse since $A \oplus A = \emptyset$. Note that $\mathcal{P}(U)$ is not a group with union or intersection.

Definition: Abelian Group. *A group is abelian if its operation is commutative.*

Most of the groups that we will discuss in this book will be abelian. The term abelian is used to honor the Norwegian mathematician N. Abel (1802-29), who helped develop group theory.

Norwegian Stamp honoring Abel

EXERCISES FOR SECTION 11.2

A Exercises

1. Discuss the analogy between the terms generic and concrete for algebraic systems and the terms generic and trade for prescription drugs.

2. Discuss the connection between groups and monoids. Is every monoid a group? Is every group a monoid?

3. Which of the following are groups?

(a) B^* with concatenation (Example 11.2.1a).

(b) $M_{2\times 3}(\mathbb{R})$ with matrix addition.

(c) $M_{2\times 3}(\mathbb{R})$ with matrix multiplication.

(d) The positive real numbers, $\mathbb{R}^+$, with multiplication.

(e) The nonzero real numbers, $\mathbb{R}^*$, with multiplication.

(f) $\{1, -1\}$ with multiplication.

(g) The positive integers with the operation M defined by $a\,M\,b =$ larger of a and b.

4. Prove that, $\oplus$, defined by $A \oplus B = (A \cup B) - (A \cap B)$ is an associative operation on $\mathcal{P}(U)$.

5. The following problem supplies an example of a non-abelian group. A rook matrix is a matrix that has only 0's and 1's as entries such that each row has exactly one 1 and each column has exactly one 1. The term rook matrix is derived from the fact that each rook matrix represents the placement of n rooks on an $n\times n$ chessboard such that none of the rooks can attack one another. A rook in chess can move only vertically or horizontally, but not diagonally. Let R_n be the set of $n\times n$ rook matrices. There are six 3×3 rook matrices:

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad R_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad R_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$F_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad F_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad F_3 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

(a) List the 2×2 rook matrices. They form a group, R_2, under matrix multiplication. Write out the multiplication table. Is the group abelian?

(b) Write out the multiplication table for R_3 . This is another group. Is it abelian?

(c) How many 4×4 rook matrices are there? How many $n\times n$ rook matrices are there?

6. For each of the following sets, identify the standard operation that results in a group. What is the identity of each group?

(a) The set of all 2×2 matrices with real entries and nonzero determinants.

(b) The set of 2×3 matrices with rational entries.

B Exercises

7. Let $V = \{e, a, b, c\}$. Let $*$ be defined (partially) by $x * x = e$ for all $x \in V$. Write a complete table for $*$ so that $[V; *]$ is a group.

11.3 Some General Properties of Groups

In this section, we will present some of the most basic theorems of group theory. Keep in mind that each of these theorems tells us something about every group. We will illustrate this point at the close of the section.

Theorem 11.3.1. *The identity of a group is unique.*

One difficulty that students often encounter is how to get started in proving a theorem like this. The difficulty is certainly not in the theorem's complexity. Before actually starting the proof, we rephrase the theorem so that the implication it states is clear.

Theorem 11.3.1 *(Rephrased). If G = $[G; *]$ is a group and e is an identity of G, then no other element of G is an identity of G.*

Proof (Indirect): Suppose that $f \in G$, $f \neq e$, and f is an identity of G. We will show that $f = e$, a contradiction, which completes the proof:

$f = f * e$ Since e is an identity.

$= e.$ Since f is an identity. ■

Theorem 11.3.2. *The inverse of any element of a group is unique.*

The same problem is encountered here as in the previous theorem. We will leave it to the reader to rephrase this theorem. The proof is also left to the reader to write out in detail. Here is a hint: If b and c are both inverses of a, then you can prove that $b = c$. If you have difficulty with this proof, note that we have already proven it in a concrete setting in Chapter 5.

The significance of Theorem 11.3.2 is that we can refer to the inverse of an element without ambiguity. The notation for the inverse of a is usually a^{-1}. (note the exception below).

Example 11.3.1.

(a) In any group, e^{-1} is the inverse of the identity e, which always is e.

(b) $(a^{-1})^{-1}$ is the inverse of a^{-1} , which is always equal to a (see Theorem 11.3.3 below).

(c) $(x*y*z)^{-1}$ is the inverse of $x * y * z$.

(d) In a concrete group with an operation that is based on addition, the inverse of a is usually written $-a$. For example, the inverse of $k - 3$ in the group $[\mathbb{Z}; +]$ is written $-(k - 3) = 3 - k$. In the group of 2×2 matrices over the real numbers under matrix addition, the inverse of $\begin{pmatrix} 4 & 1 \\ 1 & -3 \end{pmatrix}$ is written $-\begin{pmatrix} 4 & 1 \\ 1 & -3 \end{pmatrix}$, which equals $\begin{pmatrix} -4 & -1 \\ -1 & 3 \end{pmatrix}$.

Theorem 11.3.3. *If a is an element of group G, then $\left(a^{-1}\right)^{-1} = a$.*

Theorem 11.3.3 (Rephrased). *If a has inverse b and b has inverse c, then $a = c$.*

Proof:

$a = a * (b * c)$ because c is the inverse of b

$= (a * b) * c$ why?

$= e * c$ why?

$= c.$ by the identity property of e. ■

Theorem 11.3.4. *If a and b are elements of group G, then $(a * b)^{-1} = b^{-1} * a^{-1}$*

Note: This theorem simply gives you a formula for the inverse of a * b. This formula should be familiar. In Chapter 5 we saw that if A and B are invertible matrices, then $(A\,B)^{-1} = B^{-1}\,A^{-1}$.

Proof: Let $x = b^{-1} * a^{-1}$. We will prove that x inverts $a * b$. Since we know that the inverse is unique, we will have prove the theorem.

$$\begin{aligned}(a * b) * x &= (a * b) * (b^{-1} * a^{-1}) \\ &= a * (b * (b^{-1} * a^{-1})) \\ &= a * ((b * b^{-1}) * a^{-1}) \\ &= a * (e * a^{-1}) \\ &= a * a^{-1} \\ &= e\end{aligned}$$

Similarly, $x * (a * b) = e$; therefore, $(a * b)^{-1} = x = b^{-1} * a^{-1}$ ■

Theorem 11.3.5. Cancellation Laws. *If a, b, and c are elements of group G, both a * b = a * c and b * a = c * a imply that b = c.*

Proof: Since $a * b = a * c$, we can operate on both $a * b$ and $a * c$ on the left with a^{-1} :

$$a^{-1} * (a * b) = a^{-1} * (a * c)$$

Applying the associative property to both sides we get

$$(a^{-1} * a) * b = (a^{-1} * a) * c$$

or

$$e * b = e * c$$

and finally

$$b = c.$$

This completes the proof of the left cancellation law. The right law can be proven in exactly the same way. ■

Theorem 11.3.6. Linear Equations in a Group. *If G is a group and a, b, ∈ G, the equation $a * x = b$ has a unique solution, $x = a^{-1} * b$. In addition, the equation $x * a = b$ has a unique solution, $x = b * a^{-1}$.*

Proof: (for $a * x = b$):

$$\begin{aligned} a*x &= b \\ &= e * b \\ &= (a* a^{-1}) * b \\ &= a * (a^{-1} * b) \end{aligned}$$

By the cancellation law, we can conclude that $x = a^{-1} * b$.

If c and d are two solutions of the equation $a * x = b$, then $a * c = b = a * d$ and, by the cancellation law, $c = d$. This verifies that $a^{-1} * b$ is the only solution of $a * x = b$. ■

Note: Our proof of Theorem 11.3.6 was analogous to solving $4x = 9$ in the following way:

$$4x = 9 = \left(4 \cdot \tfrac{1}{4}\right) 9 = 4\left(\tfrac{1}{4}\, 9\right)$$

Therefore, by cancelling 4,

$$x = \tfrac{1}{4} \cdot 9 = \tfrac{9}{4}.$$

Exponentiation in a Group

If a is an element of a group G, then we establish the notation that

$$a * a = a^2$$
$$a*a*a = a^3$$
etc.

In addition, we allow negative exponent and define, for example, $a^{-2} = (a^2)^{-1}$

Although this should be clear, proving exponentiation properties requires a more precise recursive definition:

Definition: Exponentiation in a Group. *For $n \geq 0$, define a^n recursively by $a^0 = e$ and if $n > 0$, $a^n = a^{n-1} * a$. Also, if $n > 1$, $a^{-n} = (a^n)^{-1}$.*

Example 11.3.2.

(a) In the group of positive real numbers with multiplication,

$$5^3 = 5^2 \cdot 5 = (5^1 \cdot 5) \cdot 5 = ((5^0 \cdot 5) \cdot 5) \cdot 5 = ((1 \cdot 5) \cdot 5) \cdot 5 = 5 \cdot 5 \cdot 5 = 125.$$

and

$$5^{-3} = (125)^{-1} = \tfrac{1}{125}$$

(b) In a group with addition, we use a different form of notation, reflecting the fact that in addition repeated terms are multiples, not powers. For example, in [$\mathbb{Z}$; +], $a + a$ is written as $2a$, $a + a + a$ is written as $3a$, etc. The inverse of a multiple of a such as $-(a + a + a + a + a) = -(5a)$ is written as $(-5)a$.

Although we define, for example, $a^5 = a^4 * a$, we need to be able to extract the single factor on the left. The following lemma justifies doing precisely that.

Lemma. *Let G be a group. If $b \in G$ and $n \geq 0$, then $b^{n+1} = b * b^n$, and hence $b * b^n = b^n * b$.*

Proof (by induction): If $n = 0$,

$$\begin{aligned} b^1 &= b^0 * b && \text{by the definition of exponentiation} \\ &= e * b && \text{basis for exponentiation} \\ &= b * e && \text{identity property} \\ &= b * b^0 && \text{basis for exponentiation} \end{aligned}$$

Now assume the formula of the lemma is true for some $n \geq 0$,

$$\begin{aligned} b^{(n+1)+1} &= b^{(n+1)} * b && \text{by the definition of exponentiation} \\ &= (b * b^n) * b && \text{by the induction hypothesis} \\ &= b * (b^n * b) && \text{associativity} \\ &= b * (b^{n+1}) && \text{definition of exponentiation} \blacksquare \end{aligned}$$

Based on the definitions for exponentiation above, there are several properties that can be proven. They are all identical to the exponentiation properties from elementary algebra.

Theorem 11.3.7. Properties of Exponentiation. *If a is an element of a group G, and n and m are integers,*

(a) $a^{-n} = \left(a^{-1}\right)^n$ *and hence* $(a^n)^{-1} = \left(a^{-1}\right)^n$

(b) $a^{n+m} = a^n * a^m$

(c) $(a^n)^m = a^{n m}$

We will leave the proofs of these properties to the interested reader. All three parts can be done by induction. For example the proof of (b) would start by defining the proposition $p(m)$, $m \geq 0$, to be $a^{n+m} = a^n * a^m$ for all n. The basis is $p(0)$: $a^{n+0} = a^n * a^0$.

Our final theorem is the only one that contains a hypothesis about the group in question. The theorem only applies to finite groups.

Theorem 11.3.8. *If G is a finite group,* $|G| = n$, *and a is an element of G, then there exists a positive integer m such that* $a^m = e$ *and* $m \leq n$.

Proof: Consider the list $a, a^2, \ldots, a^{n+1}$. Since there are $n + 1$ elements of G in this list, there must be some duplication. Suppose that $a^p = a^q$, with $p < q$. Let $m = q - p$. Then

$$a^m = a^{q-p} = a^q * a^{-p} = a^q * (a^p)^{-1} = a^q * (a^q)^{-1} = e$$

Furthermore, since $1 \leq p < q \leq n + 1$, $m = q - p \leq n$. ■

Consider the concrete group [$\mathbb{Z}$; +]. All of the theorems that we have stated in this section except for the last one say something about $\mathbb{Z}$. Among the facts that we conclude from the theorems about $\mathbb{Z}$ are:

Since the inverse of 5 is -5, the inverse of -5 is 5.

The inverse of $-6 + 71$ is $-(71) + -(-6) = -71 + 6$.

The solution of $12 + x = 22$ is $x = -12 + 22$.

$-4\,(6) + 2\,(6) = (-4 + 2)\,(6) = -2\,(6) = -(2)\,(6))$.

$7\,(4\,(3)) = (7 \cdot 4)\,(3) = 28\,(3)$ (twenty-eight 3s).

EXERCISES FOR SECTION 11.3

A Exercises

1. Let [G; $*$] be a group and a be an element of G. Define $f : G \to G$ by $f(x) = a * x$.

   (a) Prove that f is a bijection.

   (b) On the basis of part a, describe a set of bijections on the set of integers.

2. Rephrase Theorem 11.3.2 and write out a clear proof.

3. Prove by induction on n that if $a_1, a_2, \ldots, a_n$ are elements of a group G, $n \geq 2$, then

   $$(a_1 * a_2 * \cdots * a_n)^{-1} = {a_n}^{-1} * \cdots * {a_2}^{-1} * {a_1}^{-1}.$$

   Interpret this result in terms of [$\mathbb{Z}$; +] and [$\mathbb{R}$; $*$].

4. True or false? If a, b, c are elements of a group G, and $a * b = c * a$, then $b = c$. Explain your answer.

5. Prove Theorem 11.3.7.

6. Each of the following facts can be derived by identifying a certain group and then applying one of the theorems of this section to it. For each fact, list the group and the theorem that are used.

(a) $\left(\frac{1}{3}\right) 5$ is the only solution of $3\,x = 5$.

(b) $-(-(-18)) = -18$.

(c) If $A,\ B,\ C$ are 3×3 matrices over the real numbers, with $A + B = A + C$, then $B = C$.

(d) There is only one subset of the natural numbers for which $K \oplus A = A$ for every $A \subseteq N$.

11.4 Greatest Common Divisors and $\mathbb{Z}_n$, the Integers Modulo n

In this section introduce the greatest common divisor operation and will introduce an important family of concrete groups.

Greatest Common Divisors

We start with a theorem about integer division that is intuitively clear. We leave the proof as an optional exercise.

The Division Property for Integers. *If $m,\ n \in \mathbb{Z}$, $n > 0$, then there exist two unique integers, q (quotient) and r (remainder), such that $m = n q + r$ and $0 \leq r < n$.*

Note: The division property says that if m is divided by n, you will obtain a quotient and a remainder, where the remainder is less than n. This is a fact that most elementary school students learn when they are introduced to long division. In doing the division problem $1986 \div 97$, you obtain a quotient of 20 and a remainder of 46. This result could either be written $\frac{1986}{97} = 20 + \frac{46}{97}$ or $1986 = 97 \cdot 20 + 46$. The later form is how the division property is normally expressed.

If $r = 0$, i. e., $a = b q$, then all of the following say the same thing

b divides a
a is a multiple of b
b is a factor of a
b is a divisor of a

Notation We use the notation $b \mid a$ if b divides a. For example $2 \mid 18$ and $9 \mid 18$, but $4 \nmid 18$

Caution: Don't confuse the "divides" symbol with the "divided by" symbol. The former is vertical while the later is slanted. Notice that the statement $2 \mid 18$ is related to the fact that $18/2$ is a whole number.

> ***Definition: Greatest Common Divisor.*** *Given two integers, a and b, not both zero. The greatest common divisor of a and b is the integer g such that $g \mid a$, $g \mid b$, and*
>
> $$c \mid a \text{ and } c \mid b \Rightarrow c \mid g$$

A little simpler way to think of $\gcd(a,\ b)$ is as the largest positive integer that is a divisor of both a and b.

For small numbers, a simple way to determine the greatest common divisior is to use factorization. For example if we want the greatest common divisor of 660 and 350, you can factor the two integers: $660 = 2^2 \times 3 \times 5 \times 11$ and $350 = 2 \times 5^2 \times 7$. Single factors of 2 and 5 are the only ones that appear in both factorizations, so the greatest common divisor is $2 \times 5 = 10$.

Relatively Prime Pairs. Some pairs of integers have no common divisors other than 1. Such pairs are called *relatively prime pairs*. For example, $128 = 2^7$ and $135 = 3^3\ 5$ are relatively prime. Notice that neither 128 nor 135 are primes. In general, a and b need not be prime in order to be relatively prime. However, if you start with a prime, like 23, for example, it will be relatively prime to everything but its multiples. This theorem, which we prove later generalizes this observation:

Theorem. *If p is a prime and a is any integer such that $p \nmid a$ then $\gcd(a,\ p) = 1$*

The Euclidean Algorithm

As early as Euclid's time it was known that factorization wasn't the best way to compute greatest common divisors.

The Euclidean Algorithm is based on the following properties of the greatest common divisor

$$\gcd(a, 0) = a \quad \text{for } a \neq 0$$
$$\gcd(a,\ b) = \gcd(b,\ r) \quad \text{if } b \neq 0 \text{ and } a = b q + r$$

To compute $\gcd(a, b)$, we divide b into a and get a remainder r such that $0 \leq r < |b|$. By the property above, $\gcd(a,\ b) = \gcd(b,\ r)$. We repeat the process until we get zero for a remainder. The last nonzero number that is the second entry in our pairs is the greatest common divisior. This is inevitable because the second number in each pair is smaller than the previous one.

Here is the computation to verify that $\gcd(99, 53) = 1$. At each line, the value of a is divided by the value of b. The quotient is placed on the next line along with the new value of a, which is the previous b; and the remainder, which is the new value of b.

q	a	b
−	99	53
1	53	46
1	46	7
6	7	4
1	4	3
1	3	1
3	1	0

If you were allowed to pick two numbers less than 100, which would you pick in order to force Euclid to work hardest? Here's a hint

q	a	b
–	34	21
1	21	13
1	13	8
1	8	5
1	5	3
1	3	2
1	2	1
2	1	0

For fixed values of a and b, consider integers of the form $a\,x + b\,y$ where x and y can be any two integers. For example if $a = 36$ and $b = 27$, some of these results are tabulated below with x values along the left column and the y values on top.

Notice any patterns? What is the smallest positive value the you see in this table? How is it connected to 36 and 27

y

x

*	−6	−5	−4	−3	−2	−1	0	1	2	3	4	5	6
−6	−378	−351	−324	−297	−270	−243	−216	−189	−162	−135	−108	−81	−54
−5	−342	−315	−288	−261	−234	−207	−180	−153	−126	−99	−72	−45	−18
−4	−306	−279	−252	−225	−198	−171	−144	−117	−90	−63	−36	−9	18
−3	−270	−243	−216	−189	−162	−135	−108	−81	−54	−27	0	27	54
−2	−234	−207	−180	−153	−126	−99	−72	−45	−18	9	36	63	90
−1	−198	−171	−144	−117	−90	−63	−36	−9	18	45	72	99	126
0	−162	−135	−108	−81	−54	−27	0	27	54	81	108	135	162
1	−126	−99	−72	−45	−18	9	36	63	90	117	144	171	198
2	−90	−63	−36	−9	18	45	72	99	126	153	180	207	234
3	−54	−27	0	27	54	81	108	135	162	189	216	243	270
4	−18	9	36	63	90	117	144	171	198	225	252	279	306
5	18	45	72	99	126	153	180	207	234	261	288	315	342
6	54	81	108	135	162	189	216	243	270	297	324	351	378

Theorem 11.4.1. *If a and b are positive integers, the smallest positive value of* $a\,x + b\,y$ *is the greatest common divisor of a and b,* $gcd(a, b)$**.**

Proof: If $g = \gcd(a, b)$, then $g \mid a$ and $g \mid b \Rightarrow g \mid (a\,x + b\,y)$ for any x and y, so $a\,x + b\,y$ can't be less than g. To show that g is exactly the least positive value, we show that g can be attained by extending the Euclidean Algorithm. Performing the extended algorithm involves building a table of numbers. There are many variations on the way that this table arranged, so if your book has this algorithm it may look slightly different.

The table for gcd(152,53) is below. In the "r" column, you will find 152 and 53, and then the successive remainders from division. So each number in "r" after the first two is the remainder after dividing the number immediately above it into the next number up. To the left of each remainder is the quotient from the division. So in this case the third row of the table tells us that $152 = 53 \times 2 + 46$. The last nonzero value in r is the greatest common divisor.

The "s" and "t" columns are new. The values of s and t in each row are maintained so that 152s + 53t is equal to the number in the "r" column. Notice that

$$152 = 152 \times 1 + 53 \times 0$$
$$53 = 152 \times 0 + 53 \times 1$$
$$46 = 152 \times 1 + 53\,(-2)$$
$$\ldots$$
$$1 = 152 \times 15 + 53\,(-43)$$
$$0 = 152\,(-53) + 53 \times 152$$

q	r	s	t
-	152	1	0
-	53	0	1
2	46	1	-2
1	7	-1	3
6	4	7	-20
1	3	-8	23
1	1	15	-43
3	0	-53	152

The next-to-last equation is what we're looking for in the end! The main problem is to identify how to determine these values after the first two rows. The first two rows in these columns will always be the same.

Let's look at the general case of computing gcd(a,b). If the s and t values in rows $i - 1$ and $i - 2$ are correct, we have

$$(A) \quad \begin{cases} a\, s_{i-2} + b\, t_{i-2} = r_{i-2} \\ a\, s_{i-1} + b\, t_{i-1} = r_{i-1} \end{cases}$$

In addition, we know that

$$\boldsymbol{r_{i-2} = r_{i-1}\, q_i + r_i \quad \Rightarrow \quad r_i = r_{i-2} - r_{i-1}\, q_i}$$

If you substitute the expressions for r_{i-1} and r_{i-2} from (A) into this last equation and then collect the a and b terms separately you get

$$r_i = a(s_{i-2} - q_i\, s_{i-1}) + b(t_{i-2} - q_i\, t_{i-1})$$

or

$$s_i = s_{i-2} - q_i\, s_{i-1} \quad \text{and} \quad t_i = t_{i-2} - q_i\, t_{i-1}$$

Look closely at the equations for r_i, s_i, and t_i. Their forms are all the same. With a little bit of practice you should be able to compute s and t values quickly.

Modular Arithmetic

If two numbers, a and b, share the same remainder after dividing by n. we say that they are congruent modulo n, denoted $a \equiv b \pmod{n}$. For example, $13 \equiv 38 \pmod{5}$ because $13 = 5 \cdot 2 + 3$ and $38 = 5 \cdot + 3$.

Modular Arithmetic. *If n is a positive integer, we define the operations of addition modulo n ($+_n$) and multiplication modulo n ($\times_n$) as follows. If $a, b \in \mathbb{Z}$,*

$$a +_n b = \text{the remainder after } a + b \text{ is divided by } n$$

$$a \times_n b = \text{the remainder after } a \cdot b \text{ is divided by } n.$$

Notes:

(a) The result of doing arithmetic modulo n is always an integer between 0 and $n - 1$, by the Division Property. This observation implies that $\{0, 1, \ldots, n-1\}$ is closed under modulo n arithmetic.

(b) It is always true that $a +_n b \equiv (a + b) \pmod{n}$ and $a \times_n b \equiv (a \cdot b) \pmod{n}$. For example, $4 +_7 5 = 2 \equiv 9 \pmod{7}$ and

$4 \times_7 5 \equiv 6 \equiv 20 \pmod{7}$.

(c) We will use the notation $\mathbb{Z}_n$ to denote the set $\{0, 1, 2, \ldots, n-1\}$.

Properties of Modular Arithmetic on $\mathbb{Z}_n$

Addition modulo n is always commutative and associative; 0 is the identity for $+_n$ and every element of $\mathbb{Z}_n$ has an additive inverse.

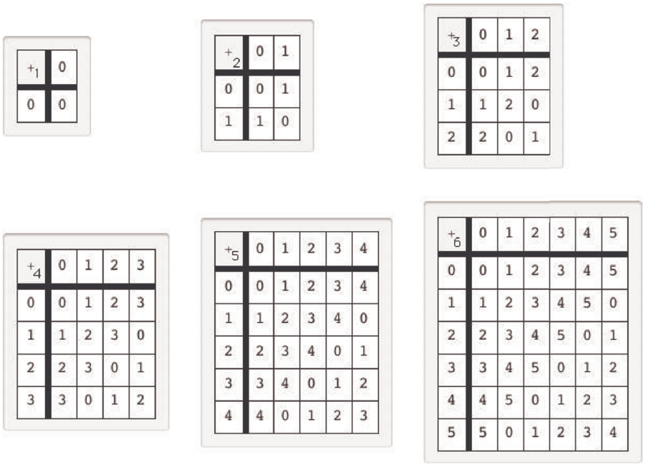
Multiplication modulo n is always commutative and associative, and 1 is the identity for $\times_n$.

Theorem 11.4.2. *If $a \in \mathbb{Z}_n$, $a \neq 0$, then the additive inverse of a is $n - a$.*

Proof: $a + (n - a) = n \equiv 0 \pmod{n}$, since $n = n \cdot 1 + 0$. Therefore, $a +_n (n - a) = 0$ ■

Note: The algebraic properties of $+_n$ and $\times_n$ on $\mathbb{Z}_n$ are identical to the properties of addition and multiplication on $\mathbb{Z}$.

The Group $\mathbb{Z}_n$. For each $n \geq 1$, $[\mathbb{Z}_n; +_n]$ is a group. Henceforth, we will use the abbreviated notation $\mathbb{Z}_n$ when referring to this group. Figure 11.4.1 contains the tables for $\mathbb{Z}_1$ through $\mathbb{Z}_6$.



$+_1$	0
0	0

$+_2$	0	1
0	0	1
1	1	0

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Figure 11.4.1
Addition tables for $\mathbb{Z}_n$, $1 \leq n \leq 6$.

Example 11.4.1.

(a) We are all somewhat familiar with $\mathbb{Z}_{12}$ since the hours of the day are counted using this group, except for the fact that 12 is used in place of 0. Military time uses the mod 24 system and does begin at 0. If someone started a four-hour trip at hour 21, the time at which she would arrive is $21 +_{24} 4 = 1$. If a satellite orbits the earth every four hours and starts its first orbit at hour 5, it would end its first orbit at time $5 +_{24} 4 = 9$. Its tenth orbit would end at $5 +_{24} 7 \times_{24} 4 = 9$ hours on the clock

(b) Virtually all computers represent unsigned integers in binary form with a fixed number of digits. A very small computer might reserve seven bits to store the value of an integer. There are only 2^7 different values that can be stored in seven bits. Since the smallest value is 0, represented as 0000000, the maximum value will be $2^7 - 1 = 127$, represented as 1111111. When a command is given to add two integer values, and the two values have a sum of 128 or more, overflow occurs. For example, if we try to add 56 and 95, the sum is an eight-digit binary integer 10010111. One common procedure is to retain the seven lowest-ordered digits. The result of adding 56 and 95 would be $0010111_{\text{two}} = 23 \equiv 56 + 95 \pmod{128}$. Integer arithmetic with this computer would actually be modulo 128 arithmetic.

Mathematica Note

In *Mathematica* you can get the gcd of two numbers using the function **GCD**:

```
GCD[660, 350]
```

```
10
```

A related function, **ExtendedGCD**, provides the x and y values guaranteed in Theorem 11.4.2.

```
ExtendedGCD[1001, 231]
```

```
{77, {1, -4}}
```

Most computer languages have a "mod" function that computes the remainder when one integer is divided by another. *Mathematica* is no exception. To determine the remainder upon dividing 1986 by 97 we can evaluate

```
Mod[1986, 97]
```

```
46
```

A mod 6 addition function can be defined based on **Mod** with the following input:

```
Plus6[a_, b_] := Mod[a + b, 6]
```

There is a free package called *AbstractAlgebra* that is available at https://sites.google.com/site/eaamhl/eaam. It contains a function that will generate the operation tables, also called *Cayley Tables,* such you see in Figure 11.4.1. First load the package, as instructed:

```
<< AbstractAlgebra`Master`
```

We can form a the group $\mathbb{Z}_6$ using the **FormGroupoid** function:

```
G = FormGroupoid[Range[0, 5], Plus6]
```

Groupoid({0, 1, 2, 3, 4, 5}, −Operation−)

Then the function called **CayleyTable** generates the table for the group $\mathbb{Z}_6$:

```
CayleyTable[G, BodyColored → False,
 HeadingsColored → False, ShowExtraCayleyInformation → False]
```

TheGroup

y

x

*	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Note: The rules **BodyColored → False, HeadingsColored → False, ShowExtraCayleyInformation → False** are included in the input above for easier black and white readability. They would not be normally included when using **CayleyTable**.

It's actually even easier to generate these tables because the family of $\mathbb{Z}_n$'s is part of the package. Here is the table for $\mathbb{Z}_9$:

```
CayleyTable[Z[9], BodyColored → False,
 HeadingsColored → False, ShowExtraCayleyInformation → False]
```

Z[9]

y

x

+	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

Sage Note

In Sage, `gcd` is the greatest common divisor function. It can be used in two ways. For the gcd of 2343 and 4319 we can evaluate the expression `gcd(2343,4319)`. If we are working with a fixed modulus m that has a value established in your Sage session, the expression `m.gcd(k)` to compute the gcd of m and any integer value k.

Sage has some extremely powerful tool for working with groups. The integers modulo n are represented by the expression `Integers(n)` and the addition and multiplications tables can be generated as follows.

```
R = Integers(6)
print R.addition_table('elements')
print R.multiplication_table('elements')
```

```
        +  0 1 2 3 4 5
         +------------
        0| 0 1 2 3 4 5
        1| 1 2 3 4 5 0
        2| 2 3 4 5 0 1
        3| 3 4 5 0 1 2
        4| 4 5 0 1 2 3
        5| 5 0 1 2 3 4

        *  0 1 2 3 4 5
         +------------
        0| 0 0 0 0 0 0
        1| 0 1 2 3 4 5
        2| 0 2 4 0 2 4
        3| 0 3 0 3 0 3
        4| 0 4 2 0 4 2
        5| 0 5 4 3 2 1
```

Once we have assigned `R` a value of `Integers(6)`, we can do calculations by wrapping `R()` around the integers 0 through 5. Here is a list containing the mod 6 sum and product, respectively, of 5 and 4:

```
[R(5)+R(4), R(5)*R(4)]
      [3, 2]
```

EXERCISES FOR SECTION 11.4

A Exercises

1. Determine the greatest common divisors of the following pairs of integers without using any computational assistance.

   (a) $2^3\,3^2\,5$ and $2^2\,3\;5^2\,7$

   (b) $2 \times 3 \times 4 \times 5 \times 6 \times 7$ and $3 \times 5 \times 7 \times 9 \times 11 \times 13$

   (c) 19^4 and 19^5

   (d) 12112 and 0

2. Find all possible values of the following, assuming that m is a positive integer.

   (a) $\gcd(m+1, m)$

   (b) $\gcd(m+2, m)$

   (c) $\gcd(m+4, m)$

3. Calculate:

   (a) $7 +_8 3$

   (b) $7 \times_8 3$

   (c) $4 \times_8 4$

   (d) $10 +_{12} 2$

   (e) $6 \times_8 2 +_8 6 \times_8 5$

   (f) $6 \times_8 (2 +_8 5)$

   (g) $3 \times_5 3 \times_5 3 \times_5 3 \equiv 3^4 \pmod 5$

   (h) $2 \times_{11} 7$

   (i) $2 \times_{14} 7$

4. List the additive inverses of the following elements:

(a) $4, 6, 9$ in $\mathbb{Z}_{10}$

(b) $16, 25, 40$ in $\mathbb{Z}_{50}$

5. In the group $\mathbb{Z}_{11}$, what are:

(a) 3(4)?

(b) 36(4)?

(c) How could you efficiently compute $m(4), m \in \mathbb{Z}$?

6. Prove that $\{1, 2, 3, 4\}$ is a group under the operation $\times_5$.

7. A student is asked to solve the following equations under the requirement that all arithmetic should be done in $\mathbb{Z}_2$. List all solutions.

(a) $x^2 + 1 = 0$.

(b) $x^2 + x + 1 = 0$.

8. Determine the solutions of the same equations as in Exercise 5 in $\mathbb{Z}_5$.

B Exercises

9. Prove the division property by induction on m.

10. Prove that congruence modulo n is an equivalence relation on the integers. Describe the set of equivalence classes that congruence modulo n defines.

11.5 Subsystems

The subsystem is a fundamental concept of algebra at the universal level.

Definition: Subsystem. *If* $[V;\, *_1,\, \ldots,\, *_n]$ *is an algebraic system of a certain kind and W is a subset of V, then W is a subsystem of V if* $[W;\, *_1,\, \ldots,\, *_n]$ *is an algebraic system of the same kind as V. The usual notation for "W is a subsystem of V" is* $W \leq V$.

Since the definition of a subsystem is at the universal level, we can cite examples of the concept of subsystems at both the axiomatic and concrete level.

Example 11.5.1

(a) (Axiomatic) If $[G;\, *]$ is a group, and H is a subset of G, then H is a subgroup of G if $[H;\, *]$ is a group.

(b) (Concrete) $U = \{-1, 1\}$ is a subgroup of $[\mathbb{R}^*; \cdot]$. Take the time now to write out the multiplication table of U and convince yourself that $[U; \cdot]$ is a group.

(c) (Concrete) The even integers, $2\,\mathbb{Z} = \{2\,k : k \text{ is an integer}\}$ is a subgroup of $[\mathbb{Z};\, +]$. Convince yourself of this fact.

(d) (Concrete) The set of nonnegative integers is not a subgroup of $[\mathbb{Z};\, +]$. All of the group axioms are true for this subset except one: no positive integer has a positive additive inverse. Therefore, the inverse property is not true. Note that every group axiom must be true for a subset to be a subgroup.

(e) (Axiomatic) If M is a monoid and P is a subset of M, then P is a submonoid of M if P is a monoid.

(f) (Concrete) If B^* is the set of strings of 0's and 1's of length zero or more with the operation of concatenation, then two examples of submonoids of B^* are: (i) the set of strings of even length, and (ii) the set of strings that contain no 0's. The set of strings of length less than 50 is not a submonoid because it isn't closed under concatenation. Why isn't the set of strings of length 50 or more a submonoid of B^*?

For the remainder of this section, we will concentrate on the properties of subgroups. The first order of business is to establish a systematic way of determining whether a subset of a group is a subgroup.

Theorem/Algorithm 11.5.1. *To determine whether H, a subset of group* $[G; *]$, *is a subgroup, it is sufficient to prove:*

(a) H is closed under $*$*; that is,* $a,\, b \in H \Rightarrow a * b \in H$;

(b) H contains the identity element for $*$*; and*

(c) H contains the inverse of each of its elements; that is, $a \in H \Rightarrow a^{-1} \in H$.

Proof: Our proof consists of verifying that if the three properties above are true, then all the axioms of a group are true for $[H\,;\, *]$. By Condition (a), $*$ can be considered an operation on H. The associative, identity, and inverse properties are the axioms that are needed. The identity and inverse properties are true by Conditions (b) and (c), respectively, leaving only the associative property. Since, $[G; *]$ is a group, $a * (b * c) = (a * b) * c$ for all $a,\, b,\, c \in G$. Certainly, if this equation is true for all choices of three elements from G, it will be true for all choices of three elements from H, since H is a subset of G. ■

For every group with at least two elements, there are at least two subgroups: they are the whole group and $\{e\}$. Since these two are automatic, they are not considered very interesting and are called the improper subgroups of the group; $\{e\}$ is sometimes referred to as the trivial subgroup. All other subgroups, if there are any, are called proper subgroups.

We can apply Theorem 11.5.1 at both the concrete and axiomatic levels.

Examples 11.5.2.

(a) (Concrete) We can verify that $2\,\mathbb{Z} \leq \mathbb{Z}$, as stated in Example 11.5.1. Whenever you want to discuss a subset, you must find some convenient way of describing its elements. An element of $2\,\mathbb{Z}$ can be described as 2 times an integer; that is, $a \in 2\,\mathbb{Z}$ is equivalent to $(\exists\, k)_{\mathbb{Z}}\,(a = 2\,k)$. Now we can verify that the three conditions of Theorem 11.5.1 are true for $2\mathbb{Z}$. First, if $a,\, b \in 2\,\mathbb{Z}$, then there exist $j,\, k \in \mathbb{Z}$ such that $a = 2\,j$ and $b = 2\,k$. A common error is to write something like $a = 2\,j$ and $b = 2\,j$. This would mean that $a = b$, which is not necessarily true. That is why two different variables are needed to describe a and b. Returning to our proof, we can add a and b:

$$a + b = 2\,j + 2\,k = 2\,(j + k).$$

Since $j + k$ is an integer, $a + b$ is an element of $2\,\mathbb{Z}$. Second, the identity, 0, belongs to $2\mathbb{Z}$ $(0 = 2\,(0))$. Finally, if $a \in 2\,\mathbb{Z}$ and $a = 2\,k$, $-a = -(2\,k) = 2\,(-k)$, and $-k \in \mathbb{Z}$, therefore, $-a \in 2\,\mathbb{Z}$. By Theorem 11.5.1, $2\,\mathbb{Z} \leq \mathbb{Z}$.

How would this argument change if you were asked to prove that $3\,\mathbb{Z} \leq \mathbb{Z}$? or $n\,\mathbb{Z} \leq \mathbb{Z},\ n \geq 2$?

(b) (Concrete) We can prove that $H = \{0,\, 3,\, 6,\, 9\}$ is a subgroup of $\mathbb{Z}_{12}$. First, for each ordered pair $(a,\, b) \in H \times H$, $a +_{12} b$ is in H. This can be checked without too much trouble since $|H \times H| = 16$. Thus we can conclude that H is closed under $+_{12}$. Second, $0 \in H$. Third, $-0 = 0, -3 = 9, -6 = 6$, and $-9 = 3$. Therefore, the inverse of each element in H is in H.

(c) (Axiomatic) If H and K are both subgroups of a group G, then $H \bigcap K$ is a subgroup of G. To justify this statement, we have no concrete information to work with, only the facts that $H \leq G$ and K ≤G. Our proof that $H \bigcap K \leq G$ reflects this and is an exercise in applying the definitions of intersection and subgroup, (i) If a and b are elements of H ⋂ K, then a and b both belong to H, and since $H \leq G$, $a * b$ must be an element of H. Similarly, $a * b \in K$; therefore, $a * b \in H \bigcap K$. (ii) The identity of G must belong to both H and K; hence it belongs to $H \bigcap K$. (iii) If $a \in H \bigcap K$, then $a \in H$, and since $H \leq G$, $a^{-1} \in H$. Similarly, $a^{-1} \in K$. Hence, by the theorem, $H \bigcap K \leq G$.

Now that this fact has been established, we can apply it to any pair of subgroups of any group. For example, since $2\mathbb{Z}$ and $3\mathbb{Z}$ are both subgroups of $[\mathbb{Z}; +]$, $2\mathbb{Z} \bigcap 3\mathbb{Z}$ is also a subgroup of $\mathbb{Z}$. Note that if $a \in 2\mathbb{Z} \bigcap 3\mathbb{Z}$, a must have a factor of 3; that is, there exists $k \in \mathbb{Z}$ such that $a = 3k$. In addition, a must be even, therefore k must be even. There exists $j \in \mathbb{Z}$ such that $k = 2j$, therefore $a = 3(2j) = 6j$. This shows that $2\mathbb{Z} \bigcap 3\mathbb{Z} \subseteq 6\mathbb{Z}$. The opposite containment can easily be established; therefore, $2\mathbb{Z} \bigcap 3\mathbb{Z} = 6\mathbb{Z}$.

Given a finite group, we can apply Theorem 11.3.7 to obtain a simpler condition for a subset to be a subgroup.

Theorem/Algorithm 11.5.2. *If $[G; *]$ is a finite group, H is a nonempty subset of G, and you can verify that H is closed under $*$, then H is a subgroup of G.*

Proof: In this proof, we demonstrate that Conditions (b) and (c) of Theorem 11.5.1 follow from the closure of H under $*$, which is Condition (a). First, select any element of H; call it β. The powers of β : $\beta^1, \beta^2, \beta^3, \ldots$ are all in H by the closure property. By Theorem 11.3.7, there exists m, $m \leq |G|$, such that $\beta^m = e$; hence $e \in H$. To prove that (c) is true, we let a be any element of H. If $a = e$, then a^{-1} is in H since $e^{-1} = e$. If $a \neq e$, $a^q = e$ for some q between 2 and $|G|$ and

$$e = a^q = a^{q-1} * a.$$

Therefore, $a^{-1} = a^{q-1}$, which belongs to H since $q - 1 \geq 1$. ■

Example 11.5.3 To determine whether $H_1 = \{0, 5, 10\}$ and $H_2 = \{0, 4, 8, 12\}$ are subgroups of $\mathbb{Z}_{15}$, we need only write out the addition tables (modulo 15) for these sets.

H_1

y

x

+	0	5	10
0	0	5	10
5	5	10	0
10	10	0	5

H_2

y

x

*	0	4	8	12
0	0	4	8	12
4	4	8	12	1
8	8	12	1	5
12	12	1	5	9

Note that H_1 is a subgroup of $\mathbb{Z}_{15}$. Since the interior of the addition table for H_2 contains elements that are outside of H_2 , H_2 is not a subgroup of $\mathbb{Z}_{15}$.

One kind of subgroup that merits special mention due to its simplicity is the cyclic subgroup.

Definition: Cyclic Subgroup Generated by an Element. *If G is a group and $a \in G$, the cyclic subgroup generated by a, (a), is the set of powers of a and their inverses:*

$$(a) = \{a^n : n \in \mathbb{Z}\}$$

A subgroup H is cyclic if there exists $a \in H$ such that $H = (a)$.

Definition: Cyclic Group. *A group G is cyclic if there exists $\beta \in G$ such that $(\beta) = G$.*

Note: If the operation on G is additive, then $(a) = \{(n)a : n \in \mathbb{Z}\}$.

Example 11.5.4.

(a) In $[\mathbb{R}; \cdot]$, $(2) = \{2^n : n \in \mathbb{Z}\} = \left\{\ldots, \frac{1}{16}, \frac{1}{8}, \frac{1}{4} \frac{1}{2}, 1, 2, 4, 8, 16, \ldots\right\}$.

(b) In $\mathbb{Z}_{15}$, $(6) = \{0, 3, 6, 9, 12\}$. If G is finite, you need list only the positive powers of a up to the first occurrence of the identity to obtain all of *(a)*. In $\mathbb{Z}_{15}$, the multiples of 6 are 6, $(2)6 = 12$, $(3)6 = 3$, $(4)6 = 9$, and $(5)6 = 0$. Note that $\{0, 3, 6, 9, 12\}$ is also (3),(9), and (12). This shows that a cyclic subgroup can have different generators.

If you want to list the cyclic subgroups of a group, the following theorem can save you some time.

Theorem 11.5.3. If a is an element of group G, then $(a) = (a^{-1})$. This is an easy way of seeing that (9) in $\mathbb{Z}_{15}$ equals (6), since $-6 = 9$.

EXERCISES FOR SECTION 11.5

A Exercises

1. Which of the following subsets of the real numbers is a subgroup of $[\mathbb{R}; +]$?

(a) the rational numbers

(b) the positive real numbers

(c) $\{k/2 \mid k \text{ is an integer}\}$

(d) $\{2^k \mid k \text{ is an integer}\}$

(e) $\{x \mid -100 \leq x \leq 100\}$

2. Describe in simpler terms the following subgroups of $\mathbb{Z}$:

(a) $5\mathbb{Z} \cap 4\mathbb{Z}$

(b) $4\mathbb{Z} \cap 6\mathbb{Z}$ (be careful)

(c) the only finite subgroup of $\mathbb{Z}$

3. Find at least two proper subgroups of R_3 , the set of 3×3 rook matrices (see Exercise 5 of Section 11.2).

4. Where should you place the following in Figure 11.5.1?

(a) e

(b) a^{-1}

(c) $x * y$

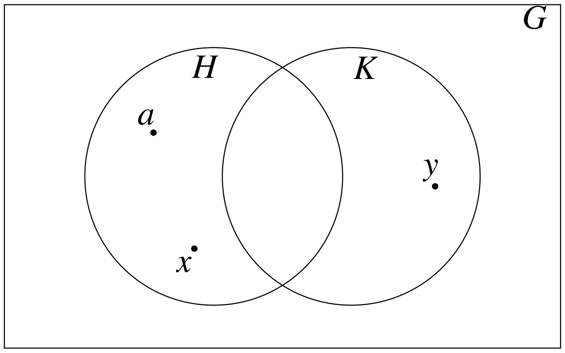


Figure 11.5.1

5. (a) List the cyclic subgroups of $\mathbb{Z}_6$ and draw an ordering diagram for

the relation "is a subset of" on these subgroups.

(b) Do the same for $\mathbb{Z}_{12}$.

(c) Do the same for $\mathbb{Z}_8$.

(d) On the basis of your results in parts a, b, and c, what would you expect if you did the same with $\mathbb{Z}_{24}$?

B Exercises

6. *Subgroups generated by subsets of a group*. The concept of a cyclic subgroup is a special case of the concept that we will discuss here. Let $[G; *]$ be a group and S a nonempty subset of G. Define the set (S) recursively by:

(i) If $a \in S$, then $a \in (S)$,

(ii) If $a,\ b \in (S)$, then $a * b \in (S)$, and

(iii) If $a \in (S)$, then $a^{-1} \in (S)$.

(a) By its definition, (S) has all of the properties needed to be a subgroup of G. The only thing that isn't obvious is that the identity of G is in (S). Prove that the identity of G is in (S).

(b) What is $(\{9,\ 15\})$ in $[\mathbb{Z};\ +]$?

(c) Prove that if $H \leq G$ and $S \subseteq H$, then $(S) \leq H$. This proves that (S) is contained in every subgroup of G that contains S; that is, $(S) = \bigcap_{\substack{S \subseteq H \\ H \leq G}} H$.

(d) Describe $(\{0.5,\ 3\})$ in $[\mathbb{R}^+; \cdot]$ and in $[\mathbb{R}; +]$.

(e) If $j,\ k \in \mathbb{Z}$, $(\{j,\ k\})$ is a cyclic subgroup of $\mathbb{Z}$. In terms of j and k, what is a generator of $(\{j,\ k\})$?

7. Prove that if $H, K \leq G$, and $H \cup K = G$, then $H = G$ or $K = G$. (Hint: Use an indirect argument.)

11.6 Direct Products

Our second universal algebraic concept lets us look in the opposite direction from subsystems. Direct products allow us to create larger systems. In the following definition, we avoid complicating the notation by not specifying how many operations the systems have.

Definition: Direct Product. *If* $[V_1; *_1, \diamond_1, \ldots], [V_2; *_2, \diamond_2, \ldots], \ldots, [V_1; *_n, \diamond_n, \ldots]$ *are algebraic systems of the same kind, then the direct product of these systems is* $V = V_1 \times V_2 \times \cdots \times V_n$ *, with operations defined below. The elements of V are n-tuples of the form* $(a_1, a_2, \ldots, a_n)$*, where* $a_k \in V_k$, $k = 1, \ldots, n$*. The systems* $V_1, V_2, \ldots, V_n$ *are called the factors of V. There are as many operations on V as there are on the factors. Each of these operations is defined componentwise:*

If $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in V$,

$$\begin{gathered}(a_1, a_2, \ldots, a_n) * (b_1, b_2, \ldots, b_n) = (a_1 *_1 b_1, a_2 *_2 b_2, \ldots, a_n *_n b_n)\\ (a_1, a_2, \ldots, a_n) \diamond (b_1, b_2, \ldots, b_n) = (a_1 \diamond_1 b_1, a_2 \diamond_2 b_2, \ldots, a_n \diamond_n b_n)\\ \vdots\end{gathered}$$

Example 11.6.1. Consider the monoids ℕ (the set of natural numbers with addition) and B^* (the set of finite strings of 0's and 1's with concatenation). The direct product of ℕ with B^* is a monoid. We illustrate its operation, which we will denote by $*$, with examples:

$$(4,\ 001) * (3,\ 11) = (4 + 3,\ 001 <> 11) = (7,\ 00111)$$

$$(0,\ 11010) * (3, 01) = (3,\ 1101001)$$

$$(0,\ \lambda) * (129,\ 00011) = (0 + 129,\ \lambda <> 00011) = (129,\ 00011)$$

$(2,\ 01) * (8,\ 10) = (10, 0110)$, and

$(8,\ 10) * (2,\ 01) = (10,\ 1001)$.

Note that our new monoid is not commutative. What is the identity for $*$?

Notes:

(a) On notation. If two or more consecutive factors in a direct product are identical, it is common to combine them using exponential notation. For example, $\mathbb{Z} \times \mathbb{Z} \times \mathbb{R}$ can be written $\mathbb{Z}^2 \times \mathbb{R}$, and $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ can be written $\mathbb{R}^4$. This is purely a notational convenience; no exponentiation is really taking place.

(b) In our definition of a direct product, the operations are called componentwise operations, and they are indeed operations on V. Consider $*$ above. If two n-tuples, a and b, are selected from V, the first components of a and b, a_1 and b_1 , are operated on with $*_1$ to obtain $a_1 *_1 b_1$, the first component of $a * b$. Note that since $*_1$ is an operation on V_1, $a_1 *_1 b_1$ is an element of V_1. Similarly, all other components of $a * b$, as they are defined, belong to their proper sets.

One significant fact about componentwise operations is that the components of the result can all be computed at the same time (concurrently). The time required to compute in a direct product can be reduced to a length of time that is not much longer than the maximum amount of time needed to compute in the factors (see Figure 11.6.1).

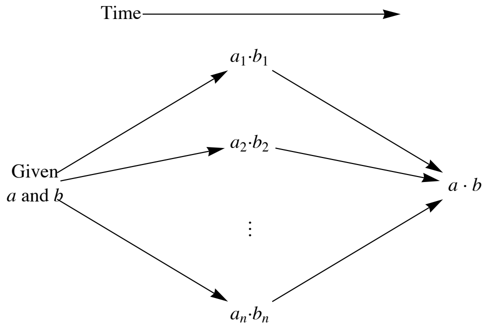


Figure 11.6.1
Concurrent calculation in a direct product.

(c) A direct product of algebraic systems is not always an algebraic system of the same type as its factors. This is due to the fact that certain axioms that are true for the factors may not be true for the set of n-tuples. This situation does not occur with groups however. You will find that whenever a new type of algebraic system is introduced, call it type T, one of the first theorems that is usually proven, if possible, is that the direct product of two or more systems of type T is a system of type T.

Theorem 11.6.1. *The direct product of two or more groups is a group; that is, the algebraic properties of a system obtained by taking the direct product of two or more groups includes the group axioms.*

We will only present the proof of this theorem for the direct product of two groups. Some slight revisions can be made to obtain a proof for any number of factors.

Proof: Stating that the direct product of two groups is a group is a short way of saying that if $[G_1; *_1]$ and $[G_2; *_2]$ are groups, then $[G_1 \times G_2; *]$ is also a group, where $*$ is the componentwise operation on $G_1 \times G_2$.

Associativity of $*$: If $a,\ b,\ c \in G_1 \times G_2$,

$$\begin{aligned} a * (b * c) &= (a_1, a_2) * ((b_1, b_2) * (c_1, c_2)) \\ &= (a_1, a_2) * (b_1 *_1 c_1, b_2 *_2 c_2) \\ &= (a_1 *_1 (b_1 *_1 c_1), a_2 *_2 (b_2 *_2 c_2)) \\ &= ((a_1 *_1 b_1) *_1 c_1, (a_2 *_2 b_2) *_2 c_2) \\ &= (a_1 *_1 b_1, a_2 *_2 b_2) * (c_1, c_2) \\ &= ((a_1, a_2) * (b_1, b_2)) * (c_1, c_2) \\ &= (a * b) * c \end{aligned}$$

Notice how the associativity property hinges on the associativity in each factor.

An identity for $*$: As you might expect, if e_1 and e_2 are identities for G_1 and G_2, respectively, then $e = (e_1,\ e_2)$ is the identity for $G_1 \times G_2$. If $a \in G_1 \times G_2$,

$$\begin{aligned} a * e &= (a_1, a_2) * (e_1,\ e_2) \\ &= (a_1 *_1 e_1, a_2 *_2 e_2) \\ &= (a_1, a_2) \\ &= a \end{aligned}$$

Similarly, $e * a = a$.

Inverses in $G_1 \times G_2$: The inverse of an element is determined componentwise $a^{-1} = (a_1, a_2)^{-1} = (a_1{}^{-1}, a_2{}^{-1})$. To verify, we compute $a * a^{-1}$:

$$\begin{aligned} a * a^{-1} &= (a_1, a_2) * (a_1{}^{-1}, a_2{}^{-1}) \\ &= (a_1 *_1 a_1{}^{-1}, a_2 *_2 a_2{}^{-1}) \\ &= (e_1,\ e_2) \\ &= e \end{aligned}$$

Similarly, $a^{-1} * a = e$. ■

Example 11.6.2.

(a) If $n \geq 2$, $\mathbb{Z}_2{}^n$, the direct product of n factors of $\mathbb{Z}_2$, is a group with 2^n elements. We will take a closer look at $\mathbb{Z}_2{}^3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. The elements of this group are triples of zeros and ones. Since the operation on $\mathbb{Z}_2$ is $+_2$, we will use the symbol $+$ for the operation on $\mathbb{Z}_2{}^3$. Two of the eight triples in the group are $a = (1,\ 0,\ 1)$ and $b = (0,\ 0,\ 1)$. Their "sum" is $a + b = (1 +_2 0,\ 0 +_2 0,\ 1 +_2 1) = (1,\ 0,\ 0)$. One interesting fact about this group is that each element is its own inverse. For example $a + a = (1,\ 0,\ 1) + (1,\ 0,\ 1) = (0,\ 0,\ 0)$; therefore $-a = a$. We use the additive notation for the inverse of a because we are using a form of addition. Note that $\{(0,\ 0,\ 0),\ (1,\ 0,\ 1)\}$ is a subgroup of $\mathbb{Z}_2{}^3$. Write out the "addition" table for this set and apply Theorem 11.5.2. The same can be said for any set consisting of $(0, 0, 0)$ and another element of $\mathbb{Z}_2{}^3$.

(b) The direct product of the positive real numbers with the integers modulo 4, $\mathbb{R}^+ \times \mathbb{Z}_4$ is an infinite group since one of its factors is infinite. The operations on the factors are multiplication and modular addition, so we will select the neutral symbol $\diamond$ for the operation on $\mathbb{R}^+ \times \mathbb{Z}_4$. If $a = (4,\ 3)$ and $b = (0.5,\ 2)$, then

$$a \diamond b = (4,\ 3) \diamond (0.5,\ 2) = (4 \cdot 0.5,\ 3 +_4 2) = (2,\ 1)$$

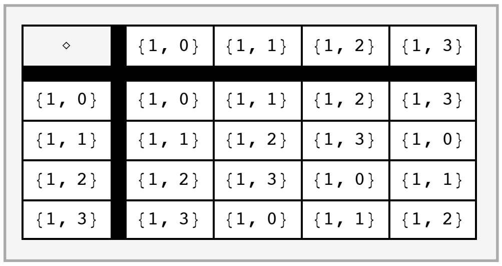
$$b^2 = b \diamond b = (0.5,\ 2) \diamond (0.5,\ 2) = (0.25,\ 0),$$

$$a^{-1} = (4^{-1}\ ,\ -3) = (0.25,\ 1) \quad \text{and}$$

$$b^{-1} = \left(0.5^{-1}\ ,\ -2\right) = (2,\ 2).$$

It would be incorrect to say that $\mathbb{Z}_4$ is a subgroup of $\mathbb{R}^+ \times \mathbb{Z}_4$, but there is a subgroup of the direct product that closely resembles $\mathbb{Z}_4$. It is $\{(1,\ 0),\ (1,\ 1),\ (1,\ 2),\ (1,\ 3)\}$. Its table is

"



◇	{1, 0}	{1, 1}	{1, 2}	{1, 3}
{1, 0}	{1, 0}	{1, 1}	{1, 2}	{1, 3}
{1, 1}	{1, 1}	{1, 2}	{1, 3}	{1, 0}
{1, 2}	{1, 2}	{1, 3}	{1, 0}	{1, 1}
{1, 3}	{1, 3}	{1, 0}	{1, 1}	{1, 2}

Imagine erasing $(1,)$ throughout the table and writing $+_4$ in place of $\diamond$. What would you get? We will explore this phenomenon in detail in the next section.

The whole direct product could be visualized as four parallel half-lines labeled 0, 1, 2, and 3 (Figure 11.6.2). On the kth line, the point that lies x units to the right of the zero mark would be (x, k). The set $\{(2^n, (n) 1) \mid n \in \mathbb{Z}\}$, which is plotted on Figure 11.6.2, is a subgroup of $\mathbb{R}^+ \times \mathbb{Z}_4$. What cyclic subgroup is it?

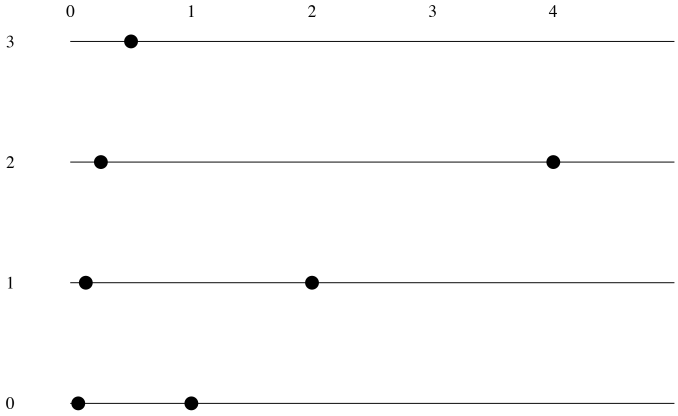


Figure 11.6.2
Graph of $\mathbb{R}^+ \times \mathbb{Z}_4$

The answer: $((2, 1))$ or $((j, 3))$.

A more conventional direct product is $\mathbb{R}^2$, the direct product of two factors of $[\mathbb{R}; +]$. The operation on $\mathbb{R}^2$ is componentwise addition; hence we will use + as the operation symbol for this group. You should be familiar with this operation, since it is identical to addition of 2×1 matrices. The Cartesian coordinate system can be used to visualize $\mathbb{R}^2$ geometrically. We plot the pair (s, t) on the plane in the usual way: s units along the x axis and t units along the y axis. There is a variety of different subgroups of $\mathbb{R}^2$, a few of which are:

(1) $\{(x, 0) \mid x \in \mathbb{R}\}$, all of the points on the x axis;

(2) $\{(x, y) \mid 2x - y = 0\}$, all of the points that are on the line 2x - y = 0;

(3) If $a, b \in \mathbb{R}$, $\{(x, y) \mid ax + by = 0\}$. The first two subgroups are special cases of this one, which represents any line that passes through the origin.

(4) $\{(x, y) \mid 2x - y = k, k \in \mathbb{Z}\}$, a set of lines that are parallel to $2x - y = 0$.

(5) $\{(n, 3n) \mid n \in \mathbb{Z}\}$, which is the only countable subgroup that we have listed.

We will leave it to the reader to verify that these sets are subgroups. We will only point out how the fourth example, call it H, is closed under "addition." If $a = (p, q)$ and $b = (s, t)$ and both belong to H, then $2p - q = j$ and $2s — t = k$, where both j and k are integers.

$$a + b = (p, q) + (s, t) = (p + s, q + t)$$

We can determine whether $a + b$ belongs to H by deciding whether or not $2(p + s) - (q + t)$ is an integer:

$$\begin{aligned}2(p + s) - (q + t) &= 2p + 2s - q - t\\ &= (2p - q) + (2s - t)\\ &= j + k\end{aligned}$$

which is an integer. This completes a proof that H is closed under the operation of $\mathbb{R}^2$.

Several useful facts can be stated in regards to the direct product of two or more groups. We will combine them into one theorem, which we will present with no proof. Parts a and c were derived for $n = 2$ in the proof of Theorem 11.6.1.

Theorem 11.6.2. If $G = G_1 \times G_2 \times \cdots \times G_n$ is a direct product of n groups and $(a_1, a_2, \ldots, a_n) \in G$, then:

(a) The identity of G is $(e_1, e_2, \ldots, e_n)$, where e_k, is the identity of G_k.

(b) $(a_1, a_2, \ldots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$.

(c) $(a_1, a_2, \ldots, a_n)^m = (a_1^m, a_2^m, \ldots, a_n^m)$ for all $m \in \mathbb{Z}$.

(d) G is abelian if and only if each of the factors $G_1, G_2, \ldots, G_n$ is abelian.

(e) If $H_1, H_2, \ldots, H_n$ are subgroups of the corresponding factors, then $H_1 \times H_2 \times \cdots \times H_n$ is a subgroup of G.

Not all subgroups of a direct product are obtained as in part e of Theorem 11.6.2. For example, $\{(n, n) \mid n \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}^2$, but is not a direct product of two subgroups of $\mathbb{Z}$.

Example 11.6.3. Using the identity $(x + y) + x = y$, in $\mathbb{Z}_2$, we can devise a scheme for representing a symmetrically linked list using only one link field. A symmetrically linked list is a list in which each node contains a pointer to its immediate successor and its immediate predecessor (see Figure 11.6.3). If the pointers are n-digit binary addresses, then each pointer can be taken as an element of $\mathbb{Z}_2{}^n$. Lists of this type can be accomplished using cells with only one link. In place of a left and a right pointer, the only "link" is the value of the sum (left link) + (right link). All standard list operations (merge, insert, delete, traverse, and so on) are possible with this structure, provided that you know the value of the nil pointer and the address, f, of the first (i. e., leftmost) cell. Since first f.left is nil, we can recover f.right by adding the value of nil: $f + \text{nil} = (\text{nil} + f.\text{right}) + \text{nil} = f.\text{right}$, which is the address of the second item. Now if we temporarily retain the address, s, of the second cell, we can recover the address of the third item. The link field of the second item contains the sum $s.\text{left} + s.\text{right} = \text{first} + \text{third}$. Therefore

$$\begin{aligned}(\text{first} + \text{third}) + \text{first} &= s + s.\text{left} \qquad .\\ &= (s.\text{left} + s.\text{right}) + s.\text{left}\\ &= s.\text{right} = \text{third}\end{aligned}$$

We no longer need the address of the first cell, only the second and third, to recover the fourth address, and so forth.

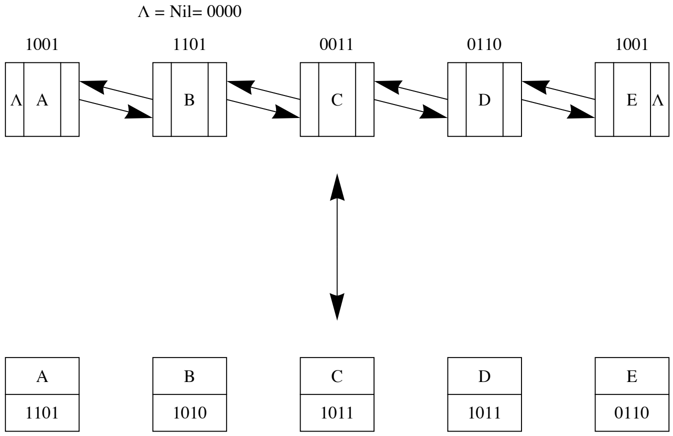


Figure 11.6.3
Symmetric Linked List

The following more formal algorithm uses names that the timing of the visits.

Algorithm 11.6.1. *Given a symmetric list represented as in Example 11.6.3, a traversal of the list is accomplished as follows, where first is the address of the first cell. We presume that each item has some information that is represented by item.info and a field called item.link that is the sum of the left and right links.*

```
(1) yesterday =nil
(2) today =first
(3) While today $\neq$ nil do
        (3.1) Write(today.info)
        (3.2) tomorrow = today.link + yesterday
        (3.3) yesterday = today
        (3.4) today = tomorrow.
```

At any point in this algorithm it would be quite easy to insert a cell between today and tomorrow. Can you describe how this would be accomplished?

EXERCISES FOR SECTION 11.6

A Exercises

1. Write out the group table of $\mathbb{Z}_2 \times \mathbb{Z}_3$ and find the two proper subgroups of this group.

2. List more examples of proper subgroups of $\mathbb{R}^2$ that are different from the ones in Example 11.6.2.

3. Algebraic properties of the n-cube:

(a) The four elements of $\mathbb{Z}_2{}^2$ can be visualized geometrically as the four corners of the 2-cube (see Figure 9.4.5). Algebraically describe the statements:

(i) Corers a and b are adjacent.

(ii) Corners a and b are diagonally opposite one another.

(b) The eight elements of $\mathbb{Z}_2{}^3$ can be visualized as the eight corners of the 3-cube. One face contains $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \{0\}$ and the opposite face contains the remaining four elements so that $(a, b, 1)$ is behind $(a, b, 0)$. As in part a, describe statements i and ii algebraically.

(c) If you could imagine a geometric figure similar to the square or cube in n dimensions, and its comers were labeled by elements of $\mathbb{Z}_2{}^n$ as in parts a and b, how would statements i and ii be expressed algebraically?

4. (a) Suppose that you were to be given a group $[G; *]$ and asked to solve the equation $x * x = e$. Without knowing the group, can you anticipate how many solutions there will be?

(b) Answer the same question as part a for the equation $x * x = x$.

5. Which of the following sets are subgroups of $\mathbb{Z} \times \mathbb{Z}$? Give a reason for any negative answers.

(a) $\{0\}$

(b) $\{(2 j,\ 2 k) \mid j, k \in \mathbb{Z}\}$

(c) $\{(2 j + 1,\ 2 k) \mid j, k \in \mathbb{Z}\}$

(d) $\{(n,\ n 2) \mid n \in \mathbb{Z}\}$

(e) $\{(j,\ k) \mid j + k \text{ is even}\}$

6. Determine the following values in group $\mathbb{Z}_3 \times \mathbb{R}^*$:

(a) $(2, 1) * (1, 2)$

(b) the identity element

(c) $(1,\ 1/2)^{-1}$

1.7 Isomorphisms

The following informal definition of isomorphic systems should be memorized. No matter how technical a discussion about isomorphic systems becomes, keep in mind that this is the essence of the concept.

Definition: Isomorphic Systems/Isomorphism. *Two algebraic systems are isomorphic if there exists a translation rule between them so that any true statement in one system can be translated to a true statement in the other*

Example 11.7.1. Imagine that you are an eight-year-old child who has been reared in an English-speaking family, has moved to Greece, and has been placed in a Greek school. Suppose that your new teacher asks the class to do the following addition problem that has been written out in Greek.

τρία συν τέσσερα ισούται ___

The natural thing for you to do is to take out your Greek-English/English-Greek dictionary and translate the Greek words to English, as outlined in Figure 11.7.1. After you've solved the problem, you can consult the same dictionary to obtain the proper Greek word that the teacher wants. Although this is not the recommended method of learning a foreign language, it will surely yield the correct answer to the problem. Mathematically, we may say that the system of Greek integers with addition (*συν*) is isomorphic to English integers with addition (plus). The problem of translation between natural languages is more difficult than this though, because two complete natural languages are not isomorphic, or at least the isomorphism between them is not contained in a simple dictionary.

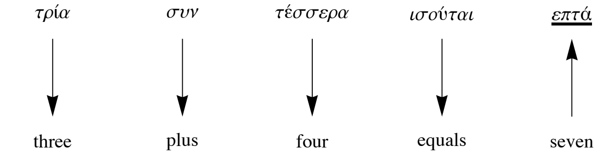


Figure 11.7.1
Solution of a Greek arithmetic problem

Example 11.7.2. Software Implementation of Sets. In this example, we will describe how set variables can be implemented on a computer. We will describe the two systems first and then describe the isomorphism between them.

System 1: The power set of {1, 2, 3, 4, 5} with the operation union, ⋃. For simplicity, we will only discuss union. However, the other operations are implemented in a similar way.

System 2: Strings of five bits of computer memory with an OR gate. Individual bit values are either zero or one, so the elements of this system can be visualized as sequences of five 0's and 1's. An OR gate, Figure 11.7.2, is a small piece of computer hardware that accepts two bit values at any one time and outputs either a zero or one, depending on the inputs. The output of an OR gate is one, except when the two bit values that it accepts are both zero, in which case the output is zero. The operation on this system actually consists of sequentially inputting the values of two bit strings into the OR gate. The result will be a new string of five 0's and 1's. An alternate method of operating in this system is to use five OR gates and to input corresponding pairs of bits from the input strings into the gates concurrently.

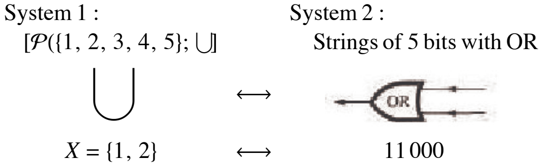


Figure 11.7.2
Translation between sets and strings of bits

The Isomorphism: Since each system has only one operation, it is clear that union and the OR gate translate into one another. The translation between sets and bit strings is easiest to describe by showing how to construct a set from a bit string. If $a_1 a_2 a_3 a_4 a_5$, is a bit string in System 2, the set that it translates to contains the number k if and only if a_k equals 1. For example, 10 001 is translated to the set {1, 5}, while the set {1, 2} is translated to 11 000. Now imagine that your computer is like the child who knows English and must do a Greek problem. To execute a program that has code that includes the set expression {1, 2} ⋃ {1, 5}, it will follow the same procedure as the child to obtain the result, as shown in Figure 11.7.3.

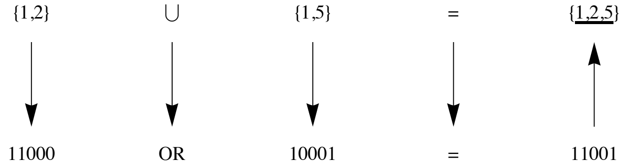


Figure 11.7.3
Translation of a problem in set theory

Example 11.7.3. Multiplying without doing multiplication. This isomorphism is between [$\mathbb{R}^+$; ·] and [$\mathbb{R}$;+]. Until the 1970s, when the price of calculators dropped, multiplication and exponentiation were performed with an isomorphism between these systems. The isomorphism ($\mathbb{R}^+$ to $\mathbb{R}$) between the two groups is that · is translated into + and any positive real number a is translated to the logarithm of a. To translate back from $\mathbb{R}$ to $\mathbb{R}^+$, you invert the logarithm function. If base ten logarithms are used, an element of $\mathbb{R}$, b, will be translated to 10^b. In pre-calculator days, the translation was done with a table of logarithms or with a slide rule. An example of how the isomorphism is used appears in Figure 11.7.4.

$$\begin{tikzcd}
8 \arrow[d] & \cdot \arrow[d] & 125 \arrow[d] & = \arrow[d] & \underline{1000} \\
0.90309 & + & 2.09691 & = & 3.000000 \arrow[u]
\end{tikzcd}$$

Figure 11.7.4
Multiplication using logarithms

The following definition of an isomorphism between two groups is a more formal one that appears in most abstract algebra texts. At first glance, it appears different, it is really a slight variation on the informal definition. It is the common definition because it is easy to apply; that is, given a function, this definition tells you what to do to determine whether that function is an isomorphism.

Procedure for showing that two groups are isomorphic

Definition: Group Isomorphism. *If* $[G_1 ; *_1]$ *and* $[G_2 ; *_2]$ *are groups,* $f : G_1 \to G_2$ *is an isomorphism from* G_1 *into* G_2 *if:*

(a) f *is a bijection, and*

(b) $f(a *_1 b) = f(a) *_2 f(b)$ *for all* $a,\ b \in G_1$

If such a function exists, then G_1 *is isomorphic to* G_2.

Notes:

(a) There could be several different isomorphisms between the same pair of groups. Thus, if you are asked to demonstrate that two groups are isomorphic, your answer need not be unique.

(b) Any application of this definition requires a procedure outlined in Figure 11.7.5.

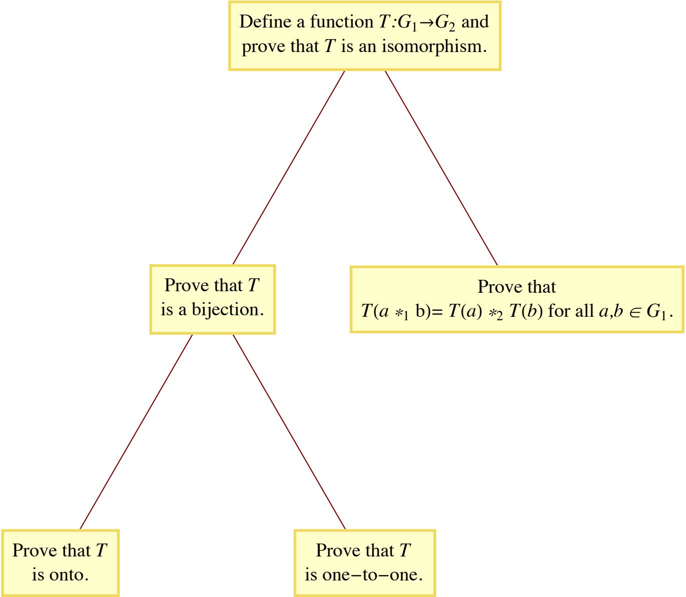

Define a function $T:G_1 \to G_2$ and prove that T is an isomorphism.
Prove that T is a bijection.
Prove that $T(a *_1 \text{b})= T(a) *_2 T(b)$ for all $a,b \in G_1$.
Prove that T is onto.
Prove that T is one−to−one.

Figure 11.7.5
Steps in proving that G_1 and G_2 are isomorphic

The first condition, that an isomorphism be a bijection, reflects the fact that every true statement in the first group should have exactly one corresponding true statement in the second group. This is exactly why we run into difficulty in translating between two natural languages. To see how Condition (b) of the formal definition is consistent with the informal definition, consider the Function $L : \mathbb{R}^+ \to \mathbb{R}$ defined by $L(x) = \log_{10} x$. The translation diagram between $\mathbb{R}^+$ and $\mathbb{R}$ for the multiplication problem $a \cdot b$ appears in Figure 11.7.6. We arrive at the same result by computing $L^{-1}(L(a) + L(b))$ as we do by computing $a \cdot b$. If we apply the function L to the two results, we get the same image:

$$L(a \cdot b) = L(L^{-1}(L(a) + L(b))) = L(a) + L(b) \quad (11.7\text{a})$$

since $L(L^{-1}(x)) = x$. Note that 11.7a is exactly Condition b of the formal definition applied to the two groups $\mathbb{R}^+$ and $\mathbb{R}$.

$$\begin{tikzcd}
a \arrow[d] & \cdot \arrow[d] & b \arrow[d] & = \arrow[d] & L^{-1}(L(a * b)) \\
L(a) & + & L(b) & = & L(a\cdot b) \arrow[u]
\end{tikzcd}$$

Figure 11.7.6
Multiplication using logarithms - general situation

Example 11.7.4. Consider $G = \left\{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \,\middle|\, a \in \mathbb{R}\right\}$ with matrix multiplication. This group $[\mathbb{R}; +]$ is isomorphic to G. Our translation rule is the function $f : \mathbb{R} \to G$ defined by $f(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. Since groups have only one operation, there is no need to state explicitly that addition is translated to matrix multiplication. That f is a bijection is clear from its definition. If a and b are any real numbers,

$$\begin{aligned} f(a)\, f(b) &= \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} \\ &= f(a+b) \end{aligned}$$

We can apply this translation rule to determine the inverse of a matrix in G. We know that $a + (-a) = 0$ is a true statement in $\mathbb{R}$. Using f to translate this statement, we get

$$f(a)\, f(-a) = f(0)$$

or

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

therefore,

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix}$$

Theorem 11.7.1 summarizes some of the general facts about group isomorphisms that are used most often in applications. We leave the proof to the reader.

Theorem 11.7.1. *If $[G; *]$ and $[H, \diamond]$ are groups with identities e and e', respectively, and $T : G \to H$ is an isomorphism from G into H, then:*

(a) $T(e) = e'$,

(b) $T(a)^{-1} = T\left(a^{-1}\right)$ for all $a \in G$, and

(c) If K is a subgroup of G, then $T(K) = \{T(a) : a \in K\}$ is a subgroup of H and is isomorphic to K.

"Is isomorphic to" is an equivalence relation on the set of all groups. Therefore, the set of all groups is partitioned into equivalence classes, each equivalence class containing groups that are isomorphic to one another.

Procedures for showing groups are not isomorphic

How do you decide that two groups are *not* isomorphic to one another? The negation of "G and H are isomorphic" is that no translation rule between G and H exists. If G and H have different cardinalities, then no bijection from G into H can exist. Hence they are not isomorphic. Given that $|G| = |H|$, it is usually impractical to list all bijections from G into H and show that none of them satisfy Condition b of the formal definition. The best way to prove that two groups are not isomorphic is to find a true statement about one group that is not true about the other group. We illustrate this method in the following checklist that you can apply to most pairs of non-isomorphic groups in this book.

Assume that $[G; *]$ and $[H; \diamond]$ are groups. The following are reasons for G and H to be not isomorphic.

(a) G and H do not have the same cardinality. For example, $\mathbb{Z}_{12} \times \mathbb{Z}_5$ can't be isomorphic to $\mathbb{Z}_{50}$ and $[\mathbb{R}; +]$ can't be isomorphic to $[\mathbb{Q}^+ ; \cdot]$,

(b) G is abelian and H is not abelian since $a * b = b * a$ is always true in G, but $T(a) \diamond T(b) = T(b) \diamond T(a)$ would not always be true. Two groups with six elements each are $\mathbb{Z}_6$ and the set of 3×3 rook matrices (see Exercise 5 in Section 11.2). The second group is non-abelian, therefore it can't be isomorphic to $\mathbb{Z}_6$.

(c) G has a certain kind of subgroup that H doesn't have. Theorem 11.7.1(c) states that this cannot happen if G is isomorphic to H. $[\mathbb{R}^* ; \cdot]$ and $[\mathbb{R}^+ ; \cdot]$ are not isomorphic since $\mathbb{R}^*$ has a subgroup with two elements, $\{-1,\ 1\}$, while the proper subgroups of $\mathbb{R}^+$ are all infinite (Convince yourself of this fact!).

(d) The number of solutions of $x * x = e$ in G is not equal to the number of solutions of $y \diamond y = e'$ in H. $\mathbb{Z}_8$ is not isomorphic to $\mathbb{Z}_2{}^3$ since $x +_8 x = 0$ has two solutions, 0 and 4, while $y + y = (0,\ 0,\ 0)$ is true for all $y \in \mathbb{Z}_2{}^3$. If the operation in G is defined by a table, then the number of solutions of $x * x = e$ will be the number of occurrences of e in the main diagonal of the table. The equations $x^3 = e$, $x^4 = e$, … can also be used in the same way to identify non-isomorphic groups.

(e) One of the cyclic subgroups of G equals G (i. e., G is cyclic), while none of H's cyclic subgroups equals H (i. e., H is noncyclic). This is a special case of Condition c. $\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$ are not isomorphic since $\mathbb{Z} = \langle 1 \rangle$ and $\mathbb{Z} \times \mathbb{Z}$ is not cyclic.

EXERCISES FOR SECTION 11.7

A Exercises

1. State whether each pair of groups below is isomorphic. If it is, give an isomorphism; if it is not, give your reason.

(a) $\mathbb{Z} \times \mathbb{R}$ and $\mathbb{R} \times \mathbb{Z}$

(b) $\mathbb{Z}_2 \times \mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$

(c) $\mathbb{R}$ and $\mathbb{Q} \times \mathbb{Q}$

(d) $\mathcal{P}(\{1, 2\})$ with symmetric difference and $\mathbb{Z}_2{}^2$

(e) $\mathbb{Z}_2{}^2$ and $\mathbb{Z}_4$

(f) $\mathbb{R}^4$ and $M_{2\times 2}(\mathbb{R})$ with matrix addition

(g) $\mathbb{R}^2$ and $\mathbb{R} \times \mathbb{R}^+$

(h) $\mathbb{Z}_2$ and the 2×2 rook matrices

(i) $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$

2. If you know two natural languages, show that they are not isomorphic.

3. Prove that the relation "is isomorphic to" on groups is transitive.

4. (a) Write out the operation table for $G = [\{1, -1, i, -i\}, \cdot]$ where i is the complex number for which $i^2 = -1$. Show that G is isomorphic to $[\mathbb{Z}_4; +_4]$.

(b) Solve $x^2 = -1$ in G by first translating to $\mathbb{Z}_4$, solving the equation in $\mathbb{Z}_4$, and then translating back to G.

B Exercises

5. It can be shown that there are five non-isomorphic groups of order eight. You should be able to describe at least three of them. Do so without use of tables. Be sure to explain why they are not isomorphic.

6. Prove Theorem 11.7.1.

7. Prove that all infinite cyclic groups are isomorphic to $\mathbb{Z}$.

8. (a) Prove that $\mathbb{R}^*$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{R}$.

(b) Describe how multiplication of nonzero real numbers can be accomplished doing only additions and translations.

9. Prove that if G is any group and g is some fixed element of G, then the function ϕ_g defined by $\phi_g(x) = g * x * g^{-1}$ is an isomorphism from G into itself. An isomorphism of this type is called an *automorphism*.

11.8 Using Computers to Study Groups

Groups in *Mathematica*

Mathematica has a wide variety of computable databases available and one of them is on finite groups. To access the database you use the function **FiniteGroupData**. Extensive documentation is available at . Since we've only scratch the surface of group theory at this point, most of the groups and concepts mentioned are likely to be unfamiliar to the reader. For this reason, we well wait until Chapter 15 to discuss that database.

The *Combinatorica* package that is included in all *Mathematica* distributions has limited abstract algebra

```
<< Combinatorica`
```

Here is how to generate the body of the operation table for the ring $[\mathbb{Z}_7; +_7]$. Notice that this really an addition table even though the function that creates the table is called **MultiplicationTable**.

```
MultiplicationTable[Range[0, 6], Function[{a, b}, Mod[a + b, 7]]]
```

```
⎛1 2 3 4 5 6 7⎞
⎜2 3 4 5 6 7 1⎟
⎜3 4 5 6 7 1 2⎟
⎜4 5 6 7 1 2 3⎟
⎜5 6 7 1 2 3 4⎟
⎜6 7 1 2 3 4 5⎟
⎝7 1 2 3 4 5 6⎠
```

An even more user-friendly package that you would need to download to use is available at Exploring Abstract Algebra with Mathematica (http://www.central.edu/EAAM/). The package, when installed on your computer, is loaded with the command

```
<< AbstractAlgebra`Master`
```

The group $\mathbb{Z}_{12}$ is

```
G = ZG[12]
```

```
Groupoid({0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11}, (#1 + #2) mod 12 &)
```

At this point **G** is an object that consists of the set {0, 1, 2, …, 11} and the binary operation $+_{12}$. Among things we can do with **G** is that we can examine its subgroups.

```
Subgroups[G]
```

```
{Groupoid({0}, (#1 + #2) mod 12 &), Groupoid({0, 2, 4, 6, 8, 10}, (#1 + #2) mod 12 &),
  Groupoid({0, 3, 6, 9}, (#1 + #2) mod 12 &), Groupoid({0, 4, 8}, (#1 + #2) mod 12 &),
  Groupoid({0, 6}, (#1 + #2) mod 12 &), Groupoid({0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11}, (#1 + #2) mod 12 &)}
```

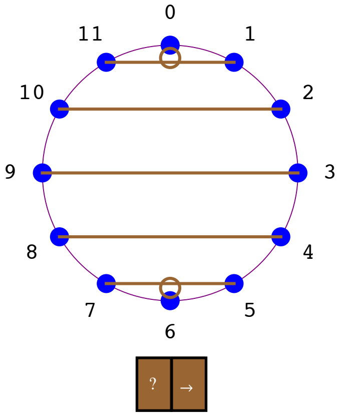
We can view the inverses of elements in a variety of ways. For example, we can get them paired up. Notice that two of the elements, 0 and 6 invert themselves.

```
Inverses[G]
```

```
⎛0  0⎞
⎜1 11⎟
⎜2 10⎟
⎜3  9⎟
⎜4  8⎟
⎜5  7⎟
⎝6  6⎠
```

There is a "Visual Mode" that gives us a different view of the inverses. The boxes with "?" and "→" give further information in you are reading this in a *Mathematica* Notebook and have the package installed.

```
Inverses[G, Mode → Visual]
```



The package was designed for teaching a first course in abstract algebra and so it has features that are more basic than other abstract algebra resources. For example, we can ask **G** is really a group and get quite a bit of information.

```
GroupQ[G, Mode → Textual]
```

Given a set S and an operation ∗, we call the pair (S,∗) a group if S is closed under the operation ∗, there is an identity element, every elemement has an inverse and the operation ∗ is associative.

We say a Groupoid G has an identity e if for all other elements g in G we have e + g = g + e = g (where + indicates the operation). In this case, Z[12] has the identity 0.

→

We say that a set S is closed under an operation op if whenever we have x and y in S, we also have op[x,y] (or x~op~y) in S. In this case, the Groupoid Z[12] is indeed closed.

→

Given a Groupoid G, we say an element g in G has an inverse h if G has an identity, say e, and g + h = h + g = e (where + indicates the operation). The Groupoid Z[12] has an inverse for every element. Here they are:

x	x^{-1}
0	0
1	11
2	10
3	9
4	8
5	7
6	6

→

Given a structured set S (Groupoid or Ringoid), we say the operation ∗ is associative if for every g, h, and k in S we have (g∗h)∗k = g∗(h∗k), where ∗ is the group operation. In this case, Z[12] is associative. Consider the following table illustrating random triples that associate. Pay attention to the last two columns.

i	j	k	(i∗j)∗k	i∗(j∗k)
2	11	4	5	5
3	1	4	8	8
8	9	8	1	1
7	5	2	2	2
8	8	2	6	6
10	6	9	1	1
4	9	7	8	8
4	5	2	11	11
11	4	1	4	4
5	10	6	9	9

→

This package also has much more capabilities than what we've covered so far and we will revisit it in Chapters 15 and 16.

Groups in Sage

Abstract Algebra seems to have been given a much higher priory in the design of Sage than it was in *Mathematica*. Again, the capabilities far exceed what we've touch on in the theory, but here are a few examples that you should understand. Here is how to generate the group related to

$\mathbb{Z}_{14}$.

```
G=AbelianGroup(1,[14])
G.list()
      [1, f, f^2, f^3, f^4, f^5, f^6, f^7, f^8, f^9, f^10, f^11, f^12, f^13]
```

There is no output from assigning G. The elements of G are generated from the `list` method. The connection with $\mathbb{Z}_{14}$ is that when we multiply powers of `f`, the exponents are added with $+_{14}$. Among other things we can ask whether G is abelian and what its subgroups are.

```
G.is_abelian()
True
G.subgroups()
[Multiplicative Abelian Group isomorphic to C2 x C7, which is the
subgroup of
Multiplicative Abelian Group isomorphic to C14
generated by [f], Multiplicative Abelian Group isomorphic to C7, which
is the subgroup of
Multiplicative Abelian Group isomorphic to C14
generated by [f^2], Multiplicative Abelian Group isomorphic to C2, which
is the subgroup of
Multiplicative Abelian Group isomorphic to C14
generated by [f^7], Trivial Abelian Group, which is the subgroup of
Multiplicative Abelian Group isomorphic to C14
generated by []]
```

SUPPLEMENTARY EXERCISES FOR CHAPTER 11

Section 11.1

1. $V = \{a, b, c\}$ is a set with operations + and · defined by the following "addition" and "multiplication" tables:

+	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

·	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

(a) With respect to V under + determine,

(i) The identity (i.e., the "zero" of the addition).

(ii) The inverse of each element, that is, $-a$, $-b$, and $-c$.

(b) With respect to V under · determine,

(i) The identity (i.e., the "one" of the multiplication).

(ii) The inverse of each element different from "zero."

(c) Is + distributive over · ? Is · distributive over + ?

2. (a) Determine whether the following are valid binary operations on the given sets. Explain fully.

(i) Matrix addition on $A = \left\{\begin{pmatrix} a & b \\ c & 0 \end{pmatrix} \middle|\ a,\ b,\ c \in \mathbb{R}\right\}$

(ii) Matrix multiplication on the set A above.

(iii) On $\mathbb{Q}^+$, define * by $a * b = (a \cdot b)/2$.

(iv) Function composition on $A^A = \{f\colon A \to A\}$, where A is $\{1, 2, 3\}$.

(v) Function composition on $B = \{f \in A^A \mid f \text{ is } a \text{ bijection}\}$.

(b) For each binary operation above give the identity element if it exists. Explain.

(c) Determine which of the above binary operations are commutative and which are associative.

3. Let S = set of all bijections of a set A, and let $\circ$ be function composition. Does $\circ$ have the inverse property? Does function composition have the involution property? Explain.

4. Does + on $M_{2\times2}(\mathbb{R})$ have the inverse property? Does + have the involution property? Explain.

5. Prove that the odd integers are closed under multiplication but not under addition. Are the even integers closed under both addition and multiplication? Prove your answers.

Section 11.2

6. (a) Show that $\mathbb{R}^2$ is a group under componentwise addition, that is,

$$(a_1, a_2) + (b_1, b_2) = (a_1 + a_2,\ b_1 + b_2).$$

(b) Show that $\{(x,\ 2x) \mid x \in \mathbb{R}\}$ is a group under componentwise addition. Draw the graph of this subset. Describe similar subsets of $\mathbb{R}^2$ that are also groups.

7. Prove that the set of all 2 × 2 invertible matrices (over $\mathbb{R}$) is a group under matrix multiplication. Assume, as indicated in Chapter 5, that the associative law is true for matrices under multiplication. This group is called the *general linear group* of degree 2 over $\mathbb{R}$, and it is denoted by GL(2, $\mathbb{R}$). It is given this name because these matrices are matrix representations of linear motions of $\mathbb{R}^2$.

8. Prove that $\left\{A = \begin{pmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix} \middle|\ \det A = 1\right\}$ is a group under matrix multiplication. Assume that the associative law is true under matrix multiplication. This group is called the *special linear group* of degree 2 over $\mathbb{R}$ and it is denoted SL(2, $\mathbb{R}$).

9. Show that $\mathbb{R}$ is a group under the operation $*$ defined by $a * b = a + b + 5$ for $a,\ b \in \mathbb{R}$.

10. (a) let $B_{3\times3}$ be the set of all 3 × 3 Boolean (adjacency) matrices discussed in Section 6.4. Is $B_{3\times3}$ a monoid under Boolean addition? Is it a group? Explain.

(b) Is $B_{3\times3}$ a monoid under Boolean multiplication? Is it a group? Explain.

Section 11.3

11. Define $*$ on $\mathbb{Q}^+$ by $a * b = (a \bullet b)/2$. *Prove* that $[\mathbb{Q}^+ ; *]$ is a group.

12. Let G be the group $\mathbb{R}$ under the operation $a * b = a + b + 5$ for $a,\ b \in \mathbb{R}$. Solve the following equations for x in G.

(a) $x * 3 = 5$ (d) $x^2 = 2$

(b) $2 * x * 4 = 6$ (e) $4 * x^2 = 5$

(e) $x^3 = 7$

13. Solve the equation $A * X * B = C$ in GL(2, $\mathbb{R}$) where

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix}, \quad \text{and} \quad C = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}.$$

14. Prove that if $[G; *]$ is a group, $(a * b)^n = a^n * b^n$ for all $n \geq 1$ and $a,\ b \in G$ if and only if [G;*] is an abelian group.

Section 11.4

15. Calculate the following in $\mathbb{Z}_5$:

(a) $3\ +_5\ 8$

(b) $(-3) \times_5 2$

(c) $(3 \times_5 2) +_5 (2 \times_5 2)$

(d) 2^{-1} (i.e., the multiplicative inverse of 2)

16. (a) Prove that $\{1, 3, 5, 7\}$, is a group under $\times_8$. Write out its group table.

(b) Let $U(\mathbb{Z}_n)$ stand for the elements of $\mathbb{Z}_n$, which have inverses under $\times_n$. Convince yourself that $U(\mathbb{Z}_n)$ is a group under $\times_n$.

(c) Prove that the elements of $U(\mathbb{Z}_n)$ are those elements $a \in \mathbb{Z}_n$ such that $gcd(a,\ n) = 1$. You may use the fact that $gcd(a,\ b) = 1 \Leftrightarrow$ there exist integers s and t such that $sa + tb = 1$.

Section 11.5

17. (a) Recall from "Supplementary Exercises," Section 11.4, that $U(\mathbb{Z}_8)$is a group under $\times_8$. List all cyclic subgroups of this group.

(b) Is $U(\mathbb{Z}_8)$ a cyclic group? Explain.

18. (a) Use Theorem 11.5.1 to prove that the set of even integers is a subgroup of the group $\mathbb{Z}$ (under +).

(b) Is the set of odd integers a subgroup of the group $\mathbb{Z}$ (under +)?

19. Prove that SL(2, $\mathbb{R}$) is a subgroup of GL(2, $\mathbb{R}$). See Exercises 7 and 8 above for an explanation of this notation.

20. Recall that $M_{2\times 2}(R)$ is a group under addition.

(a) Is $A = \left\{ \begin{pmatrix} a & b \\ a & 0 \end{pmatrix} \middle| \ a, b \in \mathbb{R} \right\}$ a subgroup of $M_{2\times 2}(\mathbb{R})$?

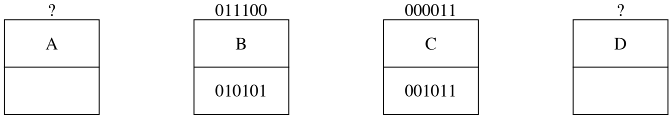
(b) Is $B = \left\{ \begin{pmatrix} a & b \\ b & 1 \end{pmatrix} \middle| \ a, b \in \mathbb{R} \right\}$ a subgroup of $M_{2\times 2}(\mathbb{R})$?

(c) Are either of the subsets in parts a and b subgroups of GL(2, $\mathbb{R}$)?

21. Let $B_{3\times 3}$ be the monoid of all 3×3 Boolean matrices, under Boolean addition. Let S be a subset of $B_{3\times 3}$ consisting of all 3×3 matrices that represent symmetric relations. Is S a submonoid of $B_{3\times 3}$?

Section 11.6

22. Using the data structure in the text for doubly linked lists with six-bit addresses, what are the addresses of the records containing A and D? Write your answer as a sum in the group $\mathbb{Z}_2^6$ and then as an address.



23. Determine the inverse of each element in the respective group.

(a) $(2, 3, 5)$ in $\mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_{25}$

(b) $(1,0, 1, 1)$ in $\mathbb{Z}^4$

(c) $(3, 2)$ in $\mathbb{R}^+ \times \mathbb{Z}_6$

(d) $(2, 3,5)$ in $\mathbb{R}^3$

24. Determine the identity elements in the following groups:

(a) $\mathbb{R}^+ \times \mathbb{R}^+$

(b) $\mathbb{R}^+ \times \mathbb{Z}_3$

(c) GL$(2, \mathbb{R}) \times \mathbb{R}^3$

25. Which of the following groups are abelian? Explain.

(a) $\mathbb{Z}_2 \times \mathbb{Z}_{24} \times \mathbb{Z}_{75}$

(b) GL$(2, \mathbb{R}) \times \mathbb{Z}_2$

(c) $\mathbb{Z}^n$

26. Is $\{0, 3\} \times \{0, 4, 8\}$ a subgroup of $\mathbb{Z}_6 \times \mathbb{Z}_8$? Explain.

Section 11.7

27. Prove that the cyclic subgroup (4) of $\mathbb{Z}_{16}$ is isomorphic to $\mathbb{Z}_4$.

28. Let $G = \{\&, \$, \%\}$. Given that $[G; *]$ is a group and that it is isomorphic to the group $[\mathbb{Z}_3; +_3]$ with isomorphism $T : G \to \mathbb{Z}_3$ defined by $T(\&) = 1, T(\$) = 2$, and $T(\%) = 0$. What are

(a) $\$ * \$$ (b) The identity of $[G; *]$

29. Let U be a set and $\mathrm{P}_U = \{$propositions over the set $U\}$. It can be shown that the algebraic system $[\mathrm{P}_U; \sim, \wedge, \vee]$ is isomorphic to $[\mathcal{P}(U); \cdot, \cap, \cup]$.

(a) Explain what this means.

(b) How does this help you understand the language of the algebra of propositions?

(c) Give the "propositional" analogue to the following statement: If $A \cap B^c = \emptyset$ and $A \cap B = \emptyset$ then $A = \emptyset$.

30. Write out the operation tables for the following systems:

(a) $[\{0, 1\}; +, \cdot]$ where + and · denote Boolean addition and multiplication.

(b) $[\{-1, 1\}; \wedge, \vee]$ where $i \wedge j$ and $i \vee j$ denote the largest and smallest, respectively, of i and j.

(c) $[\mathbb{Z}_2; +_2, \times_2]$.

Are these systems isomorphic? Explain.

31. Prove that the group $\mathbb{C}$, under +, is isomorphic to the group $\mathbb{R}^2$, under + .

32. Determine which of the following groups are isomorphic. Explain.

(a) $\mathbb{R}_3$, the 3×3 rook matrices, and $\mathbb{Z}_6$

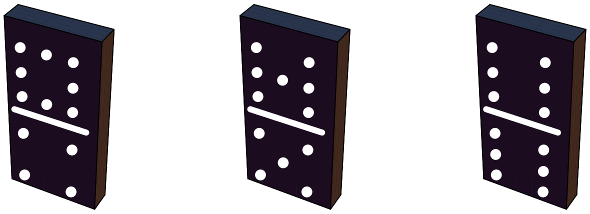
(b) $\mathbb{R}_3$ and $S_A = \{f \in A^A : f \text{ is a bijection}\}$, where A is $\{1, 2, 3\}$.

(c) $\mathbb{Z}_6$ and $U(\mathbb{Z}_7)$

33. Prove that $\mathbb{R}^4$ under addition, is isomorphic to $M_{2\times 2}(\mathbb{R})$, under addition.

34. Prove that the group $[U(\mathbb{Z}_8); \times_8]$ is isomorphic to $[\mathbb{Z}_4; +_4]$.

chapter 12



MORE MATRIX ALGEBRA

GOALS

In Chapter 5 we studied matrix operations and the algebra of sets and logic. We also made note of the strong resemblance of matrix algebra to elementary algebra. The reader should briefly review this material. In this chapter we shall look at a powerful matrix tool in the applied sciences—namely, a technique for solving systems of linear equations. We will then use this process for determining the inverse of $n\times n$ matrices, $n \geq 2$, when they exist. We conclude by a development of the diagonalization process, with a discussion of several of its applications.

12.1 Systems of Linear Equations

The method of solving systems of equations by matrices that we will look at is based on procedures involving equations that we are familiar with from previous mathematics courses. The main idea is to reduce a given system of equations to another simpler system that has the same solutions.

Definition: Solution Set. *Given a system of equations involving real variables x_1, x_2, …, x_n, the solution set of the system is the set of n-tuples in $\mathbb{R}^n$, $(a_1,\ a_2,\ \ldots, a_n)$ such that the substitutions $x_1 = a_1$, $x_2 = a_2$, …, $x_n = a_n$ make all the equations true.*

In terms of logic, a solution set is a truth set of a system of equations, which is a proposition over n-tuples of real numbers.

In general, if the variables are from a set S, then the solution set will be a subset of S^n. For example, in number theory mathematicians study Diophantine equations, where the variables can only take on integer values instead of real values.

Definition: Equivalent Systems of Equations. *Two systems of linear equations are called equivalent if they have the same set of solutions.*

Example 12.1.1. The previous definition tells us that if we know that the system

$$\begin{aligned} 4x_1+2x_2+x_3&=1\\ 2x_1+x_2\quad+x_3&=4\\ 2x_1+2x_2+x_3&=3 \end{aligned}$$

is equivalent to the system

$$\begin{aligned} x_1+0x_2+0x_3&=-1\\ 0x_1+x_2\quad+0x_3&=-1\\ 0x_1+0x_2\quad+x_3&=\ 7 \end{aligned}$$

then both systems have the solution set $\{(-1,\ -1,\ 7)\}$. In other words, the values $x_1 = -1$, $x_2 = -1$, and $x_3 = 7$ are the only values of the variables that make all three equations in either system true.

Theorem 12.1.1. Elementary Operations on Equations. *If any sequence of the following operations is performed on a system of equations, the resulting system is equivalent to the original system:*

(1) Interchange any two equations in the system.

(2) Multiply both sides of any equation by a nonzero constant.

(3) Multiply both sides of any equation by a nonzero constant and add the result to a second equation in the system, with the sum replacing the latter equation.

Let us now use the above theorem to work out the details of Example 12.1.1 and see how we can arrive at the simpler system..

Step 1. We will first change the coefficient of x_1 in the first equation to one and then use it as a pivot to obtain 0's for the coefficients of x_1 in Equations 2 and 3.

(1.1)
$$\begin{aligned} 4x_1+2x_2+x_3&=1\\ 2x_1+x_2+x_3&=4\\ 2x_1+2x_2+x_3&=3 \end{aligned}$$

Multiply Equation 1 by $\frac{1}{4}$ to obtain

(1.2)
$$\begin{aligned} x_1+\frac{x_2}{2}+\frac{x_3}{4}&=\frac{1}{4}\\ 2x_1+x_2+x_3&=4\\ 2x_1+2x_2+x_3&=3 \end{aligned}$$

Multiply Equation 1 by -2 and add the result to Equation 3 to obtain

(1.3)
$$\begin{aligned} x_1\ +\frac{x_2}{2}\ +\frac{x_3}{4}&=\frac{1}{4}\\ 0x_1+0x_2+\frac{x_3}{2}&=\frac{7}{2}\\ 2x_1+2x_2+x_3&=3 \end{aligned}$$

Multiply Equation 1 by -2 and add the result to Equation 3 to obtain

(1.4)
$$\begin{aligned} x_1\ +\ \frac{x_2}{2}\ +\frac{x_3}{4}&=\frac{1}{4}\\ 0x_1+0x_2+\frac{x_3}{2}&=\frac{7}{2}\\ 0x_1+\ x_2+\frac{x_3}{2}&=\frac{5}{2} \end{aligned}$$

Note: We've explicitly written terms with zero coefficients such as $0x_1$ to make a point that all variables can be thought of as being involved in all equations. After this example we will discontinue this practice in favor of the normal practice of making these terms "disappear."

Step 2. We would now like to proceed in a fashion analogous to Step 1—namely, multiply the coefficient of x_2 in the second equation by a suitable number so that the result is 1. Then use it as a pivot to obtain 0's as coefficients for x_2 in the first and third equations. This is clearly impossible (Why?), so we will first interchange Equations 2 and 3 and proceed as outlined above.

(2.1)
$$\begin{aligned} x_1\ +\ \frac{x_2}{2}\ +\frac{x_3}{4}&=\frac{1}{4}\\ 0x_1+0x_2+\frac{x_3}{2}&=\frac{7}{2}\\ 0x_1+\ x_2+\frac{x_3}{2}&=\frac{5}{2} \end{aligned}$$

Interchange Equations 2 and 3 to obtain

(2.2)
$$\begin{aligned} x_1\ +\ \frac{x_2}{2}\ +\frac{x_3}{4}&=\frac{1}{4}\\ 0x_1+\ x_2\ +\frac{x_3}{2}&=\frac{5}{2}\\ 0x_1+0x_2+\frac{x_3}{2}&=\frac{7}{2} \end{aligned}$$

Multiply Equation 2 by $-\frac{1}{2}$ and add the result to Equation 1 to obtain

(2.3)
$$\begin{aligned} x_1+0x_2+0x_3&=-1\\ 0x_1\ +x_2\ +\frac{x_3}{2}&=\frac{5}{2}\\ 0x_1\ +0x_2\ +\frac{x_3}{2}&=\frac{7}{2} \end{aligned}$$

Step 3. Next, we will change the coefficient of x_3 in the third equation to one and then use it as a pivot to obtain 0's for the coefficients of x_3 in Equations 1 and 2.

(3.1)
$$\begin{aligned} x_1+0x_2+0x_3&=-1\\ 0x_1\ +x_2\ +\frac{x_3}{2}&=\frac{5}{2}\\ 0x_1\ +0x_2\ +\frac{x_3}{2}&=\frac{7}{2} \end{aligned}$$

Multiply Equation 3 by 2 to obtain

(3.2)
$$\begin{aligned} x_1+0x_2+0x_3&=-1\\ 0x_1\ +x_2\ +\frac{x_3}{2}&=\frac{5}{2}\\ 0x_1\ +0x_2\ +x_3&=7 \end{aligned}$$

Multiply Equation 3 by $-\frac{1}{2}$ and add the result to Equation 2 to obtain

$$(3.3)\qquad \begin{array}{rrrl} x_1 & +\,0\,x_2 & +\,0\,x_3 & = -1 \\ 0\,x_1 & +\,x_2 & +\,0\,x_3 & = -1 \\ 0\,x_1 & +\,0\,x_2 & +\,x_3 & = \ 7 \end{array}$$

From the system of equations in Step 3.3, we see that the solution to the original system (Step 1.1) is $x_1 = -1$, $x_2 = -1$, and $x_3 = 7$.

In the above sequence of steps, we note that the variables serve the sole purpose of keeping the coefficients in the appropriate location. This we can effect by using matrices. The matrix of the system given in Step 1.1 is

$$\begin{pmatrix} 4 & 2 & 1 & 1 \\ 2 & 1 & 1 & 4 \\ 2 & 2 & 1 & 3 \end{pmatrix}$$

where the matrix of the first three columns is called the coefficient matrix and the complete matrix is referred to as the augmented matrix. Since we are now using matrices to solve the system, we will translate Theorem 12.1.1 into matrix language.

Definition: Elementary Row Operations. *The following operations on a matrix are called elementary row operations:*

(1) Interchange any two rows of the matrix.

(2) Multiply any row of the matrix by a nonzero constant.

(3) Multiply any row of the matrix by a nonzero constant and add the result to a second row, with the sum replacing the second row.

Definition: Row Equivalent. Two matrices, A and B, are said to be row-equivalent if one can be obtained from the other by any one elementary row operation or by any sequence of elementary row operations.

If we use the notation R_i to stand for Row i of a matrix and $\longrightarrow$ to stand for row equivalence, then

$$A \xrightarrow{c\,R_i + R_j} B$$

means that the matrix B is obtained from the matrix A by multiplying the Row i of A by c and adding the result to Row j. The operation of multiplying row i by c is indicated by

$$A \xrightarrow{c\,R_i} B$$

while interchanging rows i and j is denoted by

$$A \xrightarrow{R_i \leftrightarrow R_j} B.$$

The matrix notation for the system given in Step 1.1 with the subsequent steps are:

$$\begin{pmatrix} 4 & 2 & 1 & 1 \\ 2 & 1 & 1 & 4 \\ 2 & 2 & 1 & 3 \end{pmatrix} \xrightarrow{\frac{1}{4} R_1} \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ 2 & 1 & 1 & 4 \\ 2 & 2 & 1 & 3 \end{pmatrix} \xrightarrow{-2\,R_1 + R_2} \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ 0 & 0 & \frac{1}{2} & \frac{7}{2} \\ 2 & 2 & 1 & 3 \end{pmatrix}$$

$$\xrightarrow{-2\,R_1 + R_3} \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ 0 & 0 & \frac{1}{2} & \frac{7}{2} \\ 0 & 1 & \frac{1}{2} & \frac{5}{2} \end{pmatrix} \xrightarrow{R_2 \leftrightarrow R_3} \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ 0 & 1 & \frac{1}{2} & \frac{5}{2} \\ 0 & 0 & \frac{1}{2} & \frac{7}{2} \end{pmatrix}$$

$$\xrightarrow{-\frac{1}{2} R_2 + R_1} \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & \frac{1}{2} & \frac{5}{2} \\ 0 & 0 & \frac{1}{2} & \frac{7}{2} \end{pmatrix} \xrightarrow{2\,R_3} \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & \frac{1}{2} & \frac{5}{2} \\ 0 & 0 & 1 & 7 \end{pmatrix}$$

$$\xrightarrow{-\frac{1}{2} R_3 + R_2} \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 7 \end{pmatrix}$$

This again gives us the solution. This procedure is called the *Gauss-Jordan elimination method*.

It is important to remember when solving any system of equations via this or any similar approach that at any step in the procedure we can rewrite the matrix in "equation format" to help us to interpret the meaning of the augmented matrix.

In Example 12.1.1 we obtained a unique solution, only one triple, namely $(-1, -1, 7)$, which satisfies all three equations. For a system involving three unknowns, are there any other possible results? To answer this question, let's review some basic facts from analytic geometry.

The graph of a linear equation in three-dimensional space is a plane. So geometrically we can visualize the three linear equations as three planes in three-space. Certainly the three planes can intersect in a unique point, as in Example 12.1.1, or two of the planes could be parallel. If two planes are parallel, there are no common points of intersection; that is, there are no triple of real numbers that will satisfy all three equations.

Also, the three planes could intersect along a common axis or line. In this case, there would be an infinite number of real number triples in $\mathbb{R}^3$ that would satisfy all three equations. Finally if all three equations describe the same plane, the solution set would be that plane. We generalize;

In a system of n linear equations, n unknowns, there can be:

(1) a unique solution,

(2) no solution, or

(3) an infinite number of solutions.

To illustrate these points, consider the following examples:

Example 12.1.2. Find all solutions to the system

$$\begin{aligned} x_1 + 3x_2 + x_3 &= 2 \\ x_1 + x_2 + 5x_3 &= 4 \\ 2x_1 + 2x_2 + 10x_3 &= 6 \end{aligned}$$

The reader can verify that the augmented matrix of this system,

$$\begin{pmatrix} 1 & 3 & 1 & 2 \\ 1 & 1 & 5 & 4 \\ 2 & 2 & 10 & 6 \end{pmatrix},$$

reduces to

$$\begin{pmatrix} 1 & 3 & 1 & 2 \\ 1 & 1 & 5 & 4 \\ 0 & 0 & 0 & -2 \end{pmatrix} \qquad \text{(See exercise 4 of this section.)}$$

We can row-reduce this matrix further if we wish. However, any further row-reduction will not substantially change the last row, which, in equation form, is $0x_1 + 0x_2 + 0x_3 = -2$, or simply $0 = -2$. It is clear that we cannot find real numbers x_1, x_2, and x_3 that will satisfy this equation, hence we cannot find real numbers that will satisfy all three original equations simultaneously. When this occurs, we say that the system has no solution, or the solution set is empty.

Example 12.1.3. Next let's attempt to find all of the solutions to:

$$\begin{aligned} x_1 + 6x_2 + 2x_3 &= 1 \\ 2x_1 + x_2 + 3x_3 &= 2 \\ 4x_1 + 2x_2 + 6x_3 &= 4 \end{aligned}$$

The augmented matrix for the system,

$$\begin{pmatrix} 1 & 6 & 2 & 1 \\ 2 & 1 & 3 & 2 \\ 4 & 2 & 6 & 4 \end{pmatrix}$$

reduces to

$$\begin{pmatrix} 1 & 0 & \frac{16}{11} & 1 \\ 0 & 1 & \frac{1}{11} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

If we apply additional elementary row operations to this matrix, it will only become more complicated. In particular, we cannot get a one in the third row, third column. Since the matrix is in simplest form, we will express it in equation format to help us determine the solution set.

$$\begin{aligned} x_1 \qquad + \frac{16}{11}x_3 &= 1 \\ x_2 + \frac{1}{11}x_3 &= 0 \\ 0 &= 0 \end{aligned}$$

Any real numbers will satisfy the last equation. However, the first equation can be rewritten as $x_1 = 1 - \frac{16}{11}x_3$, which describes the coordinate x_1 in terms of x_3. Similarly, the second equation gives $x_1$in terms of x_3. A convenient way of listing the solutions of this system is to use set notation. If we call the solution set of the system S, then

$$S = \left\{\left(1 - \tfrac{16}{11}x_3,\ -\tfrac{1}{11}x_3,\ x_3\right) \,\middle|\, x_3 \in \mathbb{R}\right\}.$$

What this means is that if we wanted to list all solutions, we would replace x_3 by all possible numbers. Clearly, there is an infinite number of solutions, two of which are $(1,\ 0,\ 0)$ and $(-15,\ -1,\ 11)$.

A Word Of Caution: Frequently we may obtain "different-looking" answers to the same problem when a system has an infinite number of answers. Assume a student's solutions set to Example 12.1.3 is $A = \{(1 + 16x_2,\ x_2,\ -11x_3) \mid x_3 \in \mathbb{R}\}$. Certainly the result described by S looks different from that described by A. To see whether they indeed describe the same set, we wish to determine whether every solution produced in S can be generated in A. For example, the solution generated by S when $x_3 = 11$ is $(-15, -1, 11)$. The same triple can be produced by A by taking $x_2 = -1$. We must prove that *every* solution described in S is described in A and, conversely, that every solution described in A is described in S. (See Exercise 6 of this section.)

To summarize the procedure in the Gauss-Jordan technique for solving systems of equations, we attempt to obtain 1's along the main diagonal of the coefficient matrix with 0's above and below the diagonal, as in Example 12.1.1. We may find in attempting this that the closest we can come is to put the coefficient matrix in "simplest" form, as in Example 12.1.3, or we may find that the situation of Example 12.1.1 evolves as part of the process. In this latter case, we can terminate the process and state that the system has no solutions. The final matrix forms of Examples 12.1.1 and 12.1.3 are called echelon forms.

In practice, larger systems of linear equations are solved using computers. Generally, the Gauss-Jordan algorithm is the most useful; however, slight variations of this algorithm are also used. The different approaches share many of the same advantages and disadvantages. The two major concerns of all methods are:

(1) minimizing inaccuracies due to rounding off errors, and

(2) minimizing computer time.

The accuracy of the Gauss-Jordan method can be improved by always choosing the element with the largest absolute value as the pivot element, as in the following algorithm.

Algorithm 12.1.1. *Given a matrix equation $A x = b$, where A is $n \times m$, let C be the augmented matrix $[A \mid b]$. The process of* ***row-reducing to echelon form*** *involves performing the following algorithm where C_i = the i^{th} row of C:*

```
i = 1
j = 1
while (i ≤ n and j ≤ m):
  # Find pivot in column j, starting in row i:
  maxi = i
  for k = i+1 to n:
    if abs(C[k,j]) > abs(C[maxi,j]) then
      maxi := k
  if C[maxi,j] ≠ 0 then
    interchange rows i and maxi
    divide each entry in row i by C[i,j]
    # Now C[i,j] will have the value 1.
    for u = i+1 to n:
      subtract $C[u, j] * C_i$ from $C_u$
      # Now C[u,j] will be 0
    i := i + 1
  end if
  j = j + 1
end while
```

At the end of this algorithm, with the final form of C you can revert back to the equation form of the system and a solution should be clear. In general,
(a) If any row of C is all zeros, it can be ignored.
(b) If any row of C has all zero entries except for the entry in the $(m+1)^{st}$ position, the system has no solution. Otherwise, if a column has no pivot, the variable corresponding to it is a ***free variable****. Variables corresponding to pivots are* ***basic variables*** *and can be expressed in terms of the free variables.*

Example 12.1.4. If we apply Algorithm 12.1.1 to the system

$$\begin{aligned} 5x_1 + x_2 + 2x_3 + x_4 &= 2 \\ 3x_1 + x_2 - 2x_3 \phantom{{}+x_4} &= 5 \\ x_1 + x_2 + 3x_3 - x_4 &= -1 \end{aligned}$$

the augmented matrix

$$C = \begin{pmatrix} 5 & 1 & 2 & 1 & 2 \\ 3 & 1 & -2 & 0 & 5 \\ 1 & 1 & 3 & -1 & -1 \end{pmatrix}$$

is reduced to a new value of C:

$$C = \begin{pmatrix} 1 & 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 0 & -\frac{3}{2} & \frac{3}{2} \\ 0 & 0 & 1 & 0 & -1 \end{pmatrix}$$

therefore x_4 is a free variable in the solution and general solution of the system is

$$x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} - \frac{1}{2} x_4 \\ \frac{3}{2} + \frac{3}{2} x_4 \\ -1 \\ x_4 \end{pmatrix}$$

This conclusion is easy to see if you revert back to the equations that the final value matrix C represents.

Mathematica Note

The *Mathematica* function **RowReduce** does the same reduction as described in Algorithm 12.1.1. For example, here is the result for the system in Example 12.1.4.

$$\mathbf{RowReduce}\left[\begin{pmatrix} \mathbf{5} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{2} \\ \mathbf{3} & \mathbf{1} & \mathbf{-2} & \mathbf{0} & \mathbf{5} \\ \mathbf{1} & \mathbf{1} & \mathbf{3} & \mathbf{-1} & \mathbf{-1} \end{pmatrix}\right]$$

$$\begin{pmatrix} 1 & 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 0 & -\frac{3}{2} & \frac{3}{2} \\ 0 & 0 & 1 & 0 & -1 \end{pmatrix}$$

```
Options[RowReduce]
```

{Method → Automatic, Modulus → 0, Tolerance → Automatic, ZeroTest → Automatic}

Only one caution: One needs to be aware that if the pivoting process continues into the last column, which *Mathematica* will do, there will not be a solution to the system. For example the system

$$\begin{aligned} 2\,x_1 \;\; - x_2 &= 1 \\ 3\,x_2 \;\; - x_1 &= 5 \\ x_1 \;\; + 5\,x_2 &= 7 \end{aligned}$$

has augmented matrix

$$C = \begin{pmatrix} 2 & -1 & 1 \\ -1 & 3 & 5 \\ 1 & 5 & 7 \end{pmatrix}.$$

Here is the computation to row-reduce:

$$\mathbf{RowReduce}\left[\begin{pmatrix} \mathbf{2} & \mathbf{-1} & \mathbf{1} \\ \mathbf{-1} & \mathbf{3} & \mathbf{5} \\ \mathbf{1} & \mathbf{5} & \mathbf{7} \end{pmatrix}\right]$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

The last row of the final form of C is $0 = 1$ and so there is no solution to the original system.

Sage Note

Given an augmented matrix, C, there is a matrix method called `eschewing_form` that can be used to row reduce C. Here is the result for the system in Example 12.1.4. In the assignment of a matrix value to `C`, notice that the first argument is QQ, which indicates that the entries should be rational numbers. As long as all the entries are rational, which is the case here since integers are rational, the row-reduced matrix will be all rational.

```
C = Matrix(QQ,[[5,1,2,1,2],[3,1,-2,0,5],[1,1,3,-1,-1]])
C.echelon_form()
     [   1    0    0  1/2  1/2]
     [   0    1    0 -3/2  3/2]
     [   0    0    1    0   -1]
```

If we didn't specify the set from which entries are taken, it would assumed to be the integers and we would not get a fully row-reduced matrix.

The next step would involve multiplying row 3 by $\frac{1}{9}$, which isn't an integer.

```
C2 = Matrix([[5,1,2,1,2],[3,1,-2,0,5],[1,1,3,-1,-1]])
C2.echelon_form()
     [ 1  1  3 -1 -1]
     [ 0  2  2 -3  1]
     [ 0  0  9  0 -9]
```

This is why we would avoid specifying real entries:

```
C3 = Matrix(RR,[[5,1,2,1,2],[3,1,-2,0,5],[1,1,3,-1,-1]])
C3.echelon_form()
[    1.00000000000000    0.000000000000000    0.000000000000000     0.500000000000000     0.500000000000000]
[   0.000000000000000     1.00000000000000    0.000000000000000     -1.50000000000000      1.50000000000000]
[   0.000000000000000    0.000000000000000     1.00000000000000 4.93432455388958e-17     -1.00000000000000]
```

This is the default number of decimal places, which could be controlled and the single small number in row three column four isn't exactly zero because of round-off and we could just set it to zero. However, the result isn't as nice and clean as the rational output in this case.

EXERCISES FOR SECTION 12.1

A Exercises

1. Solve the following systems by describing the solution sets completely:

(a) $$\begin{aligned} 2x_1 + x_2 &= 3 \\ x_1 - x_2 &= 1 \end{aligned}$$

(b) $$\begin{aligned} 2x_1 + x_2 + 3x_3 &= 5 \\ 4x_1 + x_2 + 2x_3 &= -1 \\ 8x_1 + 2x_2 + 4x_3 &= -2 \end{aligned}$$

(c) $$\begin{aligned} x_1 + x_2 + 2x_3 &= 1 \\ x_1 + 2x_2 - x_3 &= -1 \\ x_1 + 3x_2 + x_3 &= 5 \end{aligned}$$

(d) $$\begin{aligned} x_1 - x_2 + 3x_3 &= 7 \\ x_1 + 3x_2 + x_3 &= 4 \end{aligned}$$

2. Solve the following systems by describing the solution sets completely:

(a) $$\begin{aligned} 2x_1 + 2x_2 + 4x_3 &= 2 \\ 2x_1 + x_2 + 4x_3 &= 0 \\ 3x_1 + 5x_2 + x_3 &= 0 \end{aligned}$$

(b) $$\begin{aligned} 2x_1 + x_2 + 3x_3 &= 2 \\ 4x_1 + x_2 + 2x_3 &= -1 \\ 8x_1 + 2x_2 + 4x_3 &= 4 \end{aligned}$$

(c) $$\begin{aligned} x_1 + x_2 + 2x_3 + x_4 &= 3 \\ x_1 - x_2 + 3x_3 - x_4 &= -2 \\ 3x_1 + 3x_2 + 6x_3 + 3x_4 &= 9 \end{aligned}$$

(d) $$\begin{aligned} 6x_1 + 7x_2 + 2x_3 &= 3 \\ 4x_1 + 2x_2 + x_3 &= -2 \\ 6x_1 + x_2 + x_3 &= 1 \end{aligned}$$

(e) $$\begin{aligned} x_1 + x_2 - x_3 + 2x_4 &= 1 \\ x_1 + 2x_2 + 3x_3 + x_4 &= 5 \\ x_1 + 3x_2 + 2x_3 - x_4 &= -1 \end{aligned}$$

3. Given that the final augmented matrices below obtained from Algorithm 12.1.1, identify the solutions sets. Identify the basic and free variables, and describe the solution set of the original system.

(a) $\begin{pmatrix} 1 & 0 & -5 & 0 & 1.2 \\ 0 & 1 & 4 & 0 & 2.6 \\ 0 & 0 & 0 & 1 & 4.5 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & 0 & 9 & 3 \\ 0 & 1 & 0 & 4 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 0 & 6 & 5 \\ 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & 0 & 0 & -3 & 1 \\ 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 1 & -1 & 1 \end{pmatrix}$

4. (a) Write out the details of Example 12.1.2.

(b) Write out the details of Example 12.1.3.

(c) Write out the details of Example 12.1.4.

5. Solve the following systems using only mod 5 arithmetic. Your solutions should be $n-$ tuples from $\mathbb{Z}_5$.

(a) $\begin{array}{l} 2x_1 + x_2 = 3 \\ x_1 + 4x_2 = 1 \end{array}$ (compare your solution to the system in 5(a))

(b) $\begin{array}{l} x_1 + x_2 + 2x_3 = 1 \\ x_1 + 2x_2 + 4x_3 = 4 \\ x_1 + 3x_2 + 3x_3 = 0 \end{array}$

6. (a) Use the solution set S of Example 12.1.3 to list three different solutions to the given system. Then show that each of these solutions can be described by the set A of Example 12.1.3.

(b) Prove that S = A.

B Exercise

7. Given a system of n linear equations in n unknowns in matrix form $Ax = b$, prove that if b is a matrix of all zeros, then the solution set of $Ax = b$ is a subgroup of $\mathbb{R}^n$.

12.2 Matrix Inversion

In Chapter 5 we defined the inverse of an $n \times n$ matrix. We noted that not all matrices have inverses, but when the inverse of a matrix exists, it is unique. This enables us to define the inverse of an n × n matrix A as the unique matrix B such that $AB = BA = I$, where I is the $n \times n$ identity matrix. In order to get some practical experience, we developed a formula that allowed us to determine the inverse of invertible 2×2 matrices. We will now use the Gauss-Jordan procedure for solving systems of linear equations to compute the inverses, when they exist, of $n\times n$ matrices, $n \geq 2$. The following procedure for a 3×3 matrix can be generalized for $n\times n$ matrices, $n \geq 2$.

Example 12.2.1. Given the matrix

$$A = \begin{pmatrix} 1 & 1 & 2 \\ 2 & 1 & 4 \\ 3 & 5 & 1 \end{pmatrix}$$

we want to find the matrix

$$B = \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{pmatrix},$$

if it exists, such that (a) $AB = I$ and (b) $BA = I$. We will concentrate on finding a matrix that satisfies Equation (a) and then verify that B also satisfies Equation (b).

$$\begin{pmatrix} 1 & 1 & 2 \\ 2 & 1 & 4 \\ 3 & 5 & 1 \end{pmatrix}\begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is equivalent to

$$\begin{pmatrix} x_{11} + x_{21} + 2x_{31} & x_{12} + x_{22} + 2x_{32} & x_{13} + x_{23} + 2x_{33} \\ 2x_{11} + x_{21} + 4x_{31} & 2x_{12} + x_{22} + 4x_{32} & 2x_{13} + x_{23} + 4x_{33} \\ 3x_{11} + 5x_{21} + x_{31} & 3x_{12} + 5x_{22} + x_{32} & 3x_{13} + 5x_{23} + x_{33} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (12.2.a)$$

By definition of equality of matrices, this gives us three systems of equations to solve. The augmented matrix of one of the 12.2a systems, the one equating the first columns of the two matrices is:

$$\begin{pmatrix} 1 & 1 & 2 & 1 \\ 2 & 1 & 4 & 0 \\ 3 & 5 & 1 & 0 \end{pmatrix} \quad (12.2.b)$$

Using the Gauss-Jordan technique of Section 12.1, we have:

$$\begin{pmatrix}1&1&2&1\\2&1&4&0\\3&5&1&0\end{pmatrix}\xrightarrow{-2R_1+R_2}\begin{pmatrix}1&1&2&1\\0&-1&0&-2\\3&5&1&0\end{pmatrix}\xrightarrow{-3R_1+R_3}\begin{pmatrix}1&1&2&1\\0&-1&0&-2\\0&2&-5&-3\end{pmatrix}$$

$$\xrightarrow{-1R_2}\begin{pmatrix}1&1&2&1\\0&1&0&2\\0&2&-5&-3\end{pmatrix}\xrightarrow{\substack{-R_2+R_1\\ \text{and } -2R_2+R_3}}\begin{pmatrix}1&0&2&-1\\0&1&0&2\\0&0&-5&-7\end{pmatrix}$$

$$\xrightarrow{-\frac{1}{5}R_3}\begin{pmatrix}1&0&2&-1\\0&1&0&2\\0&0&1&7/5\end{pmatrix}\xrightarrow{-2R_3+R_1}\begin{pmatrix}1&0&0&-\frac{19}{5}\\0&1&0&2\\0&0&1&\frac{7}{5}\end{pmatrix}$$

So $x_{11} = -19/5$, $x_{21} = 2$ and $x_{31} = 7/5$, which gives us the first column of the matrix B. The matrix form of the system to obtain x_{12}, x_{22}, and x_{32} , the second column of B, is:

$$\begin{pmatrix}1&1&2&0\\2&1&4&1\\3&5&1&0\end{pmatrix} \qquad (12.2.c)$$

which reduces to

$$\begin{pmatrix}1&0&0&\frac{9}{5}\\0&1&0&-1\\0&0&1&-\frac{2}{5}\end{pmatrix} \qquad (12.2.d)$$

The critical idea to note here is that the coefficient matrix in 12.2c is the same as the matrix in 12.2b, hence the sequence of row operations that we used to reduce the matrix in 12.2b can be used to reduce the matrix in 12.2c. To determine the third column of B, we reduce

$$\begin{pmatrix}1&1&2&0\\2&1&4&0\\3&5&1&1\end{pmatrix}$$

to obtain $x_{13} = 2/5$, $x_{23} = 0$ and $x_{33} = -1/5$,. Here again it is important to note that the sequence of row operations used to "solve" this system is exactly the same as those we used in the first system. Why not save ourselves a considerable amount of time and effort and solve all three systems simultaneously? This we can effect by augmenting the coefficient matrix by the identity matrix I. We then have

$$\begin{pmatrix}1&1&2&1&0&0\\2&1&4&0&1&0\\3&5&1&0&0&1\end{pmatrix}\xrightarrow{\substack{\text{Same sequence of row}\\ \text{operations as above}}}\begin{pmatrix}1&0&0&-\frac{19}{5}&\frac{9}{5}&\frac{2}{5}\\0&1&0&2&-1&0\\0&0&1&\frac{7}{5}&-\frac{2}{5}&-\frac{1}{5}\end{pmatrix}$$

So that

$$B = \begin{pmatrix}-\frac{19}{5}&\frac{9}{5}&\frac{2}{5}\\2&-1&0\\\frac{7}{5}&-\frac{2}{5}&-\frac{1}{5}\end{pmatrix}$$

The reader should verify that $BA = I$ so that $A^{-1} = B$.

As the following theorem indicates, the verification that $BA = I$ is not necessary. The proof of the theorem is beyond the scope of this text. The interested reader can find it in most linear algebra texts.

Theorem 12.2.1. *Let A be an $n \times n$ matrix. If a matrix B can be found such that $AB = I$, then $BA = I$, so that $B = A^{-1}$. In fact, to find A^{-1}, we need only find a matrix B that satisfies one of the two conditions $AB = I$ or $BA = I$.*

It is clear from Chapter 5 and our discussions in this chapter that not all $n \times n$ matrices have inverses. How do we determine whether a matrix has an inverse using this method? The answer is quite simple: the technique we developed to compute inverses is a matrix approach to solving several systems of equations simultaneously.

Example 12.2.2. The reader can verify that if

$$A = \begin{pmatrix}1&2&1\\-1&-2&-1\\0&5&8\end{pmatrix}$$

then the augmented matrix

$$\begin{pmatrix} 1 & 2 & 1 & 1 & 0 & 0 \\ -1 & -2 & -2 & 0 & 1 & 0 \\ 0 & 5 & 8 & 0 & 0 & 1 \end{pmatrix}$$

reduces to

$$\begin{pmatrix} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 5 & 8 & 0 & 0 & 1 \end{pmatrix} \qquad (12.2.e)$$

Although this matrix can be row-reduced further, it is not necessary to do so since in equation form we have:

$$\text{(i)} \begin{array}{r} x_{11} + 2\,x_{21} + x_{31} = 1 \\ 0 = 1 \\ 5\,x_{21} + 8\,x_{31} = 0 \end{array} \quad \text{(ii)} \begin{array}{r} x_{12} + 2\,x_{22} + x_{32} = 0 \\ 0 = 1 \\ 5\,x_{22} + 8\,x_{32} = 0 \end{array} \quad \text{(iii)} \begin{array}{r} x_{13} + 2\,x_{23} + x_{33} = 0 \\ 0 = 0 \\ 5\,x_{23} + 8\,x_{33} = 1 \end{array}$$

Clearly, there is no solution to Systems (i) and (ii), therefore A^{-1} does not exist. From this discussion it should be obvious to the reader that the zero row of the coefficient matrix together with the nonzero entry in the fourth column of that row in matrix 12.2e tells us that A^{-1} does not exist.

EXERCISES FOR SECTION 12.2

A Exercises

1. In order to develop an understanding of the technique of this section, work out all the details of Example 12.2.1.

2. Use the method of this section to find the inverses of the following matrices whenever possible. If an inverse does not exist, explain why.

(a) $\begin{pmatrix} 1 & 2 \\ -1 & 3 \end{pmatrix}$ (b) $\begin{pmatrix} 0 & 3 & 2 & 5 \\ 1 & -1 & 4 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 3 & -1 \end{pmatrix}$

(c) $\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & 2 & 1 \\ -2 & -3 & -1 \\ 1 & 4 & 4 \end{pmatrix}$

(e) $\begin{pmatrix} 6 & 7 & 2 \\ 4 & 2 & 1 \\ 6 & 1 & 1 \end{pmatrix}$ (f) $\begin{pmatrix} 2 & 1 & 3 \\ 4 & 2 & 1 \\ 8 & 2 & 4 \end{pmatrix}$

3. Same as question 2:

(a) $\begin{pmatrix} \frac{1}{3} & 2 \\ \frac{1}{5} & -1 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 0 & 0 & 3 \\ 2 & -1 & 0 & 6 \\ 0 & 2 & 1 & 0 \\ 0 & -1 & 3 & 2 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 1 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & 0 & 0 \\ 2 & 2 & -1 \\ 1 & -1 & 1 \end{pmatrix}$

(e) $\begin{pmatrix} 2 & 3 & 4 \\ 3 & 4 & 5 \\ 4 & 5 & 6 \end{pmatrix}$ (f) $\begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{3} \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{5} \end{pmatrix}$

4. (a) Find the inverses of the following matrices.

(i) $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 5 \end{pmatrix}$ (ii) $\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & \frac{5}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{7} & 0 \\ 0 & 0 & 0 & \frac{3}{4} \end{pmatrix}$

(b) If D is a diagonal matrix whose diagonal entries are nonzero, what is D^{-1} ?

5. Express each system of equations in Exercise 1, Section 12.1, in the form $A x = B$. Solve each system by first finding A^{-1} whenever possible.

12.3 An Introduction to Vector Spaces

When we encountered various types of matrices in Chapter 5, it became apparent that a particular kind of matrix, the diagonal matrix, was much easier to use in computations. For example, if $A = \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix}$, then A^5 can be found, but its computation is tedious. If

$$D = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$$

then

$$D^5 = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}^5 = \begin{pmatrix} 1^5 & 0 \\ 0 & 4^5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1024 \end{pmatrix}$$

In a variety of applications it is beneficial to be able to diagonalize a matrix. In this section we will investigate what this means and consider a few applications. In order to understand when the diagonalization process can be performed, it is necessary to develop several of the underlying concepts of *linear algebra*.

By now, you realize that mathematicians tend to generalize. Once we have found a "good thing," something that is useful, we apply it to as many different concepts as possible. In doing so, we frequently find that the "different concepts" are not really different but only look different. Four sentences in four different languages might look dissimilar, but when they are translated into a common language, they might very well express the exact same idea.

Early in the development of mathematics, the concept of a vector led to a variety of applications in physics and engineering. We can certainly picture vectors, or "arrows," in the $x y -$ plane and even in the three-dimensional space. Does it make sense to talk about vectors in four-dimensional space, in ten-dimensional space, or in any other mathematical situation? If so, what is the essence of a vector? Is it its shape or the rules it follows? The shape in two- or three-space is just a picture, or geometric interpretation, of a vector. The essence is the rules, or properties, we wish vectors to follow so we can manipulate them algebraically. What follows is a definition of what is called a *vector space*. It is a list of all the essential properties of vectors, and it is the basic definition of the branch of mathematics called linear algebra.

Definition: Vector Space. *Let V be any nonempty set of objects. Define on V an operation, called addition, for any two elements $\vec{x}$, $\vec{y} \in V$, and denote this operation by $\vec{x} + \vec{y}$. Let scalar multiplication be defined for a real number $a \in \mathbb{R}$ and any element $\vec{x} \in V$ and denote this operation by $a \vec{x}$. The set V together with operations of addition and scalar multiplication is called a vector space over $\mathbb{R}$ if the following hold for all $\vec{x}$, $\vec{y}$, $\vec{z} \in V$, and a, b $\in \mathbb{R}$:*

(1) $\vec{x} + \vec{y} = \vec{y} + \vec{x}$

(2) $(\vec{x} + \vec{y}) + \vec{z} = \vec{x} + (\vec{y} + \vec{z})$

(3) There exists a vector $\vec{0} \in V$*, such that it* $\vec{x} + \vec{0} = \vec{x}$

(4) For each vector $\vec{x} \in V$*, there exists a unique vector* $-\vec{x} \in V$*, such that* $-\vec{x} + \vec{x} \in V = 0$.

These are the main properties associated with the operation of addition. They can be summarized by saying that $[V; +]$ *is an abelian group.*

The next five properties are associated with the operation of scalar multiplication and how it relates to vector addition.

(5) $a(\vec{x} + \vec{y}) = a \vec{x} + a \vec{y}$

(6) $(a + b) \vec{x} = a \vec{x} + b \vec{x}$

(7) $a (b \vec{x}) = (a b) \vec{x}$

(8) $1 \vec{x} = \vec{x}$.

In a vector space it is common to call the elements of V vectors and those from $\mathbb{R}$ scalars. Vector spaces over the real numbers are also called real vector spaces.

Example 12.3.1. Let $V = M_{2\times3}(\mathbb{R})$ and let the operations of addition and scalar multiplication be the usual operations of addition and scalar multiplication on matrices. Then V together with these operations is a real vector space. The reader is strongly encouraged to verify the definition for this example before proceeding further (see Exercise 3 of this section). Note we can call the elements of $M_{2\times3}(\mathbb{R})$ vectors even though they are not arrows.

Example 12.3.2. Let $\mathbb{R}^2 = \{(a_1, a_2) \mid a_1, a_2 \in \mathbb{R}\}$. If we define addition and scalar multiplication the natural way, that is, as we would on 1×2 matrices, then $\mathbb{R}^2$ is a vector space over R. (See Exercise 4 of this section.

In this example, we have the "bonus" that we can illustrate the algebraic concept geometrically. In mathematics, a "geometric bonus" does not always occur and is not necessary for the development or application of the concept. However, geometric illustrations are quite useful in helping us understand concepts and should be utilized whenever available.

Let's consider some illustrations of the vector space $\mathbb{R}^2$. Let $\vec{x} = (1,\ 4)$ and $\vec{y} = (3,\ 1)$.\

We illustrate the vector $(a_1,\ a_2)$ as a directed line segment, or "arrow," from the point (0, 0) to the point $(a_1,\ a_2)$. The vectors $\vec{x}$ and $\vec{y}$ are as pictured in Figure 12.3.1 together with $\vec{x} + \vec{y} = (1,\ 4) + (3,\ 1) = (4,\ 5)$, which also has the geometric representation as pictured in Figure 12.3.1. The vector $2\vec{x} = 2(1,\ 4) = (2,\ 8)$ is a vector in the same direction as $\vec{x}$, but with twice its length.

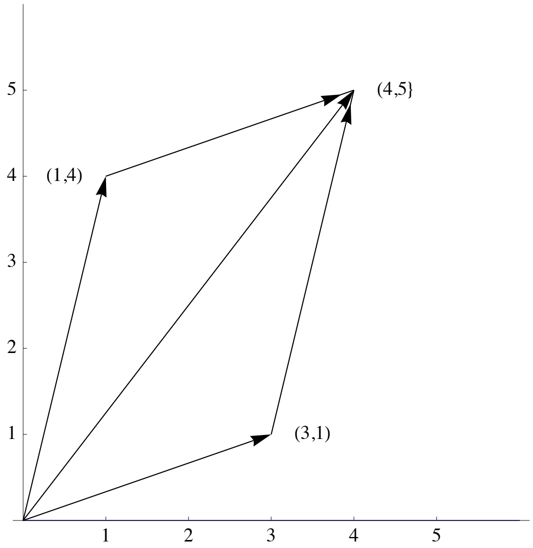


Figure 12.3.1
Addition in $\mathbb{R}^2$

Remarks:

(1) We will henceforth drop the arrow above a vector name and use the common convention that boldface letters toward the end of the alphabet are vectors, while letters early in the alphabet are scalars.

(2) The vector $(a_1,\ a_2,\ \ldots,\ a_n) \in \mathbb{R}^n$ is referred to as an n-tuple.

(3) For those familiar with vector calculus, we are expressing the vector $x = a_1\,\boldsymbol{i} + a_2\,\boldsymbol{j} + a_3\,\boldsymbol{k} \in \mathbb{R}^3$ as $(a_1,\ a_2,\ a_3)$. This allows us to discuss vectors in $\mathbb{R}^n$ in much simpler notation.

In many situations a vector space V is given and we would like to describe the whole vector space by the smallest number of essential reference vectors. An example of this is the description of $\mathbb{R}^2$, the xy plane, via the x and y axes. Again our concepts must be algebraic in nature so we are not restricted solely to geometric considerations.

Definition: Linear Combination. *A vector* $\boldsymbol{y}$ *in vector space V (over* $\mathbb{R}$*) is a linear combination of the vectors* $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$ *if there exist scalars* $a_1, a_2, \ldots, a_n$ *in* $\mathbb{R}$ *such that* $\boldsymbol{y} = a_1\,\boldsymbol{x}_1 + a_2\,\boldsymbol{x}_2 + \ldots + a_n\,\boldsymbol{x}_n$

Example 12.3.3 The vector (2, 3) in $\mathbb{R}^2$ is a linear combination of the vectors (1, 0) and (0, 1) since $(2,\ 3) = 2(1,\ 0) + 3(0,\ 1)$.

Example 12.3.4. Prove that the vector (5, 4) is a linear combination of the vectors (4, 1) and (1, 3). By the definition we must show that there exist scalars a_1 and a_2 such that:

$$(5,\ 4) = a_1(4,\ 1) + a_2(1,\ 3),$$

which reduces to

$$(5,\ 4) = (4\,a_1 + a_2\ ,\ a_1 + 3\,a_2),$$

which gives us the system of linear equations

$$\begin{aligned} 4\,a_1 \ \ + a_2 &= 5 \\ a_1 + 3\,a_2 &= 4 \end{aligned}$$

which has solution $a_1 = 1, a_2 = 1$.

Another way of looking at the above example is if we replace a_1 and a_2 both by 1, then the two vectors (4, 1) and (1, 3) produce, or generate, the vector (5,4). Of course, if we replace a_1 and a_2 by different scalars, we can generate more vectors from $\mathbb{R}^2$. If $a_1 = 3$ and $a_2 = -2$, then

$$\begin{aligned} a_1(4,\ 1) + a_2(1,\ 3) &= 3(4,\ 1) + (-2)(1,\ 3) \\ &= (12,\ 3) + (-2,\ -6) \\ &= (12 - 2, 3 - 6) = (10,\ -3) \end{aligned}$$

Example 12.3.5. Will the vectors (4, 1) and (1, 3) generate any vector we choose in $\mathbb{R}^2$? To see if this is so, we let (b_1, b_2) be an arbitrary vector in $\mathbb{R}^2$ and see if we can always find scalars a_1 and a_2 such that $a_1(4, 1) + a_2(1, 3) = (b_1, b_2)$. This is equivalent to solving the following system of equations:

$$\begin{aligned} 4a_1 \;+\; a_2 &= b_1 \\ a_1 + 3a_2 &= b_2 \end{aligned}$$

which always has solutions for a_1 and a_2 regardless of the values of the real numbers b_1 and b_2. Why? We formalize in a definition:

Definition: Generate*. Let* $\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n\}$ *be a set of vectors in a vector space V over* $\mathbb{R}$*. This set is said to generate, or span, V if, for any given vector* $\mathbf{y} \in V$*, we can always find scalars* $a_1, a_2, \ldots, a_n$ *such that* $y = a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + \ldots + a_n\mathbf{x}_n$ *. A set that generates a vector space is called a generating set.*

We now give a geometric interpretation of the above.

We know that the standard coordinate system, x axis and y axis, were introduced in basic algebra in order to describe all points in the xy plane geometrically. It is also quite clear that to describe any point in the plane we need exactly two axes. Form a new coordinate system the following way:

Draw the vector (4, 1) and an axis from the origin through (4, 1) and label it the x' axis. Also draw the vector (1, 3) and an axis from the origin through (1, 3) to be labeled the y' axis. Draw the coordinate grid for the axis, that is, lines parallel, and let the unit lengths of this "new" plane be the lengths of the respective vectors, (4, 1) and (1, 3), so that we obtain Figure 12.3.2.

From Example 12.3.5 and Figure 12.3.2, we see that any vector on the plane can be described using the old (standard xy) axes or our new $x'y'$ axes. Hence the position which had the name (4, 1) in reference to the standard axes has the name (1, 0) with respect to the $x'y'$ axes, or, in the phraseology of linear algebra, the coordinates of the point (1, 3) with respect to the $x'y'$ axes are (1, 0).

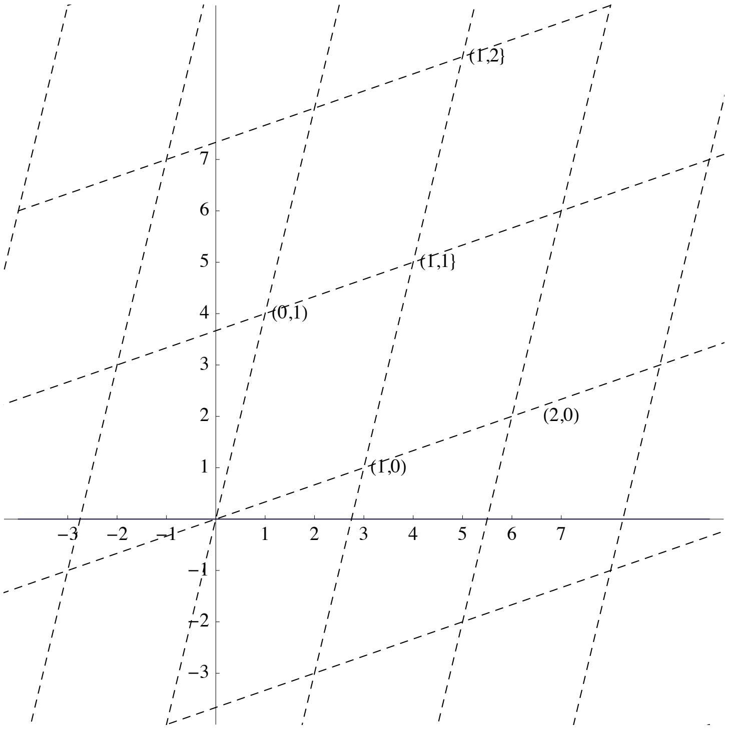


Figure 12.3.2

Example 12.3.6. From Example 12.3.4 we found that if we choose $a_1 = 1$ and $a_2 = 1$, then the two vectors (4, 1) and (1, 3) generate the vector (5, 4). Another geometric interpretation of this problem is that the coordinates of the position (5, 4) with respect to the $x'y'$ axes of Figure 12.3.2 is (1, 1). In other words, a position in the plane has the name (5, 4) in reference to the xy axes and the same position has the name (1, 1) in reference to the $x'y'$ axes.

From the above, it is clear that we can use different axes to describe points or vectors in the plane. No matter what choice we use, we want to be able to describe each position in a unique manner. This is not the case in Figure 12.3.3. Any point in the plane could be described via the $x'y'$ axes, the $x'z'$ axes or the $y'z'$ axes. Therefore, in this case, a single point would have three different names, a very confusing situation.

We formalize the above discussion in two definitions and a theorem.

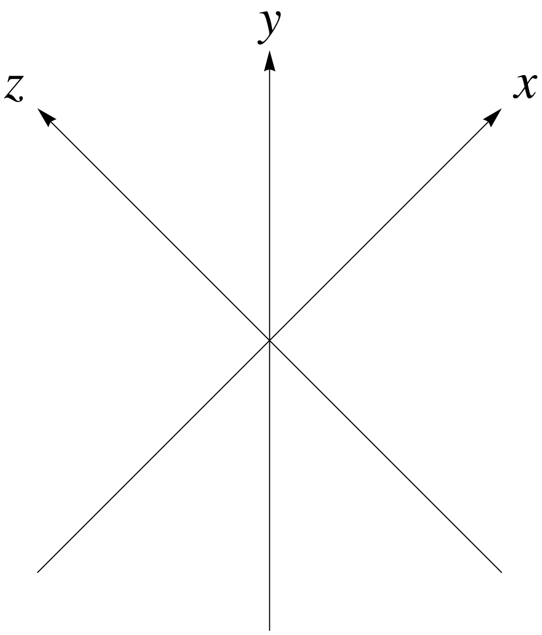


Figure 12.3.3

Definition: Linear Independence/Linear Dependence. *The set of vectors* $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$ *a vector space V (over* $\mathbb{R}$*) is linearly independent if the only solution to the equation* $a_1 \boldsymbol{x}_1 + a_2 \boldsymbol{x}_2 + \ldots + a_3 \boldsymbol{x}_3 = \boldsymbol{0}$ *is* $a_1 = a_2 = \ldots = a_n = 0$*. Otherwise the set is called a linearly dependent set.*

Definition: Basis. *A set of vectors* $B = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$ *is a basis for a vector space V (over* $\mathbb{R}$*) if:*

(1) B generates V, and

(2) B is linearly independent.

Theorem 12.3.1. If $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$ is a basis for a vector space V over $\mathbb{R}$, then any vector $y \in V$ can be uniquely expressed as a linear combination of the $\boldsymbol{x}_i$'s.

Proof: Assume that $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$ is a basis for V over $\mathbb{R}$. We must prove two facts:

(1) each vector $y \in V$ can be expressed as a linear combination of the $\boldsymbol{x}_i$'s, and

(2) each such expression is unique.

Part (1) is trivial since a basis, by its definition, must be a generating set for V.

The proof of (2) is a bit more difficult. We follow the standard approach for any uniqueness facts. Let **y** be any vector in V and assume that there are two different ways of expressing y, namely

$$y = a_1 \boldsymbol{x}_1 + a_2 \boldsymbol{x}_2 + \ldots + a_n \boldsymbol{x}_n$$

and

$$y = b_1 \boldsymbol{x}_1 + b_2 \boldsymbol{x}_2 + \ldots + b_n \boldsymbol{x}_n$$

where at least one a_i is different from the corresponding b_i. Then equating these two linear combinations we get

$$a_1 \boldsymbol{x}_1 + a_2 \boldsymbol{x}_2 + \ldots + a_n \boldsymbol{x}_n = b_1 \boldsymbol{x}_1 + b_2 \boldsymbol{x}_2 + \ldots + b_n \boldsymbol{x}_n$$

so that

$$(a_1 - b_1) \boldsymbol{x}_1 + (a_2 - b_2) \boldsymbol{x}_2 + \ldots + (a_n - b_n) \boldsymbol{x}_n = \boldsymbol{0}$$

Now a crucial observation: since the $\boldsymbol{x}_i$'s form a linearly independent set, the only solution to the previous equation is that each of the coefficients must equal zero, so $a_i - b_i = 0$ for $i = 1, 2, \ldots, n$. Hence $a_i = b_i$, for all i. This contradicts our assumption that at least one a_i is different from the corresponding b_i, so each vector $\boldsymbol{y} \in V$ can be expressed in one and only one way. ■

Theorem 12.3.1, together with the previous examples, gives us a clear insight into the meaning of linear independence, namely uniqueness.

Example 12.3.7. Prove that $\{(1, 1), (-1, 1)\}$ is a basis for $\mathbb{R}^2$ over $\mathbb{R}$ and explain what this means geometrically. First we must show that the vectors $(1, 1)$ and $(-1, 1)$ generate all of $\mathbb{R}^2$. This we can do by imitating Example 12.3.5 and leave it to the reader (see Exercise 10 of this section). Secondly, we must prove that the set is linearly independent.

Let a_1 and a_2 be scalars such that $a_1(1,\ 1) + a_2\{-1,\ 1) = (0,\ 0)$. We must prove that the only solution to the equation is that a_1 and a_2 must both equal zero. The above equation becomes $(a_1 - a_2\ ,\ a_1 + a_2\ ) = (0,\ 0)$ which gives us the system

$$\begin{aligned} a_1 - a_2 &= 0 \\ a_1 + a_2 &= 0 \end{aligned}$$

The augmented matrix of this system reduces in such way that the only solution is the trivial one of all zeros:

$$\begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \Rightarrow a_1 = a_2 = 0$$

Therefore, the set is linearly independent.

To explain the results geometrically, note through Exercise 12, part a, that the coordinates of each vector $\boldsymbol{y} \in \mathbb{R}^2$ can be determined uniquely using the vectors (1,1) and (-1, 1). The concept of dimension is quite obvious for those vector spaces that have an immediate geometric interpretation. For example, the dimension of $\mathbb{R}^2$ is two and that of $\mathbb{R}^3$ is three. How can we define the concept of dimension algebraically so that the resulting definition correlates with that of $\mathbb{R}^2$ and $\mathbb{R}^3$? First we need a theorem, which we will state without proof.

Theorem 12.3.2. If V is a vector space with a basis containing n elements, then all bases of V contain n elements.

Definition: Dimension. Let V be a vector space over $\mathbb{R}$ with basis $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$. Then the dimension of V is n. We use the notation $\dim V = n$ to indicate that V is n-dimensional

EXERCISES FOR SECTION 12.3

A Exercises

1. If $a = 2, b = -3$,

$$A = \begin{pmatrix} 1 & 0 & -1 \\ 2 & 3 & 4 \end{pmatrix},\quad B = \begin{pmatrix} 2 & -2 & 3 \\ 4 & 5 & 8 \end{pmatrix}, \text{ and } C = \begin{pmatrix} 1 & 0 & 0 \\ 3 & 2 & -2 \end{pmatrix}$$

verify that all properties of the definition of a vector space are true for $M_{2\times 3}(\mathbb{R})$ with these values.

2. Let $a = 3, b = 4, \boldsymbol{x} = (-1,\ 3), \boldsymbol{y} = (2,\ 3)$,and $\boldsymbol{z} = (1,\ 0)$. Verify that all properties of the definition of a vector space are true for $\mathbb{R}^2$ for these values.

3. (a) Verify that $M_{2\times 3}(\mathbb{R})$ is a vector space over $\mathbb{R}$.

(b) Is $M_{m\times n}(\mathbb{R})$ a vector space over $\mathbb{R}$?

4. (a) Verify that $\mathbb{R}^2$ is a vector space over $\mathbb{R}$.

(b) Is $\mathbb{R}^n$ a vector space over $\mathbb{R}$ for every positive integer n?

5. Let $P^3 = \{a_0 + a_1 x + a_2 x^2 + a_3 x^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{R}\}$; that is, P^3 is the set of all polynomials in x having real coefficients with degree less than or equal to 3. Verify that P^3 is a vector space over $\mathbb{R}$.

6. For each of the following, express the vector **y** as a linear combination of the vectors x_1 and x_2.

(a) $\boldsymbol{y} = (5,\ 6),\ \boldsymbol{x}_1 = (1,\ 0)$, and $\boldsymbol{x}_2 = (0,\ 1)$

(b) $\boldsymbol{y} = (2,\ 1),\ \boldsymbol{x}_1 = (2,\ 1)$, and $\boldsymbol{x}_2 = (1,\ 1)$

(c) $\boldsymbol{y} = (3, 4),\ \boldsymbol{x}_1 = (1,\ 1)$, and $\boldsymbol{x}_2 = (-1,\ 1)$

7. Express the vector $\begin{pmatrix} 1 & 2 \\ -3 & 3 \end{pmatrix} \in M_{2\times 2}(\mathbb{R})$, as a linear combination of

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 5 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

8. Express the vector x^3 $- 4x^2 + 3 \in P^3$ as a linear combination of the vectors $1, x, x^2$, and x^3.

9. (a) Show that the set $\{\boldsymbol{x}_1, \boldsymbol{x}_2\}$ generates $\mathbb{R}^2$ for each of the parts in Exercise 6 of this section.

(b) Show that $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3\}$ generates $\mathbb{R}^2$ where $\boldsymbol{x}_1 = (1,\ 1),\ \boldsymbol{x}_2 = (3, 4)$, and $\boldsymbol{x}_3 = (-1,\ 5)$.

(c) Create a set of four or more vectors that generates $\mathbb{R}^2$.

(d) What is the smallest number of vectors needed to generate $\mathbb{R}^2$? $\mathbb{R}^n$?

(e) Show that the set of matrices containing

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

generates $M_{2\times 2}(\mathbb{R})$

(f) Show that $\{1, x, x^2, x^3\}$ generates P^3.

10. Complete Example 12.3.7 by showing that $\{(1, 1), (-1, 1)\}$ generates $\mathbb{R}^2$

11. (a) Prove that $\{(4, 1), (1, 3)\}$ is a basis for $\mathbb{R}^2$ over $\mathbb{R}$.

(b) Prove that $\{(1, 0), (3, 4)\}$ is a basis for $\mathbb{R}^2$ over $\mathbb{R}$.

(c) Prove that $\{(1, 0, -1), (2, 1, 1), (1, -3, -1)\}$ is a basis for $\mathbb{R}^3$ over $\mathbb{R}$.

(d) Prove that the sets in Exercise 9, parts e and f, form bases of the respective vector spaces.

12. (a) Determine the coordinates of the points or vectors $(3, 4)$, $(-1, 1)$, and $(1, 1)$ with respect to the basis $\{(1, 1), (-1, 1)\}$ of $\mathbb{R}^3$. Interpret your results geometrically,

(b) Determine the coordinates of the points or vector $(3, 5, 6)$ with respect to the basis $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$. Explain why this basis is called the standard basis for $\mathbb{R}^3$.

13. (a) Let $\boldsymbol{y}_1 = (1, 3, 5, 9)$, $\boldsymbol{y}_2 = (5, 7, 6, 3)$, and $c = 2$. Find $\boldsymbol{y}_1 + \boldsymbol{y}_2$ and $c\,\boldsymbol{y}_1$.

(b) Let $f_1(x) = 1 + 3x + 5x^2 + 9x^3$, $f_2(x) = 5 + 7x + 6x^2 + 3x^3$ and $c = 2$. Find $f_1(x) + f_2(x)$ and $c\,f_1(x)$.

(c) Let $A = \begin{pmatrix} 1 & 3 \\ 5 & 9 \end{pmatrix}$, $B = \begin{pmatrix} 5 & 7 \\ 6 & 3 \end{pmatrix}$, and $c = 2$. Find $A + B$ and $c\,A$.

(d) Are the vector spaces $\mathbb{R}^4$, P^3 and $M_{2\times 2}(\mathbb{R})$ isomorphic to each other? Discuss with reference to parts a, b, and c.

12.4 The Diagonalization Process

We now have the background to understand the main ideas behind the diagonalization process.

Definition: Eigenvalue, Eigenvector. *Let A be an $n \times n$ matrix over $\mathbb{R}$. λ is an eigenvalue of A if for some nonzero column vector $\boldsymbol{x} \in \mathbb{R}^n$ we have $A\boldsymbol{x} = \lambda\boldsymbol{x}$. $\boldsymbol{x}$ is called an Eigenvectors corresponding to the eigenvalue λ.*

Example 12.4.1. Find the eigenvalues and corresponding eigenvectors of the matrix $A = \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix}$. We want to find nonzero vectors $\boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ and real numbers λ such that

$$\begin{aligned} A X = \lambda X \quad &\Leftrightarrow \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \lambda \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \\ &\Leftrightarrow \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} - \lambda \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \\ &\Leftrightarrow \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \\ &\Leftrightarrow \left(\begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \\ &\Leftrightarrow \begin{pmatrix} 2-\lambda & 1 \\ 2 & 3-\lambda \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \qquad \text{(12.4 a)} \end{aligned}$$

The last matrix equation will have nonzero solutions if and only if

$$\det\begin{pmatrix} 2-\lambda & 1 \\ 2 & 3-\lambda \end{pmatrix} = 0$$

or $(2-\lambda)(3-\lambda) - 2 = 0$, which simplifies to $\lambda^2 - 5\lambda + 4 = 0$. Therefore, the solutions to this quadratic equation, $\lambda_1 = 1$ and $\lambda_2 = 4$, are the eigenvalues of A. We now have to find eigenvectors associated with each eigenvalue.

Case 1. For $\lambda_1 = 1$, Equation 12.4a becomes:

$$\begin{pmatrix} 2-1 & 1 \\ 2 & 3-1 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

which reduces to the single equation, $x_1 + x_2 = 0$. From this, $x_1 = -x_2$. This means the solution set of this equation is (in column notation)

$$E_1 = \left\{\begin{pmatrix} -c \\ c \end{pmatrix} \middle| \; c \in \mathbb{R}\right\}$$

So any column vector of the form $\begin{pmatrix} -c \\ c \end{pmatrix}$ where c is any nonzero real number is an eigenvector associated with $\lambda_1 = 1$. The reader should verify that, for example,

$$\begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} \frac{2}{3} \\ -\frac{2}{3} \end{pmatrix} = 1\begin{pmatrix} \frac{2}{3} \\ -\frac{2}{3} \end{pmatrix}$$

so that $\begin{pmatrix} \frac{2}{3} \\ -\frac{2}{3} \end{pmatrix}$ is an eigenvector associated with eigenvalue 1.

Case 2. For $\lambda_2 = 4$ equation 12.4.a becomes:

$$\begin{pmatrix} 2-4 & 1 \\ 2 & 3-4 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$
$$\begin{pmatrix} -2 & 1 \\ 2 & -1 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

which reduces to the single equation $-2x_1 + x_2 = 0$, so that $x_2 = 2x_1$. The solution set of the equation is

$$E_2 = \left\{\begin{pmatrix} c \\ -2c \end{pmatrix} \middle| \; c \in \mathbb{R}\right\}$$

Therefore, all eigenvectors of A associated with the eigenvalue $\lambda_2 = 4$ are of the form $\begin{pmatrix} c \\ -2c \end{pmatrix}$, where c can be any nonzero number.

The following theorems summarize the more important aspects of this example:

Theorem 12.4.1. *Let A be any $n \times n$ matrix over $\mathbb{R}$. Then $\lambda \in \mathbb{R}$ is an eigenvalue of A if and only if $\det(A - \lambda I) = 0$.*

The equation $\det(A - \lambda I) = 0$ is called the *characteristic equation* and the left side of this equation is called the *characteristic polynomial* of A.

Theorem 12.4.2. *Nonzero eigenvectors corresponding to distinct eigenvalues are linearly independent.*

The solution space of $(A - \lambda I)\boldsymbol{x} = \boldsymbol{0}$ is called the *eigenspace of A corresponding to λ*. This terminology is justified by Exercise 2 of this section.

We now consider the main aim of this section. Given an $n \times n$ (square) matrix A, we would like to "change" A into a diagonal matrix D, perform our tasks with the simpler matrix D, and then describe the results in terms of the given matrix A.

Definition: Diagonalizable Matrix. *An $n \times n$ matrix A is called diagonalizable if there exists an invertible $n \times n$ matrix P such that $P^{-1} A P$ is a diagonal matrix D. The matrix P is said to diagonalize the matrix A.*

Example 12.4.2. We will now diagonalize the matrix A of Example 12.4.1. Form the matrix P as follows: Let $P^{(1)}$ be the first column of P. Choose for $P^{(1)}$ any eigenvector from E_1. We may as well choose a simple vector in E_1 so $P^{(1)} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ is our candidate. Similarly, let $P^{(2)}$ be the second

column of P, and choose for $P^{(2)}$ any eigenvector from E_2. The vector $P^{(2)} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ is a reasonable choice, thus

$$P = \begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix} \quad \text{and} \quad P^{-1} = \frac{1}{3}\begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} \frac{2}{3} & -\frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} \end{pmatrix}$$

So that

$$P^{-1} A P = \frac{1}{3}\begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$$

Notice that the elements on the main diagonal of D are the eigenvalues of A, where $D_{i\,i}$ is the eigenvalue corresponding to the eigenvector $P^{(i)}$.

Remarks:

(1) The first step in the diagonalization process is the determination of the eigenvalues. The ordering of the eigenvalues is purely arbitrary. If we designate $\lambda_1 = 4$ and $\lambda_2 = 1$, the columns of P would be interchanged and D would be $\begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}$ (see Exercise 3b of this section). Nonetheless, the final outcome of the application to which we are applying the diagonalization process would be the same.

(2) If A is an $n \times n$ matrix with distinct eigenvalues, then P is also an $n \times n$ matrix whose columns $P^{(1)}, P^{(2)}, \ldots, P^{(n)}$ are n linearly independent vectors.

Example 12.4.3. Diagonalize the matrix

$$A = \begin{pmatrix} 1 & 12 & -18 \\ 0 & -11 & 18 \\ 0 & -6 & 10 \end{pmatrix}.$$

$$\begin{aligned} \det(A - \lambda I) &= \det\begin{pmatrix} 1-\lambda & 12 & -18 \\ 0 & -\lambda - 11 & 18 \\ 0 & -6 & 10 - \lambda \end{pmatrix} \\ &= (1-\lambda)\det\begin{pmatrix} -\lambda - 11 & 18 \\ -6 & 10 - \lambda \end{pmatrix} \\ &= (1-\lambda)\left((-\lambda - 11)(10 - \lambda) + 108\right) \\ &= (1-\lambda)(\lambda^2 + \lambda - 2) \end{aligned}$$

Hence, the equation $\det(A - \lambda I) = 0$ becomes

$$(1-\lambda)(\lambda^2 + \lambda - 2) = -(\lambda - 1)^2(\lambda + 2)$$

Therefore, our eigenvalues for A are $\lambda_1 = -2$ and $\lambda_2 = 1$. We note that we do not have three distinct eigenvalues, but we proceed as in the previous example.

Case 1. For $\lambda_1 = -2$ the equation $(A - \lambda I)\boldsymbol{x} = \boldsymbol{0}$ becomes

$$\begin{pmatrix} 3 & 12 & -18 \\ 0 & -9 & 18 \\ 0 & -6 & 12 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Using *Mathematica*, we can row reduce the matrix:

$$\mathbf{RowReduce}\left[\begin{pmatrix} \mathbf{3} & \mathbf{12} & \mathbf{-18} \\ \mathbf{0} & \mathbf{-9} & \mathbf{18} \\ \mathbf{0} & \mathbf{-6} & \mathbf{12} \end{pmatrix}\right]$$

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{pmatrix}$$

In equation form, the matrix equation is then equivalent to

$$\begin{aligned} x_1 &= -2\,x_3 \\ x_2 &= 2\,x_3 \end{aligned}$$

Therefore, the solution, or eigenspace, corresponding to $\lambda_1 = -2$ consists of vectors of the form

$$\begin{pmatrix} -2\,x_3 \\ 2\,x_3 \\ x_3 \end{pmatrix} = x_3 \begin{pmatrix} -2 \\ 2 \\ 1 \end{pmatrix}$$

Therefore $\begin{pmatrix} -2 \\ 2 \\ 1 \end{pmatrix}$ is an eigenvector corresponding to the eigenvalue $\lambda_1 = -2$, and can be used for our first column of P:

$$P^{(1)} = \begin{pmatrix} -2 \\ 2 \\ 1 \end{pmatrix}$$

Before we continue we make the observation: E_2 is a subspace of $\mathbb{R}^3$ with basis $\{P^{(1)}\}$ and $\dim E_1 = 1$.

Case 2. If $\lambda_2 = 1$, then the equation $(A - \lambda\, I)\,\boldsymbol{x} = \mathbf{0}$ becomes

$$\begin{pmatrix} 0 & 12 & -18 \\ 0 & -12 & 18 \\ 0 & -6 & 9 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Without the aid of any computer technology, it should be clear that all three equations that correspond to this matrix equation are equivalent to $2\,x_2 - 3\,x_3 = 0$, or $x_2 = \frac{3}{2}\,x_3$. Notice that x_1 can take on any value, so any vector of the form

$$\begin{pmatrix} x_1 \\ \frac{3}{2}\,x_3 \\ x_3 \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + x_3 \begin{pmatrix} 0 \\ \frac{3}{2} \\ 1 \end{pmatrix}$$

will solve the matrix equation.

We note that the solution set contains two independent variables, x_1 and x_3. Further, note that we cannot express the eigenspace E_2 as a linear combination of a single vector as in Case 1. However, it can be written as

$$E_2 = \left\{ x_1 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + x_3 \begin{pmatrix} 0 \\ \frac{3}{2} \\ 1 \end{pmatrix} \;\middle|\; x_1, x_3 \in \mathbb{R} \right\}.$$

We can replace any vector in a basis is with a nonzero multiple of that vector. Simply for aesthetic reasons, we will multiply the second vector that generates E_2 by 2. Therefore, the eigenspace E_2 is a subspace of $\mathbb{R}^3$ with basis $\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 2 \end{pmatrix} \right\}$ and so $\dim E_2 = 2$.

What this means with respect to the diagonalization process is that $\lambda_2 = 1$ gives us both Column 2 and Column 3 the diagonalizing matrix. The order is not important. Let

$$P^{(2)} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \text{ and } P^{(3)} = \begin{pmatrix} 0 \\ 3 \\ 2 \end{pmatrix} \text{ and so } P = \begin{pmatrix} -2 & 1 & 0 \\ 2 & 0 & 3 \\ 1 & 0 & 2 \end{pmatrix}$$

The reader can verify (see Exercise 5 of this section) that

$$P^{-1} = \begin{pmatrix} 0 & 2 & -3 \\ 1 & 4 & -6 \\ 0 & -1 & 2 \end{pmatrix} \text{ and } P^{-1} A P = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

In doing Example 12.4.3, the given 3×3 matrix A produced only two, not three, distinct eigenvalues, yet we were still able to diagonalize A. The reason we were able to do so was because we were able to find three linearly independent eigenvectors. Again, the main idea is to produce a matrix P that does the diagonalizing. If A is an $n \times n$ matrix, P will be an $n \times n$ matrix, and its n columns must be linearly independent eigenvectors. The main question in the study of diagonalizability is "When can it be done?" This is summarized in the following theorem.

Theorem 12.4.3. *Let A be an n × n matrix. Then A is diagonalizable if and only if A has n linearly independent eigenvectors.*

Outline of a proof: ($\Longleftarrow$) Assume that A has linearly independent eigenvectors, $P^{(1)}, P^{(2)}, \ldots, P^{(n)}$, with corresponding eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$. We want to prove that A is diagonalizable. Column i of the $n \times n$ matrix $A P$ is $A P^{(i)}$ (see Exercise 7 of this section). Then, since the $P^{(i)}$ is an eigenvector of A associated with the eigenvalue λ_i we have $A P^{(i)} = \lambda_i P^{(i)}$ for $i = 1, 2, \ldots, n$. But this means that $A P = P D$, where D is the diagonal matrix with diagonal entries $\lambda_1, \lambda_2, \ldots, \lambda_n$. If we multiply both sides of the equation by P^{-1} we get the desired $P^{-1} A P = D$.

($\Longrightarrow$) The proof in this direction involves a concept that is not covered in this text (rank of a matrix); so we refer the interested reader to virtually any linear algebra text for a proof. ■

We now give an example of a matrix which is not diagonalizable.

Example 12.4.4. Let us attempt to diagonalize the matrix $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 1 & -1 & 4 \end{pmatrix}$

$$\mathbf{A} = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{2} & \mathbf{1} \\ \mathbf{1} & \mathbf{-1} & \mathbf{4} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 1 & -1 & 4 \end{pmatrix}$$

$$\begin{aligned} \det(A - \lambda I) &= \det \begin{pmatrix} 1-\lambda & 0 & 0 \\ 0 & 2-\lambda & 1 \\ 1 & -1 & 4-\lambda \end{pmatrix} \\ &= (1-\lambda) \det \begin{pmatrix} 2-\lambda & 1 \\ -1 & 4-\lambda \end{pmatrix} \\ &= (1-\lambda)((2-\lambda)(4-\lambda)+1) \\ &= (1-\lambda)(\lambda^2 - 6\lambda + 9) \\ &= (1-\lambda)(\lambda-3)^2 \end{aligned}$$

$$\det(A - \lambda I) = 0 \Rightarrow \lambda = 1 \text{ or } \lambda = 3$$

Therefore there are two eigenvalues, $\lambda_1 = 1$ and $\lambda_2 = 3$. Since λ_1 is an eigenvalue of degree it will have an eigenspace of dimension 1. Since λ_2 is a double root of the characteristic equation, the dimension of its eigenspace must be 2 in order to be able to diagonalize.

Case 1. For $\lambda_1 = 1$, the equation $(A - \lambda I)\boldsymbol{x} = \mathbf{0}$ becomes

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & -1 & 3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

A quick *Mathematica* evaluation make the solution to this system obvious

```
RowReduce[A - IdentityMatrix[3]]
```

$$\begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

There is one free variable, x_3, and

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -4\,x_3 \\ -x_3 \\ x_3 \end{pmatrix} = x_3 \begin{pmatrix} -4 \\ -1 \\ 1 \end{pmatrix}$$

Hence, $\left\{\begin{pmatrix} -4 \\ -1 \\ 1 \end{pmatrix}\right\}$ is a basis for the eigenspace of $\lambda_1 = 1$.

Case 2. For $\lambda_2 = 3$, the equation $(A - \lambda I)\,\boldsymbol{x} = \mathbf{0}$ becomes

$$\begin{pmatrix} -2 & 0 & 0 \\ 0 & -1 & 1 \\ 1 & -1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

```
RowReduce[A - 3 IdentityMatrix[3]]
```

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix}$$

Once again there is only one free variable in the row reduction and so the dimension of the eigenspace will be one:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ x_3 \\ x_3 \end{pmatrix} = x_3 \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

Hence, $\left\{\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}\right\}$ is a basis for the eigenspace of $\lambda_2 = 3$. This means that $\lambda_2 = 3$ produces only one column for P. Since we began with only two eigenvalues, we had hoped that one of them would produce a vector space of dimension two, or, in matrix terms, two linearly independent columns of P. Since A does not have three linearly independent eigenvectors A cannot be diagonalized.

Mathematica Note

Diagonalization can be easily done with a few built-in functions of *Mathematica*. Here is a 3 × 3 matrix we've selected because the eigenvalues are very simple, and could be found by hand with a little work.

$$\mathbf{A} = \begin{pmatrix} \mathbf{4} & \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{5} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} & \mathbf{4} \end{pmatrix};$$

The set of linearly independent eigenvectors of A can be computed:

```
Eigenvectors[A]
```

$$\begin{pmatrix} 1 & 2 & 1 \\ -1 & 0 & 1 \\ 1 & -1 & 1 \end{pmatrix}$$

The rows of this matrix are the eigenvectors, so we transpose the result to get our diagonalizing matrix P whose columns are eigenvectors.

```
P = Transpose[Eigenvectors[A]]
```

$$\begin{pmatrix} 1 & -1 & 1 \\ 2 & 0 & -1 \\ 1 & 1 & 1 \end{pmatrix}$$

We then use P to diagonalize. The entries in the diagonal matrix are the eigenvalues of A.

```
Inverse[P].A.P
```

$$\begin{pmatrix} 6 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

We could have gotten the eigenvalues directly this way:

```
Eigenvalues[A]
```

{6, 4, 3}

Most matrices that are selected at random will not have "nice" eigenvalues. Here is a new matrix *A* that looks similar to the one above.

$$\mathbf{A} = \begin{pmatrix} \mathbf{8} & \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{5} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} & \mathbf{7} \end{pmatrix};$$

Asking for the eigenvalues first, we see that the result is returned symbolically as the three roots to a cubic equation. The default for *Mathematica* is to leave these non-computed. Since the entries of *A* are exact numbers, *Mathematica* is capable of giving an exact solution, but it's very messy. The easiest way around the problem is to make the entries in *A* approximate. The following expression redefines *A* as approximate.

```
A = N[A]
```

$$\begin{pmatrix} 8. & 1. & 0. \\ 1. & 5. & 1. \\ 0. & 1. & 7. \end{pmatrix}$$

Now we can get approximate eigenvalues, and the approximations are very good for most purposes.

```
Eigenvalues[A]
```

{8.3772, 7.27389, 4.34891}

We can verify that the matrix can be diagonalized although due to round-off error some of the off-diagonal entries of the "diagonal" matrix are nonzero.

```
P = Transpose[Eigenvectors[A]]
```

$$\begin{pmatrix} 0.906362 & -0.341882 & 0.248244 \\ 0.341882 & 0.248244 & -0.906362 \\ 0.248244 & 0.906362 & 0.341882 \end{pmatrix}$$

```
Inverse[P].A.P
```

$$\begin{pmatrix} 8.3772 & 2.22045\times 10^{-16} & 6.66134\times 10^{-16} \\ 0. & 7.27389 & 4.44089\times 10^{-16} \\ 1.66533\times 10^{-15} & -4.44089\times 10^{-16} & 4.34891 \end{pmatrix}$$

The **Chop** function will set small numbers to zero. The default thresh hold for "small" is 10^{-10} but that can be adjusted, if desired.

```
Diag = Chop[Inverse[P].A.P]
```

$$\begin{pmatrix} 8.3772 & 0 & 0 \\ 0 & 7.27389 & 0 \\ 0 & 0 & 4.34891 \end{pmatrix}$$

We can't use the name **D** here because *Mathematica* reserves it for the differentiation function.

If you experiment with more matrices, you will undoubtedly encounter situations where some eigenvalues are complex. The process is the same, although we've avoided these just for simplicity.

Sage Note

We start by defining the same matrix as we did in *Mathematica*. We also declare `D` and `P` to be variables.

```
A = Matrix (QQ, [[4, 1, 0], [1, 5, 1], [0, 1, 4]]);A
    [4 1 0]
    [1 5 1]
    [0 1 4]
var (' D, P')
    (D, P)
```

We have been working with "right eigenvectors" since the x in $A x = \lambda x$ is a column vector to the right of *A*. It's not so common but still desirable in some situations to consider "left eigenvectors," so Sage allows either one. The `right_eigenmatrix` method returns a pair of matrices. The diagonal matrix, `D`, with eigenvalues and the diagonalizing matrix, `P`, which is made up of columns that are eigenvectors corresponding to the eigenvectors of `D`.

```
(D,P)=A.right_eigenmatrix();(D,P)


   (
  [6 0 0]  [ 1  1  1]
  [0 4 0]  [ 2  0 -1]
  [0 0 3], [ 1 -1  1]
  )
```

We should note here that **P** is not unique because even if an eigenspace has dimension one, any nonzero vector in that space will serve as an eigenvector. For that reason, the `P` generated by Sage isn't identical to the one generated by *Mathematica*, but they both work. Here we verify the result for our Sage calculation. Recall that an asterisk is used for matrix multiplication in Sage.

```
P.inverse()*A*P
=    [6 0 0]
     [0 4 0]
     [0 0 3]
```

Here is a second matrix, again the same as we used with *Mathematica*.

```
A2=Matrix(QQ,[[8,1,0],[1,5,1],[0,1,7]]);A2
    [8 1 0]
    [1 5 1]
    [0 1 7]
```

Here we've already specified that the underlying system is the rational numbers. Since the eigenvalues are not rational, Sage will revert to approximate number by default. We'll just pull out the matrix of eigenvectors this time and display rounded entries. Here the diagonalizing matrix looks very different from the result from *Mathematica*, but this is because he eigenvalues are not in the same order in the two calculations. They both diagonalize but with a different diagonal matrix.

```
P=A2.right_eigenmatrix()[1]
P.numerical_approx(digits=3)

    [  1.00   1.00   1.00]
    [ -3.65 -0.726  0.377]
    [  1.38  -2.65  0.274]
D=(P.inverse()*A2*P);D.numerical_approx(digits=3)
    [ 4.35 0.000 0.000]
    [0.000  7.27 0.000]
    [0.000 0.000  8.38]
```

EXERCISES FOR SECTION 12.4

A Exercises

1. (a) List three different eigenvectors of $A = \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix}$, the matrix of Example 12.4.1, associated with the two eigenvalues 1 and 4. Verify your results.

((b) Choose one of the three eigenvectors corresponding to 1 and one of the three eigenvectors corresponding to 4, and show that the two chosen vectors are linearly independent.

2. (a) Verify that E_1 and E_2 in Example 12.4.1 are vector spaces over $\mathbb{R}$. Since they are also subsets of $\mathbb{R}^2$, they are called subvector-spaces, or subspaces for short, of $\mathbb{R}^2$. Since these are subspaces consisting of eigenvectors, they are called eigenspaces.

(b) Use the definition of dimension in the previous section to find $\dim E_1$ and $\dim E_2$. Note that $\dim E_1 + \dim E_2 = \dim \mathbb{R}^2$. This is not a coincidence.

3. (a) Verify that $P^{-1} A P$ is indeed equal to $\begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$, as indicated in Example 12.4.2.

(b) Choose $P^{(1)} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ and $P^{(2)} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ and verify that the new value of P satisfies $P^{-1} A P = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$

(c) Take any two linearly independent eigenvectors of the matrix A of Example 12.4.2 and verify that $P^{-1} A P$ is a diagonal matrix.

4. (a) Let A be the matrix in Example 12.4.3 and $P = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 2 \end{pmatrix}$. Without doing any actual matrix multiplications, determine the value of $P^{-1} A P$

(b) If you choose the columns of P in the reverse order, what is $P^{-1} A P$?

5. Diagonalize the following, if possible:

(a) $\begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}$ (b) $\begin{pmatrix} -2 & 1 \\ -7 & 6 \end{pmatrix}$ (c) $\begin{pmatrix} 3 & 0 \\ 0 & 4 \end{pmatrix}$

(d) $\begin{pmatrix} 1 & -1 & 4 \\ 3 & 2 & -1 \\ 2 & 1 & -1 \end{pmatrix}$ (e) $\begin{pmatrix} 6 & 0 & 0 \\ 0 & 7 & -4 \\ 9 & 1 & 3 \end{pmatrix}$ (f) $\begin{pmatrix} 1 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 1 \end{pmatrix}$

6. Diagonalize the following, if possible:

(a) $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ (b) $\begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix}$ (c) $\begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$

(d) $\begin{pmatrix} 1 & 3 & 6 \\ -3 & -5 & -6 \\ 3 & 3 & 6 \end{pmatrix}$ (e) $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ (f) $\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}$

B Exercise

7. Let A and P be as in Example 12.4.3. Show that the columns of the matrix $A P$ can be found by computing $A P^{(1)}, A P^{(2)}, \ldots, A P^{(n)}$.

8. Prove that if P is an $n \times n$ matrix and D is a diagonal matrix with diagonal entries $d_1, d_2, \ldots, d_n$, then $P D$ is the matrix obtained from P, but multiplying column i of P by d_i, $i = 1, 2, \ldots, n$.

C Exercise

9. (a) There is an option to the *Mathematica* functions **Eigenvectors** and **Eigenvalues** called **Cubics** that will use the cubic equation to find exact eigenvalues of a matrix like $\begin{pmatrix} 8 & 1 & 0 \\ 1 & 5 & 1 \\ 0 & 1 & 7 \end{pmatrix}$. Use that option to find the exact eigenvalues of the matrix. Diagonalize the matrix using the **Cubics** option and then convert the result to a matrix of approximate numbers to compare your result with the approximate result we found in the *Mathematica* Note.

12.5 Some Applications

A large and varied number of applications involve computations of powers of matrices. These applications can be found in science, the social sciences, economics, the analysis of relationships with groups, engineering, and, indeed, any area where mathematics is used and, therefore, where programs are to be developed. We will consider a few diverse examples here.

To aid your understanding of the following examples, we develop a helpful technique to compute A^m, $m > 1$. If A can be diagonalized, then there is a matrix P such that $P^{-1} A P = D$, where D is a diagonal matrix and

$$A^m = P D^m P^{-1} \text{ for all } m \geq 1. \qquad (12.5\text{ a})$$

You are asked to prove this equation in Exercise 9 of Section 5.4. The condition that D be a diagonal matrix is not necessary but when it is, the calculation on the right side is particularly easy to perform. Although the formal proof of equation 12.4a is done by induction, the reason *why* it is true is easily seen by writing out an example such as $m = 3$:

$$\begin{aligned} A^m &= (P D P^{-1})^m \quad \text{To get this, solve } P^{-1} A P = D \text{ for } A \text{ and substitute} \\ &= (P D P^{-1})(P D P^{-1})(P D P^{-1}) \\ &= P D (P^{-1} P) D (P^{-1} P) D P^{-1} \quad \text{by associativity of matrix mult.} \\ &= P D I D I D P^{-1} \\ &= P D D D P^{-1} \\ &= P D^3 P^{-1} \end{aligned}$$

Example 12.5.1: Recursion. Consider the computation of terms of the Fibonacci sequence, which we examined in Example 8.1.5:

$F_0 = 1,\ F_1 = 1$

$F_k = F_{k-1} + F_{k-2}$ for $k \geq 2$.

In order to formulate the calculation in matrix form, we introduced the "dummy equation" $F_{k-1} = F_{k-1}$ so that now we have two equations

$$\begin{aligned} F_k &= F_{k-1} + F_{k-2} \\ F_{k-1} &= F_{k-1} \end{aligned}$$

These two equations can be expressed in matrix form as

$$\begin{aligned} \begin{pmatrix} F_k \\ F_{k-1} \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_{k-1} \\ F_{k-2} \end{pmatrix} \quad \text{if } k \geq 2 \\ &= A \begin{pmatrix} F_{k-1} \\ F_{k-2} \end{pmatrix} \quad \text{if } A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \\ &= A^2 \begin{pmatrix} F_{k-2} \\ F_{k-3} \end{pmatrix} \quad \text{if } k \geq 3 \\ &\text{etc.} \quad \text{if } k \text{ is large enough} \end{aligned}$$

We can use induction to prove that if $k \geq 2$,

$$\begin{pmatrix} F_k \\ F_{k-1} \end{pmatrix} = A^{k-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Next, by diagonalizing A and using the fact that $A^m = P D^m P^{-1}$. we can show that

$$F_k = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^k - \left(\frac{1-\sqrt{5}}{2} \right)^k \right)$$

See Exercise la of this section.

Comments:

(1) An equation of the form $F_k = a F_{k-1} + b F_{k-2}$, where a and b are given constants, is referred to linear homogeneous second-order difference equation. The conditions $F_0 = c_0$ and $F_1 = c_1$, where c_1 and c_2 are constants, are called initial conditions. Those of you who are familiar with differential equations may recognize that the this language parallels what is used in differential equations. Difference (AKA recurrence) equations move forward discretely—that is, in a finite number of positive steps—while a differential equation moves continuously—that is, takes an infinite number of infinitesimal steps.

(2) A recurrence relationship of the form $F_k = a F_{k-1} + b$, where a and b are constants, is called a first-order difference equation. In order to write out the sequence, we need to know one initial condition. Equations of this type can be solved similarly to the method outlined in Example 12.5.1 by introducing the superfluous equation $1 = 0\ F_{k-1} + 1$ to obtain in matrix equation:

$$\begin{pmatrix} F_k \\ 1 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} F_{k-1} \\ 1 \end{pmatrix} \Rightarrow \begin{pmatrix} F_k \\ 1 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^k \begin{pmatrix} F_0 \\ 1 \end{pmatrix}$$

Example 12.5.2: Graph Theory. Consider the graph in Figure 12.5.1.

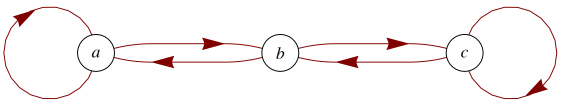


Figure 12.5.1

From the procedures outlined in Section 6.4, the adjacency matrix of this graph is

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

Recall that A^k is the adjacency matrix of the relation r^k , where r is the relation $\{(a, a), (a, b), (b, a), (b, c), (c, b), (c, c)\}$ of the above graph. Also recall that in computing A^k, we used Boolean arithmetic. What happens if we use "regular" arithmetic? For example,

$$A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$$

How can we interpret this? We note that $A_{33} = 2$ and that there are two paths of length two from c (the third node) to c. Also, $A_{13} = 1$, and there is one path of length 2 from a to c. The reader should verify these claims from the graph in Figure 12.5.1.

Theorem 12.5.1. The entry $\left(A^k\right)_{i j}$ is the number of paths, or walks, of length k from node v_i, to node v_j .

How do we find A^k for possibly large values of k? From the discussion at the beginning of this section, we know that $A^k = P D^k P^{-1}$ if A is diagonalizable. We leave to the reader to show that $\lambda = 1,\ 2,$ and -1 are eigenvalues of A with eigenvectors

$$\begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \text{ and} \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$$

respectively, so that

$$A^k = P \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2^k & 0 \\ 0 & 0 & (-1)^k \end{pmatrix} P^{-1}$$

where $P = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & -2 \\ -1 & 1 & 1 \end{pmatrix}$ and $P^{-1} = \begin{pmatrix} \frac{1}{2} & 0 & -\frac{1}{2} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{6} & -\frac{1}{3} & \frac{1}{6} \end{pmatrix}$

See Exercise 5 of this section for the completion of this example.

Example 12.5.3: Matrix Calculus. Those who have studied calculus recall that the Maclaurin series is a useful way of expressing many common functions. For example,

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$$

Indeed, calculators and computers use these series for calculations. Given a polynomial $f(x)$, we defined the matrix-polynomial $f(A)$ for square matrices in Chapter 5. Hence, we are in a position to describe e^A for an $n \times n$ matrix A as a limit of polynomial. Formally, we write

$$e^A = I + A + \frac{A^2}{2!} + \frac{A^3}{3!} + \cdots = \sum_{k=0}^{\infty} \frac{A^k}{k!}$$

Again we encounter the need to compute high powers of a matrix. Let A be an $n \times n$ diagonalizable matrix. Then there exists an invertible $n \times n$ matrix P such that $P^{-1} A P = D$, a diagonal matrix, so that

$$\begin{aligned} e^A &= e^{P D P^{-1}} \\ &= \sum_{k=0}^{\infty} \frac{\left(P D P^{-1}\right)^k}{k!} \\ &= P \left(\sum_{k=0}^{\infty} \frac{D^k}{k!} \right) P^{-1} \end{aligned}$$

The infinite sum in the middle of this final expression can be easily evaluated if D is diagonal. All entries of powers off the diagonal are zero and the i^{th} entry of the diagonal is

$$\left(\sum_{k=0}^{\infty} \frac{D^k}{k!} \right)_{i i} = \sum_{k=0}^{\infty} \frac{{D_{i i}}^k}{k!} = e^{D_{i i}}$$

For example, if $A = \begin{pmatrix} 2 & 1 \\ 2 & 3 \end{pmatrix}$, the first matrix we diagonalized in Section 12.3, we found that $P = \begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix}$ and $D = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$. Therefore,

$$\begin{aligned} e^A &= \begin{pmatrix} 1 & 1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} e & 0 \\ 0 & e^4 \end{pmatrix} \begin{pmatrix} \frac{2}{3} & -\frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} \end{pmatrix} \\ &= \begin{pmatrix} \frac{2e}{3} + \frac{e^4}{3} & -\frac{e}{3} + \frac{e^4}{3} \\ -\frac{2e}{3} + \frac{2e^4}{3} & \frac{e}{3} + \frac{2e^4}{3} \end{pmatrix} \\ &\approx \begin{pmatrix} 20.0116 & 17.2933 \\ 34.5866 & 37.3049 \end{pmatrix} \end{aligned}$$

Comments on Example 12.5.3:

(1) Many of the ideas of calculus can be developed using matrices. For example, if

$$A(t) = \begin{pmatrix} t^3 & 3t^2 + 8t \\ e^t & 2 \end{pmatrix}$$

then

$$\frac{d\,A(t)}{d\,t} = \begin{pmatrix} 3\,t^2 & 6\,t+8 \\ e^t & 0 \end{pmatrix}$$

(2) Many of the basic formulas in calculus are true in matrix calculus. For example,

$$\frac{d\,(A(t)+B(t))}{d\,t} = \frac{d\,A(t)}{d\,t} + \frac{d\,B(t)}{d\,t}$$

and if A is a constant matrix,

$$\frac{d\,e^{A\,t}}{d\,t} = A\,e^{A\,t}$$

(3) Matrix calculus can be used to solve systems of differential equations in a similar manner to the procedure used in ordinary differential equations.

Mathematica Note

Mathematica's matrix exponential function is **`MatrixExp`**.

$$\mathtt{\mathbf{MatrixExp}}\left[\begin{pmatrix} \mathbf{2} & \mathbf{1} \\ \mathbf{2} & \mathbf{3} \end{pmatrix}\right]$$

$$\begin{pmatrix} \frac{1}{3}\,(2\,e+e^4) & \frac{1}{3}\,(-e+e^4) \\ \frac{2}{3}\,(-e+e^4) & \frac{1}{3}\,(e+2\,e^4) \end{pmatrix}$$

Sage Note

Sage's matrix exponential method is called `exp`.

```
A=Matrix(QQ,[[2,1],[2,3]]);
A.exp()
    [ 2/3*e + 1/3*e^4 -1/3*e + 1/3*e^4]
    [-2/3*e + 2/3*e^4  1/3*e + 2/3*e^4]
```

EXERCISES FOR SECTION 12.5

A Exercises

1. (a) Write out all the details of Example 12.5.1 to show that the formula for F_k given in the text is correct.

(b) Use induction to prove the assertion made in Example 12.5.1 that

$$\begin{pmatrix} F_k \\ F_{k-1} \end{pmatrix} = A^{k-1}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

2. (a) Do Example 8.3.8 of Chapter 8 using the method outlined in Example 12.5.1. Note that the terminology characteristic equation, characteristic polynomial, and so on, introduced in Chapter 8, comes from the language of matrix algebra,

(b) What is the significance of Algorithm 8.3.1, part c, with respect to this section?

3. Solve $S(k) = 5\,S(k-1) + 4$, with $S(0) = 0$, using the method of this section.

4. How many paths are there of length 6 between vertex 1 and vertex 3 in Figure 12.5.2? How many paths from vertex 2 to vertex 2 of length 6 are there? Hint: The characteristic polynomial of the adjacency matrix is λ^4.

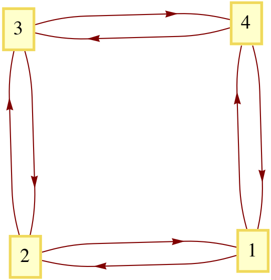


Figure 12.5.2

5. Use the matrix A of Example 12.5.2 to:

(a) Determine the number of paths of length 1 that exist from vertex a to each of the vertices in Example 12.5.2. Verify using the graph. Do the same for vertices b and c.

(b) Verify all the details of Example 12.5.2.

(c) Use Example 12.5.2 to determine the number of paths of length 4 there are from each node in the graph of Figure 12.5.1 to every node in the graph. Verify your results using the graph.

6. Let $A = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$

(a) Find e^A

(b) Recall that $\sin x = \sum_{k=0}^{\infty} \frac{(-1)^k x^k}{(2k+1)!}$ and compute $\sin A$.

(d) Formulate a reasonable definition of the natural logarithm of a matrix and compute $\ln A$.

7. We noted in Chapter 5 that since matrix algebra is not commutative under multiplication, certain difficulties arise. Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}$.

(a) Compute e^A, e^B, and e^{A+B}. Compare $e^A e^B$, $e^B e^A$ and e^{A+B}.

(b) Show that if $\mathbf{0}$ is the 2×2 zero matrix, then $e^{\mathbf{0}} = I$.

(c) Prove that if A and B are two matrices that do commute, then $e^{A+B} = e^A e^B$, thereby proving that e^A and e^B commute.

(d) Prove that for any matrix A, $(e^A)^{-1} = e^{-A}$.

8. Another observation for adjacency matrices: For the matrix in Example 12.5.2, note that the sum of the elements in the row corresponding to the node a (that is, the first row) gives the outdegree of a. Similarly, the sum of the elements in any given column gives the indegree of the node corresponding to that column.

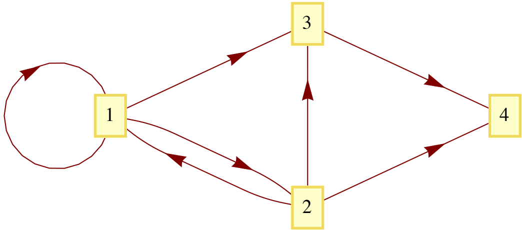


Figure 12.5.3

(a) Using the matrix A of Example 12.5.2, find the outdegree and the indegree of each node. Verify by the graph.

(b) Repeat part (a) for the directed graphs in Figure 12.5.3.

SUPPLEMENTARY EXERCISES FOR CHAPTER 12

Section 12.1

1. Find all solutions of the following systems:

(a)
$$\begin{array}{rcrcrcl} 2x_1 & - & 2x_2 & + & x_3 & = & 1 \\ & & x_2 & - & x_3 & = & 0 \\ x_1 & + & x_2 & + & x_3 & = & 3 \end{array}$$

(b)
$$\begin{array}{rcrcrcl} x_1 & & & - & x_3 & = & 0 \\ 2x_1 & - & 4x_2 & & & = & 1 \\ -x_1 & + & x_2 & - & x_3 & = & -1 \end{array}$$

2. Find all solutions of

$$\begin{array}{rcrcrcl} x_1 & - & x_2 & + & 2x_3 & = & 1 \\ 3x_1 & & & + & x_3 & = & 2 \\ 2x_1 & + & x_2 & - & x_3 & = & 1 \end{array}$$

Section 12.2

3. Determine A^{-1} using the method of the text if

$$A = \begin{pmatrix} 1 & 2 & 1 \\ -2 & -3 & -1 \\ 1 & 4 & 4 \end{pmatrix}.$$

4. Find the inverse of the matrix

$$\begin{pmatrix} 0 & -4 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

Section 12.3

5. In this exercise, write elements of $\mathbb{R}^2$ in column form. Let $\{x_1, x_2\}$ be a basis in $\mathbb{R}^2$. Prove that $\{Ax_1, Ax_2\}$ is a basis for $\mathbb{R}^2$ if and only if A has an inverse.

6. Let $V = \{f : X \to \mathbb{R}\}$, where X is any nonempty set. Show that V is a vector space under the operations:

$$(f + g)(x) = f(x) + g(x) \text{ for } f, g \in V, \text{and } x \in X$$

$$(c f)(x) = c f(x) \text{ for } f \in V, c \in \mathbb{R}, \text{and } x \in X.$$

7. (a) Convince yourself that $M_{2\times 3}(\mathbb{Z}_2)$ is a vector space over $\mathbb{Z}_2$ (i.e., allow only scalars from $\mathbb{Z}_2$ and use mod 2 arithmetic).

(b) What is the vector $-\mathbf{X}$, for any $\mathbf{X} \in M_{2\times 3}(\mathbb{Z}_2)$?

(c) What is $|M_{2\times 3}(\mathbb{Z}_2)|$?

8. (a) Define operations on $\mathbb{R}$ so that $\mathbb{R}$ is a vector space over $\mathbb{R}$.

(b) What is a basis for the vector space part a? What is its dimension?

Section 12.4

9. Employ the diagonalization process to approximate the 100th power of A, where $A = \begin{bmatrix} 0.6 & 0.2 \\ 0.4 & 0.8 \end{bmatrix}$.

10. Let $B = \begin{pmatrix} 0 & -\frac{3}{5} & 0 \\ \frac{5}{3} & 0 & -\frac{5}{3} \\ 0 & 6 & -6 \end{pmatrix}$ and $C = \begin{pmatrix} 4 & 2 & 2 \\ 2 & 4 & 2 \\ 2 & 2 & 4 \end{pmatrix}$

(a) Find all of the eigenvalues of B.

(b) Given that 2 and 8 are the only eigenvalues of C, find invertible matrix P and diagonal matrix D such that $C = PDP^{-1}$.

11. Let $A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 4 & 1 \\ 0 & 0 & 2 \end{pmatrix}$

(a) Find all of the eigenvalues of A.

(b) Given that 4 and 2 are the only eigenvalues of B, find invertible matrix P and diagonal matrix D such that $B = PDP^{-1}$.

12. Find all eigenvalues and associated eigenvectors of the matrix A, and write A in the form $A = PDP^{-1}$.

$$A = \begin{bmatrix} 3 & 1 \\ 0 & 2 \end{bmatrix}$$

Section 12.5

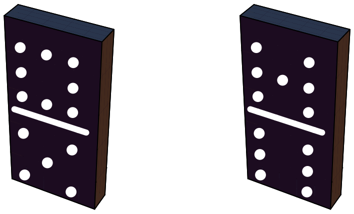
13. For a multigraph we can define its matrix representation as follows: A_{ij} = the number of different edges e from vertex a_i to vertex a_j.

(a) Draw the digraph that is described by the following matrix:

$$A = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 0 & 3 \\ 1 & 1 & 0 \end{pmatrix}$$

(b) Determine A^2 and interpret the result using Theorem 12.5.1.

Chapter 13



BOOLEAN ALGEBRA

George Boole, 1815 - 1864

George Boole

George Boole wasn't idle a lot.
He churned out ideas on the spot,
Making marvellous use of
Inclusive/exclusive
Expressions like AND, OR, and NOT

- limerick by Andrew Robinson from the Omnificent English Dictionary In Limerick Form

GOALS

In this chapater we will develop an algebra that is particularly important to computer scientists, as it is the mathematical foundation of computer design, or switching theory. The similarities of Boolean algebra and the algebra of sets and logic will be discussed, and we will discover special properties of finite Boolean algebras.

In order to achieve these goals, we will recall the basic ideas of posets introduced in Chapter 6 and develop the concept of a lattice, which has applications in finite-state machines. The reader should view the development of the topics of this chapter as another example of an algebraic system. Hence, we expect to define first the elements in the system, next the operations on the elements, and then the common properties of the operations in the system.

13.1 Posets Revisited

From Chapter 6, Section 3, we recall the following definition:

Definition: *Poset. A set L on which a partial ordering relation (reflexive, antisymmetric, and transitive) r is defined is called a partially ordered set, or poset, for short.*

We recall a few examples of posets:

(1) $L = \mathbb{R}$ and r is the relation $\leq$.

(2) $L = \mathcal{P}(A)$ where $A = \{a, b\}$ and r is the relation $\subseteq$.

(3) $L = \{1, 2, 3, 6\}$ and r is the relation $\mid$ (divides). We remind the reader that the pair (a, b) as an element of the relation r can be expressed as $(a, b) \in r$, or $a\, r\, b$, depending on convenience and readability.

The posets we will concentrate on in this chapter will be those which have maxima and minima. These partial orderings resemble that of $\leq$ on $\mathbb{R}$, so the symbol $\leq$ is used to replace the symbol r in the definition of a partially ordered set. Hence, the definition of a poset becomes:

Definition: *Poset. A set on which a partial ordering, $\leq$, is defined is called a partially ordered set, or, in brief, a poset. Here, $\leq$ is a partial ordering on L if and only if for all $a, b, c \in L$:*

(1) $a \leq a$(*reflexivity*),

(2) $a \leq b$ *and* $b \leq a \Rightarrow a = b$ (*antisymmetry*), *and*

We now proceed to introduce maximum and minimum concepts. To do this, we will first define these concepts for two elements of the poset L, and then define the concepts over the whole poset L.

Definition: *Lower Bound, Upper Bound. Let $a, b \in L$, a poset. Then $c \in L$ is a lower bound of a and b if $c \leq a$ and $c \leq b$. $d \in L$ is an upper bound of a and b if $a \leq d$ and $b \leq d$.*

Definition: ***Greatest Lower Bound.*** *Let L be a poset and $\leq$ be the partial ordering on L. Let $a, b \in L$, then $g \in L$ is a greatest lower bound of a and b, denoted glb(a, b), if and only if*

- $g \leq a$,
- $g \leq b$, *and*
- *if $g' \in L$ such that if $g' \leq a$ and $g' \leq b$, then $g' \leq g$.*

The last condition says, in other words, that if g' is also a lower bound, then g is "greater" than g', so g is a greatest lower bound.

The definition of a least upper bound is a mirror image of a greatest lower bound:

Definition: Least Upper Bound. *Let L be a poset and $\leq$ be the partial ordering on L. Let $a, b \in L$, then $\ell \in L$ is a least upper bound of a and b, denoted lub(a, b), if and only if*

- $a \leq \ell$,
- $b \leq \ell$, *and*
- *if $\ell' \in L$ such that if $a \leq \ell'$ and $b \leq \ell'$, then $\ell \leq \ell'$.*

Notice that the two definitions above refer to "...a greatest lower bound" and "a least upper bound." Any time you define an object like these you need to have an open mind as to whether more than one such object can exist. In fact, we now can prove that there can't be two greatest lower bounds or two least upper bounds.

Theorem 13.1.1. *Let L be a poset and $\leq$ be the partial ordering on L, and $a, b \in L$. If a greatest lower bound of a and b exists, then it is unique. The same is true of a least upper bound, if it exists.*

Proof: Let g and g' be greatest lower bounds of a and b. We will prove that $g = g'$.

(1) g a greatest lower bound of a and $b \Rightarrow g$ is a lower bound of a and b.

(2) g' a greatest lower bound of a and b and g a lower bound of a and $b \Rightarrow g \leq g'$ by the definition of greatest lower bound.

(3) g' a greatest lower bound of a and $b \Rightarrow g'$ is a lower bound of a and b.

(4) g a greatest lower bound of a and b and g' a lower bound of a and $b \Rightarrow g' \leq g$ by the definition of greatest lower bound.

(5) $g \leq g'$ and $g' \leq g \Rightarrow g = g'$ by the antisymmetry property of a partial ordering.

The proof of the second statement in the theorem is almost identical to the first and is left to the reader. ■

Definition: Greatest Element, Least Element. *Let L be a poset. $M \in L$ is called the greatest (maximum) element of L if, for all $a \in L$, $a \leq M$. In addition, $m \in L$ is called the least (minimum) element of L if for all $a \in L$, $m \leq a$.*

Note: The greatest and least elements, when they exist, are frequently denoted by 1 and 0 respectively.

Example 13.1.1. Let $L = \{1, 3, 5, 7, 15, 21, 35, 105\}$ and let $\leq$ be the relation | (divides) on L. Then L is a poset. To determine the *lub* of 3 and 7, we look for all $\ell \in L$, such that $3 \mid \ell$ and $7 \mid \ell$. Certainly, both $\ell = 21$ and $\ell = 105$ satisfy these conditions and no other element of L does. Next, since $21 \mid 105$, then $21 = \text{lub}(3, 7)$. Similarly, the $lub(3, 5) = 15$. The greatest element of L is 105 since $a \mid 105$ for all $a \in L$. To find the *glb* of 15 and 35, we first consider all elements g of L such that $g \mid 15$ and $g \mid 35$. Certainly, both $g = 5$ and $g = 1$ satisfy these conditions. But since $1 \mid 5$, then $glb\,(15, 35) = 5$. The least element of L is 1 since $1 \mid a$ for all $a \in L$.

Henceforth, for any positive integer n, D_n will denote the set of all positive integers which are divisors of n. For example, the set L of Example 13.1.1 is D_{105}.

Example 13.1.2. Consider the poset $\mathcal{P}(A)$, where $A = \{a, b, c\}$, with the relation $\subseteq$ on $\mathcal{P}(A)$. The *glb* of the $\{a, b\}$ and $\{a, c\}$ is $g = \{a\}$. For any other element g' of M which is a subset of $\{a, b\}$ and $\{a, c\}$ (there is only one; what is it?), $g' \subseteq g$. The least element of $\mathcal{P}(A)$ is $\emptyset$ and the greatest element of $\mathcal{P}(\text{A})$ is $A = \{a, b, c\}$. The Hasse diagram of $\mathcal{P}(\text{A})$ is shown in Figure 13.1.1.

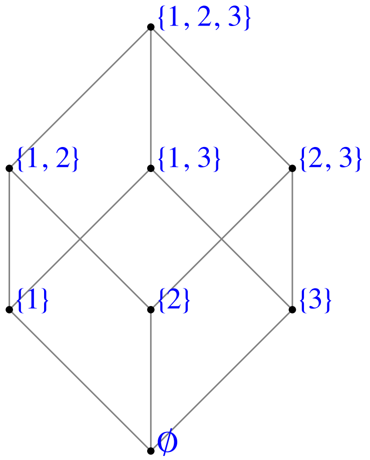


Figure 13.1.1
Example 13.1.2

With a little practice, it is quite easy to find the least upper bounds and greatest lower bounds of all possible pairs in $\mathcal{P}(A)$ directly from the graph of the poset.

The previous examples and definitions indicate that the *lub* and *glb* are defined in terms of the partial ordering of the given poset. It is not yet clear whether all posets have the property such every pair of elements has both a *lub* and a *glb*. Indeed, this is not the case (see Exercise 3).

EXERCISES FOR SECTION 13.1

A Exercises

1. Let $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ and let the relation | be a partial ordering on D_{30}.

(a) Find all lower bounds of 10 and 15.

(b) Find the *glb* of 10 and 15.

(c) Find all upper bounds of 10 and 15.

(d) Determine the *lub* of 10 and 15.

(e) Draw the Hasse diagram for D_{30} with |. Compare this Hasse diagram with that of Example 13.1.2. Note that the two diagrams are structurally the same.

2. List the elements of the sets D_8, D_{50}, and D_{1001}. For each set, draw the Hasse diagram for "divides."

3. Figure 13.1.2 contains Hasse diagrams of posets.

(a) Determine the *lub* and *glb* of all pairs of elements when they exist. Indicate those pairs that do not have a *lub* (or a *glb*).

(b) Find the least and greatest elements when they exist.

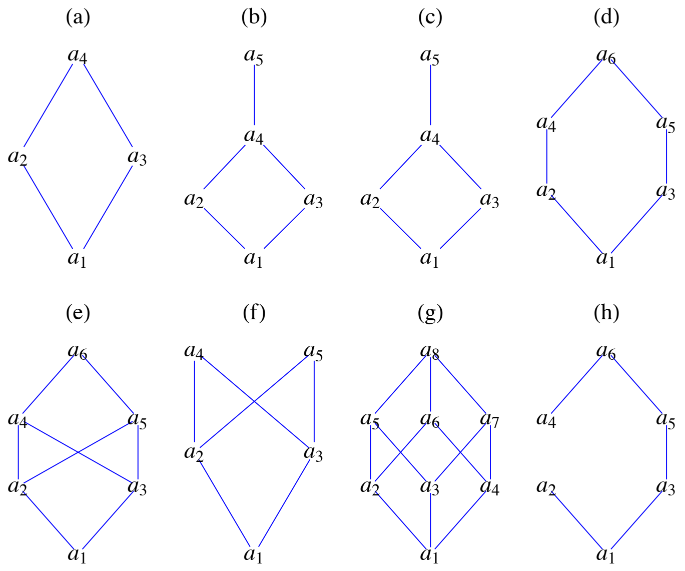


Figure 13.1.2
Exercise 3

4. For the poset $(\mathbb{N}, \leq)$, what are $glb(a, b)$ and $lub(a, b)$? Are there least and/or greatest elements?

5. (a) Prove the second part of Theorem 13.1.1, the least upper bound of two elements in a poset is unique, it one exists.

(b) Prove that if a poset L has a least element, then that element is unique.

6. We naturally order the numbers in $A_m = \{1, 2, \ldots, m\}$ with "less than or equal to," which is a partial ordering. We may order the elements of $A_m \times A_n$ by $(a, b) \leq (a', b') \Leftrightarrow a \leq a'$ and $b \leq b'$.

(a) Prove that this defines a partial ordering of $A_m \times A_n$.

(b) Draw the ordering diagrams for $\leq$ on $A_2 \times A_2$, $A_2 \times A_3$, and $A_3 \times A_3$.

(c) What are $glb((a, b), (a', b'))$ and $lub((a, b), (a', b'))$?

(d)Are there least and/or greatest elements in $A_m \times A_n$?

13.2 Lattices

In this section, we restrict our discussion to *lattices*, those posets where every pair of elements has a *lub* and a *glb*. We first introduce some notation.

Definitions: Join, Meet. *Let L be a poset under an ordering* $\leq$ *. Let* $a, b \in L$*. We define:*

$a \vee b$ (read "a join b") as the least upper bound of a and b, and

$a \wedge b$ (read "a meet b") as greatest lower bound of a and b.

Since the join and meet operations produce a unique result in all cases where they exist, by Theorem 13.1.1, we can consider them as binary operations on a set if they aways exist. Thus the following definition:

Definition: Lattice. *A lattice is a poset L (under $\leq$) in which every pair of elements has a lub and a glb. Since a lattice L is an algebraic system with binary operations $\vee$ and $\wedge$, it is denoted by* $[L; \vee, \wedge]$.

In Example 13.1.2, the operation table for the *lub* operation is easy, although admittedly tedious, to do. We can observe that every pair of elements in this poset has a least upper bound. In fact, $A \vee B = A \cup B$.

The reader is encouraged to write out the operation table for the *glb* operation and to note that every pair of elements in this poset also has a *glb*, so that $\mathcal{P}(A)$ together with these two operations is a lattice. We further observe that:

(1) $[\mathcal{P}(A); \vee, \wedge]$ is a lattice (under $\subseteq$) for any set A, and

(2) the join operation is the set operation of union and the meet operation is the operation intersection; that is, $\vee = \cup$ and $\wedge = \cap$.

It can be shown (see the exercises) that the commutative laws, associative laws, idempotent laws, and absorption laws are all true for any lattice. An example of this is clearly $[\mathcal{P}(A); \cup, \cap]$, since these laws hold in the algebra of sets. This lattice is also distributive in that join is distributive over meet and meet is distributive over join. This is not always the case for lattices in general however.

Definition: Distributive Lattice. *Let* $[L; \vee, \wedge]$ *be a lattice (under* $\leq$*).* $[L; \vee, \wedge\}$ *is called a distributive lattice if and only if the distributive laws hold; that is, for all* $a, b, c \in L$*, we have:*

$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ and

$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Example 13.2.1. If A is any set, the lattice $[\mathcal{P}(A); \bigcup, \bigcap]$ is distributive.

Example 13.2.2. We now give an example of a lattice where the distributive laws do not hold. Let $L = \{1, 2, 3, 5, 30\}$. Then L is a poset under the relation divides. The operation tables for $\vee$ and $\wedge$ on L are:

$\vee$	1	2	3	5	30
1	1	2	3	5	30
2	2	2	30	30	30
3	3	30	3	30	30
5	5	30	30	5	30
30	30	30	30	30	30

$\wedge$	1	2	3	5	30
1	1	1	1	1	1
2	1	2	1	1	2
3	1	1	3	1	3
5	1	1	1	5	5
30	1	2	3	5	30

Since every pair of elements in L has both a join and a meet, $[L; \vee, \wedge]$ is a lattice (under divides). Is this lattice distributive? We note that:

$2 \vee (5 \wedge 3) = 2 \vee 1 = 2$ and

$(2 \vee 5) \wedge (2 \vee 3) = 30 \wedge 30 = 30$,

so that $a \vee (b \wedge c) \neq (a \vee b) \wedge (a \vee c)$ for some values of $a, b, c \in L$. Hence L is not a distributive lattice.

It can be shown that a lattice is nondistributive if and only if it contains a sublattice isomorphic to one of the lattices in Figure 13.2.1.

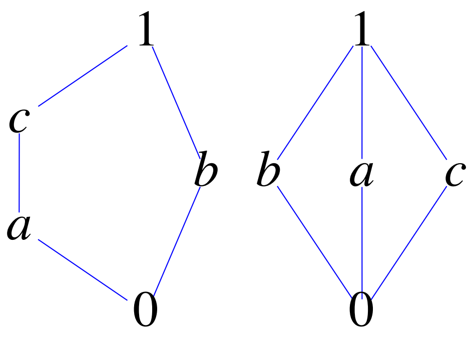


Figure 13.2.1
Nondistributive lattices

It is interesting to note that for the relation "divides" on $\mathbb{P}$, if $a, b \in \mathbb{P}$ we have:

$a \vee b = lcm(a, b)$, the least common multiple of a and b; that is, the smallest integer (in $\mathbb{P}$) that is divisible by both a and b;

$a \wedge b = gcd(a, b)$, the greatest common divisor of a and b; that is, the largest integer that divides both a and b.

EXERCISES FOR SECTION 13.2

A Exercises

1. Let L be the set of all propositions generated by p and q. What are the meet and join operations in this lattice. What are the maximum and minimum elements?

2. Which of the posets in Exercise 3 of Section 13.1 are lattices? Which of the lattices are distributive?

B Exercises

3. (a) State the commutative laws, associative laws, idempotent laws, and absorption laws for lattices.

   (b) Prove these laws.

4. Let $[L; \bigvee, \bigwedge]$ be a lattice based on a partial ordering $\leq$. Prove that if $a, b, c \in L$,

   (a) $a \bigvee b \geq a$.

   (b) $a \bigwedge b \leq a$.

   (c) $a \geq b$ and $a \geq c \Rightarrow a \geq b \bigvee c$.

13.3 Boolean Algebras

In order to define a Boolean algebra, we need the additional concept of complementation.

Definition: Complemented Lattice. *Let $[L; \bigvee, \bigwedge]$ be a lattice that contains a least element, 0, and a greatest element, 1. $[L; \bigvee, \bigwedge]$ is called a complemented lattice if and only if for every element $a \in L$, there exists an element $\overline{a}$ in L such that $a \wedge \overline{a} = 0$ and $a \vee \overline{a} = 1$. Such an element $\overline{a}$ is called a complement of the element a.*

Example 13.3.1. Let $L = \mathcal{P}(A)$, where $A = \{a, b, c\}$. Then $[L; \bigcup, \bigcap]$ is a bounded lattice with $0 = \emptyset$ and $1 = A$. Then, to find if it exists, the complement, $\overline{B}$, of, say $B = \{a, b\} \in L$, we want $\overline{B}$ such that

$$\{a, b\} \bigcap \overline{B} = \emptyset \text{ and } \{a, b\} \bigcup \overline{B} = A .$$

Here, $\overline{B} = \{c\}$, and since it can be shown that each element of L has a complement (see Exercise 1), $[L; \bigcup, \bigcap]$ is a complemented lattice. Note that if A is any set and $L = \mathcal{P}(A)$, then $[L; \bigcup, \bigcap]$ is a complemented lattice where the complement of $B \in L$ is $\overline{B} = B^c = A - B$.

In Example 13.3.1, we observe that the complement of each element of L is unique. Is this always the case? The answer is no. Consider the following.

Example 13.3.2. Let $L = \{1, 2, 3, 5, 30\}$ and consider the lattice $[L; \bigvee, \bigwedge]$ (under "divides"). The least element of L is 1 and the greatest element is 30. Let us compute the complement of the element $a = 2$. We want to determine $\overline{a}$ such that $2 \bigwedge \overline{a} = 1$ and $2 \bigvee \overline{a} = 30$. Certainly, $\overline{a} = 3$ works, but so does $\overline{a} = 5$, so the complement of $a = 2$ in this lattice is not unique. However, $[L; \bigvee, \bigwedge]$ is still a complemented lattice since each element does have at least one complement.

The following theorem gives us an insight into when uniqueness of complements occurs.

Theorem 13.3.1. *If $[L; \bigvee, \bigwedge]$ is a complemented and distributive lattice, then the complement $\overline{a}$ of any element $a \in L$ is unique.*

Proof: Let $a \in L$ and assume to the contrary that a has two complements, namely a_1 and a_2. Then by definition of complement,

$$a \wedge a_1 = 0 \text{ and } a \vee a_1 = 1,$$

Also,

$$a \wedge a_2 = 0 \text{ and } a \vee a_2 = 1.$$

So that

$$\begin{aligned} a_1 = {} & a_1 \bigwedge 1 = a_1 \wedge (a \vee a_2) \\ & = (a_1 \wedge a) \vee (a_1 \wedge a_2) \\ & = 0 \bigvee (a_1 \wedge a_2) \\ & = a_1 \wedge a_2. \end{aligned}$$

On the other hand,

$$\begin{aligned} a_2 & = a_2 \bigwedge 1 = a_2 \wedge (a \vee a_1) \\ & = (a_2 \wedge a) \vee (a_2 \wedge a_1) \\ & = 0 \bigvee (a_2 \wedge a_1) \\ & = a_2 \wedge a_1. \end{aligned}$$

Hence $a_1 = a_2$, which contradicts the assumption that a has two different complements, a_1 and a_2. ■

Definition: Boolean Algebra. *A Boolean algebra is a lattice that contains a least element and a greatest element and that is both complemented and distributive.*

Since the complement of each element in a Boolean algebra is unique (by Theorem 13.3.1), complementation is a valid unary operation over the set under discussion, and we will list it together with the other two operations to emphasize that we are discussing a set together with three operations. Also, to help emphasize the distinction between lattices and lattices that are Boolean algebras, we will use the letter B as the generic symbol for the set of a Boolean algebra; that is, $[B; -, \bigvee, \bigwedge]$ will stand for a general Boolean algebra.

Example 13.3.3. Let A be any set, and let $B = \mathcal{P}(A)$. Then $[B;\ c,\ \bigcup,\ \bigcap]$ is a Boolean algebra. Here, c stands for the complement of an element of B with respect to A, $A - B$.

This is a key example for us since all finite Boolean algebras and many infinite Boolean algebras look like this example for some A. In fact, a glance at the basic Boolean algebra laws in Table 13.3.1, in comparison with the set laws of Chapter 4 and the basic laws of logic of Chapter 3, indicates that all three systems behave the same; that is, they are isomorphic.

The "pairing" of the above laws reminds us of the principle of duality, which we state for a Boolean algebra.

Definition: Principle of Duality for Boolean Algebras. *Let* $[B;\ -,\ \bigvee,\ \bigwedge]$ *be a Boolean algebra (under* $\leq$*), and let S be a true statement for* $[B;\ -,\ \bigvee,\ \bigwedge]$. *If* S^* *is obtained from S by replacing* $\leq$ *by* $\geq$ *(this is equivalent to turning the graph upside down),* $\vee$ *by* $\wedge$, $\wedge$ *by* $\vee$, 0 *by* 1, *and* 1 *by* 0, *then* S^* *is also a true statement.*

TABLE 13.3.1

Basic Boolean Algebra Laws

Commutative Laws	
1. $a \bigvee b = b \bigvee a$	1.' $a \bigwedge b = b \bigwedge a$
Associative Laws	
2. $a \bigvee (b \bigvee c) = (a \bigvee b) \bigvee c$	2.' $a \bigwedge (b \bigwedge c) = (a \bigwedge b) \bigwedge c$
Distributive Laws	
3. $a \bigwedge (b \bigvee c) = (a \bigwedge b) \bigvee (a \wedge c)$	3.' $a \bigvee (b \bigwedge c) = (a \bigvee b) \bigwedge (a \vee c)$
Identity Laws	
4. $a \bigvee 0 = 0 \bigvee a = a$	4.' $a \bigwedge 1 = 1 \bigwedge a = a$
Complement Laws	
5. $a \vee \overline{a} = 1$	5.' $a \wedge \overline{a} = 0$
Idempotent Laws	
6. $a \vee a = a$	6.' $a \wedge a = a$
Null Laws	
7. $a \bigvee 1 = 1$	7.' $a \bigwedge 0 = 0$
Absorption Laws	
8. $a \bigvee (a \bigwedge b) = a$	8.' $a \bigwedge (a \bigvee b) = a$
DeMorgan's Laws	
9. $\overline{a \bigvee b} = \overline{a} \wedge \overline{b}$	9.' $\overline{a \bigwedge b} = \overline{a} \vee \overline{b}$
Involution Law	
10. $\overline{\overline{a}} = a$	

Example 13.3.4. The laws 1' through 9' are the duals of the Laws 1 through 9 respectively. Law 10 is its own dual.

We close this section with some comments on notation. The notation for operations in a Boolean algebra is derived from the algebra of logic. However, other notations are used. These are summarized in the following chart;

Notation used in this text (Mathematics notation)	Set Notation	Logic Design (CS / EE notation)	Read as
$\bigvee$	$\bigcup$	$\oplus$	join
$\bigwedge$	$\bigcap$	$\otimes$	meet
$-$	c	$-$	complement
$\leq$	$\subseteq$	$\leq$	underlying partial ordering

Mathematicians most frequently use the notation of the text, and, on occasion, use set notation for Boolean algebras. Thinking in terms of sets may be easier for some people. Computer designers traditionally use the arithmetic and notation. In this latter notation, DeMorgan's Laws become:

$$(9)\quad \overline{a \oplus b} = \bar{a} \otimes \bar{b}$$

and

$$(9')\quad \overline{a \otimes b} = \bar{a} \oplus \bar{b}.$$

EXERCISES FOR SECTION 13.3

A Exercises

1. Determine the complement of each element $B \in L$ in Example 13.3.1. Is this lattice a Boolean algebra? Why?

2. (a) Determine the complement of each element of D_6 in $[D_6; \bigvee, \bigwedge]$.

   (b) Repeat part a using the lattice in Example 13.2.2.

   (c) Repeat part a using the lattice in Exercise 1 of Section 13.1.

   (d) Are the lattices in parts a, b, and c Boolean algebras? Why?

3. Determine which of the lattices of Exercise 3 of Section 13.1 are Boolean algebras.

4. Let $A = \{a, b\}$ and $B = \mathcal{P}(A)$.

   (a) Prove that $[B; c, \bigcup, \bigcap]$ is a Boolean algebra.

   (b) Write out the operation tables for the Boolean algebra.

5. It can be shown that the following statement, S, holds for any Boolean algebra $[B; -, \bigvee, \bigwedge]$: $(a \bigwedge b) = a$ if $a \leq b$.

   (a) Write the dual, S^*, of the statement S.

   (b) Write the statement S and its dual, S^*, in the language of sets.

   (c) Are the statements in part b true for all sets?

   (d) Write the statement S and its dual, S^*, in the language of logic.

   (e) Are the statements in part d true for all propositions?

6. State the dual of:

   (a) $a \bigvee (b \bigwedge a) = a.$

   (b) $a \bigvee (\overline{(\bar{b} \vee a) \bigwedge b}) = 1.$

   (c) $(\overline{a \wedge \bar{b}}) \wedge b = a \bigvee b.$

   B Exercises

7. Formulate a definition for isomorphic Boolean algebras.

13.4 Atoms of a Boolean Algebra

In this section we will look more closely at previous claims that every finite Boolean algebra is isomorphic to an algebra of sets. We will show that every finite Boolean algebra has 2^n elements for some n with precisely n generators, called *atoms*.

Consider the Boolean algebra $[B; -, \bigvee, \bigwedge]$, whose graph is:

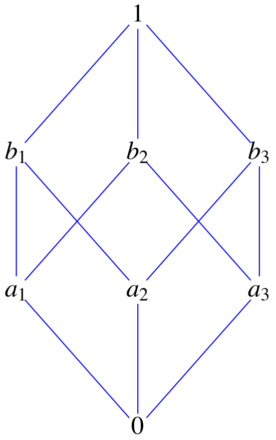


Figure 13.4.1
Illustration of the atom concept

We note that $1 = a_1 \vee a_2 \vee a_3$, $b_1 = a_1 \vee a_2$, $b_2 = a_1 \vee a_3$, and $b_3 = a_2 \vee a_3$; that is, each of the elements above level one can be described completely and uniquely in terms of the elements on level one. The a_i s have uniquely generated the nonzero elements of B much like a basis in linear algebra generates the elements in a vector space. We also note that the a_i s are the immediate successors of the minimum element, 0. In any Boolean algebra, the immediate successors of the minimum element are called *atoms*. Let A be any nonempty set. In the Boolean algebra $[\mathcal{P}(A);\ c,\ \bigcup,\ \bigcap]$ (over $\subseteq$), the singleton sets are the generators, or atoms, of the algebraic structure since each element $\mathcal{P}(A)$ can be described completely and uniquely as the join or union of singleton sets.

Definition: Atom. *A nonzero element a in a Boolean algebra* $[B;\ -,\ \vee,\ \wedge]$ *is called an atom if for every* $x \in B$, $x \wedge a = a$ *or* $x \wedge a = 0$.

The condition that $x \wedge a = a$ tells us that x is a successor of a; that is, $a \leq x$, as depicted in Figure 13.4.2a.

The condition $x \wedge a = 0$ is true only when x and a are "not connected." This occurs when x is another atom or if x is a successor of atoms different from a, as depicted in Figure 13.4.2b.

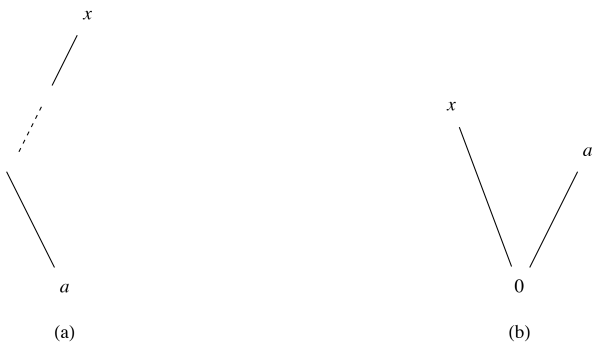


Figure 13.4.2

Example 13.4.1. The set of atoms of the Boolean algebra $[D_{30};\ -,\ \bigvee,\ \bigwedge]$ is $M = \{2,\ 3,\ 5\}$. To see that $a = 2$ is an atom, let x be any nonzero element of D_{30} and note that one of the two conditions $x \bigwedge 2 = 2$ or $x \bigwedge 2 = 1$ holds. Of course, to apply the definition to this Boolean algebra, we must remind ourselves that in this case the 0-element is 1, the operation $\wedge$ is *gcd*, and the poset relation $\leq$ is "divides." So if $x = 10$, we have $10 \bigwedge 2 = 2$ (or $2 \mid 10$), so Condition 1 holds. If $x = 15$, the first condition is not true. (Why?) However, Condition 2, $15 \bigwedge 2 = 1$, is true. The reader is encouraged to show that each of the elements 2, 3, and 5 satisfy the definition (see Exercise 13.4.1). Next, if we compute the join (*lcm* in this case) of all possible combinations of the atoms 2, 3, and 5, we will generate all nonzero elements of D_{30}. For example, $2 \bigvee 3 \bigvee 5 = 30$ and $2 \bigvee 5 = 10$. We state this concept formally in the following theorem, which we give without proof.

Theorem 13.4.1. *Let* $[B;\ -,\ \vee,\ \wedge]$ *be any finite Boolean algebra. Let* $A = \{a_1,\ a_2, \ldots, a_n\}$ *be the set of all n atoms of* $[B;\ -,\ \vee,\ \wedge]$. *Then every nonzero element in B can be expressed uniquely as the join of a subset of A.*

We now ask ourselves if we can be more definitive about the structure of different Boolean algebras of a given order. Certainly, the Boolean algebras $[D_{30};\ -,\ \bigvee,\ \bigwedge]$ and $[\mathcal{P}(A);\ c,\ \bigcup,\ \bigcap]$ have the same graph (that of Figure 13.4.1), the same number of atoms, and, in all respects, look the same except for the names of the elements and the operations. In fact, when we apply corresponding operations to corresponding elements, we obtain corresponding results. We know from Chapter 11 that this means that the two structures are isomorphic as Boolean algebras. Furthermore, the graphs of these examples are exactly the same as that of Figure 13.4.1, which is an arbitrary Boolean algebra of order $8 = 2^3$.

In these examples of a Boolean algebra of order 8, we note that each had 3 atoms and $2^3 = 8$ number of elements, and all were isomorphic to $[\mathcal{P}(A); c, \bigcup, \bigcap]$, where $A = \{a, b, c\}$. This leads us to the following questions:

(1) Are there any other different (nonisomorphic) Boolean algebras of order 8?

(2) What is the relationship, if any, between finite Boolean algebras and their atoms?

(3) How many different (nonisomorphic) Boolean algebras are there of order 2? Order 3? Order 4? And so on.

The answers to these questions are given in the following theorem and corollaries. We include the proofs of the corollaries since they are instructive.

Theorem 13.4.2. *Let* $[B; -, \lor, \land]$ *be any finite Boolean algebra, and let A be the set of all atoms in this Boolean algebra. Then* $[B; -, \lor, \land]$ *is isomorphic to* $[\mathcal{P}(A); c, \bigcup, \bigcap]$.

Corollary 13.4.1. *Every finite Boolean algebra* $[B; -, \lor, \land]$ *has* 2^n *elements for some positive integer n.*

Proof: Let A be the set of all atoms of B and let $|A| = n$. Then there are exactly 2^n elements (subsets) in $\mathcal{P}(A)$, and by Theorem 13.4.2, $[B; -, \bigvee, \bigwedge]$ is isomorphic to $[\mathcal{P}(A); c, \bigcup, \bigcap]$. ■

Corollary 13.4.2. All Boolean algebras of order 2^n are isomorphic to each other. (The graph of the Boolean algebra of order 2^n is the n-cube).

Proof: By Theorem 13.4.2, every Boolean algebra of order 2^n is isomorphic to $[\mathcal{P}(A); c, \bigcup, \bigcap]$ when $|A| = n$. Hence, they are all isomorphic to one another. ■

The above theorem and corollaries tell us that we can only have finite Boolean algebras of orders $2^1, 2^2, 2^3, \ldots, 2^n$, and that all finite Boolean algebras of any given order are isomorphic. These are powerful tools in determining the structure of finite Boolean algebras. In the next section, we will try to find the easiest way of describing a Boolean algebra of any given order.

EXERCISES FOR SECTION 13.4

A Exercises

1. (a) Show that $a = 2$ is an atom of the Boolean algebra $[D_{30}; -, \bigvee, \bigwedge]$.

(b) Repeat part a for the elements 3 and 5 of D_{30}.

(c) Verify Theorem 13.4.1 for the Boolean algebra $[D_{30}; -, \bigvee, \bigwedge]$.

2. Let $A = \{a, b, c\}$.

(a) Rewrite the definition of atom for $[\mathcal{P}(A); c, \bigcup, \bigcap]$. What does $a \leq x$ mean in this example?

(b) Find all atoms of $[\mathcal{P}(A); c, \bigcup, \bigcap]$.

(c) Verify Theorem 13.4.1 for $[\mathcal{P}(A); c, \bigcup, \bigcap]$.

3. Verify Theorem 13.4.2 and its corollaries for the Boolean algebras in Exercises 1 and 2 of this section.

4. Give a description of all Boolean algebras of order 16. (*Hint*: Use Theorem 13.4.2.) Note that the graph of this Boolean algebra is given in Figure 9.4.5.

5. Corollary 13.4.1 states that there do not exist Boolean algebras of orders 3, 5, 6, 7, 9, etc. (orders different from 2^n). Prove that we cannot have a Boolean algebra of order 3. (*Hint*: Assume that $[B; -, \bigvee, \bigwedge]$ is a Boolean algebra of order 3 where $B = \{0, x, 1\}$ and show that this cannot happen by investigating the possibilities for its operation tables.)

6. (a) There are many different, yet isomorphic, Boolean algebras with two elements. Describe one such Boolean algebra that is derived from a power set, $\mathcal{P}(A)$, under $\subseteq$. Describe a second that is described from D_n, for some $n \in P$, under "divides."

(b) Since the elements of a two-element Boolean algebra must be the greatest and least elements, 1 and 0, the tables for the operations on $\{0, 1\}$ are determined by the Boolean algebra laws. Write out the operation tables for $[\{0, 1\}; -, \bigvee, \bigwedge]$.

B Exercises

7. Find a Boolean algebra with a countably infinite number of elements.

8. Prove that the direct product of two Boolean algebras is a Boolean algebra. (*Hint*: "Copy" the corresponding proof for groups in Section 11.6.)

13.5 Finite Boolean Algebras as n-tuples of 0's and 1's

From the previous section we know that all finite Boolean algebras are of order 2^n, where n is the number of atoms in the algebra. We can therefore completely describe every finite Boolean algebra by the algebra of power sets. Is there a more convenient, or at least an alternate way, of defining finite Boolean algebras? In Chapter 11 we found that we could produce new groups by taking Cartesian products of previously known groups. We imitate this process for Boolean algebras.

The simplest nontrivial Boolean algebra is the Boolean algebra on the set $B_2 = \{0, 1\}$. The ordering on B_2 is the natural one, $0 \leqslant 0$, $0 \leqslant 1$, $1 \leqslant 1$. If we treat 0 and 1 as the truth values "false" and "true," respectively, we see that the Boolean operations $\vee$ (join) and $\wedge$ (meet) are nothing more than the logical connectives $\vee$ (or) and $\wedge$ (and). The Boolean operation, $-$, (complementation) is the logical $\neg$ (negation). In fact, this is why the symbols $-$, $\vee$, and $\wedge$ were chosen as the names of the Boolean operations. The operation tables for $[B_2; -, \vee, \wedge]$ are simply those of "or," "and," and "not," which we repeat here:

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

u	$\bar{u}$
0	1
1	0

By Theorem 13.4.2 and its corollaries, all Boolean algebras of order 2 are isomorphic to this one.

We know that if we form $B_2 \times B_2 = B_2^2$ we obtain the set $\{(0, 0), (0, 1), (1, 0), (1, 1)\}$, a set of order 4. We define operations on B_2^2 the natural way, namely, componentwise, so that $(0, 1) \vee (1, 1) = (0 \vee 1, 1 \vee 1) = (1, 1)$, $(0, 1) \wedge (1, 1) = (0 \wedge 1, 1 \wedge 1) = (0, 1)$ and $\overline{(0, 1)} = (\bar{0}, \bar{1}) = (1, 0)$. We claim that B_2^2 is a Boolean algebra under the componentwise operations. Hence, $[B_2^2; -, \vee, \wedge]$ is a Boolean algebra of order 4. Since all Boolean algebras of order 4 are isomorphic to each other, we have found a simple way of describing all Boolean algebras of order 4.

It is quite clear that we can describe any Boolean algebra of order 8 by considering $B_2 \times B_2 \times B_2 = B_2^3$ and, in general, any Boolean algebra of order 2^n— that is, all finite Boolean algebras—by $B_2^n = B_2 \times B_2 \times \cdots \mathrm{B}_2$ (n factors).

EXERCISES FOR SECTION 13.5

A Exercises

1. (a) Write out the operation tables for $[B_2^2; -, \vee, \wedge]$.

(b) Draw the Hasse diagram for $[B_2^2; -, \vee, \wedge]$ and compare your results with Figure 9.4.6.

(c) Find the atoms of this Boolean algebra.

2. (a) Write out the operation table for $[B_2^3; -, \vee, \wedge]$.

(b) Draw the Hasse diagram for $[B_2^3; -, \vee, \wedge]$ and compare the results with Figure 9.4.6.

3. (a) List all atoms of B_2^4.

(b) Describe the atoms of B_2^n $n \geqslant 1$.

B Exercise

4. Theorem 13.4.2 tells us we can think of any finite Boolean algebra in terms of sets. In Chapter 4, Section 3, we defined the terms *minset* and *minset normal form*. Rephrase these definitions in the language of Boolean algebra. The generalization of minsets are called *minterms*.

13.6 Boolean Expressions

In this section, we will use our background from the previous sections and set theory to develop a procedure for simplifying Boolean expressions. This procedure has considerable application to the simplification of circuits in switching theory or logical design.

Definition: *Boolean Expression. Let $[B; -, \vee, \wedge]$ be any Boolean algebra. Let x_1, x_2, …, x_k be variables in B; that is, variables that can assume values from B. A Boolean expression generated by x_1, x_2, …, x_k is any valid combination of the x_i and the elements of B with the operations of meet, join, and complementation.*

This definition, as expected, is the analog of the definition of a proposition generated by a set of propositions, presented in Section 3.2.

Each Boolean expression generated by k variables, $e(x_1, \ldots, x_k)$, defines a function $f : B^k \to B$ where $f(a_1, \ldots, a_k) = e(a_1, \ldots, a_k)$. If B is a finite Boolean algebra, then there are a finite number of functions from B^k into B. Those functions that are defined in terms of Boolean expressions are called *Boolean functions*. As we will see, there is an infinite number of Boolean expressions that define each Boolean function. Naturally, the "shortest" of these expressions will be preferred. Since electronic circuits can be described as Boolean functions with $B = B_2$, this economization is quite useful.

Example 13.6.1. Consider any Boolean algebra $[B; -, \vee, \wedge]$ of order 2. How many functions $f : B^2 \to B$ are there? First, all Boolean algebras of order 2 are isomorphic to $[B_2; -, \vee, \wedge]$ so we want to determine the number of functions $f : B_2^2 \to B_2$. If we consider a Boolean function of two variables, x_1 and x_2, we note that each variable has two possible values 0 and 1, so there are 2^2 ways of assigning these two values to the $k = 2$ variables. Hence, the table below has $2^2 = 4$ rows. So far we have a table such as that labeled 13.6.1.

x_1	x_2	$f(x_1, x_2)$
0	0	?
0	1	?
1	0	?
1	1	?

Table 13.6.1
General Form Of Boolean Function $f(x_1, x_2)$ of Example 13.6.1

How many possible different function values $f(x_1, x_2)$ can there be? To list a few:$f_1(x_1, x_2) = x_1$, $f_2(x_1, x_2) = x_2$, $f_3(x_1, x_2) = x_1 \vee x_2$, $f_4(x_1, x_2) = (x_1 \wedge \overline{x_2}) \vee x_2$, $f_5(x_1, x_2) = x_1 \wedge x_2 \vee \overline{x_2}$, etc. Each of these will give a table like that of Table 13.6.1. The tables for f_1 , and f_3 appear in Table 13.6.2.

x_1	x_2	$f_1(x_1, x_2)$
0	0	0
0	1	0
1	0	1
1	1	1

x_1	x_2	$f_3(x_1, x_2)$
0	0	0
0	1	1
1	0	1
1	1	1

Table 13.6.2
Boolean Functions f_1 and f_3 of Example 13.6.1

Two functions are different if and only if their tables (values) are different for at least one row. Of course by using the basic laws of Boolean algebra we can see that $f_3 = f_4$. Why? So if we simply list by brute force all "combinations" of x_1 and x_2 we will obtain unnecessary duplication. However, we note that for any combination of the variables x_1, and x_2 there are only two possible values for $f(x_1, x_2)$, namely 0 or 1. Thus, we could write $2^4 = 16$ different functions on 2 variables.

Now let's count the number of different Boolean functions in a more general setting. We will consider two cases: first, when $B = B_2$, and second, when B is any finite Boolean algebra with 2^n elements.

Let $B = B_2$. Each function $f : B^k \to B$ is defined in terms of a table having 2^k rows. Therefore, since there are two possible images for each element of B^k, there are 2 raised to the 2^k, or 2^{2^k} different functions. *We claim that every one of these functions is a Boolean function.*

Now suppose that $|B| = 2^n > 2$. A function from B^k into B can still be defined in terms of a table. There are $|B|^k$ rows to each table and $|B|$ possible images for each row. Therefore, there are 2^n raised to the power 2^{nk} different functions. If $n > 1$, then not every one of these functions is a Boolean function. Notice that in counting the numbers of functions we are applying the result of Exercise 5 of Section 7.1.

Since all Boolean algebras are isomorphic to a Boolean algebra of sets, the analogues of statements in sets are useful in Boolean algebras.

Definition: *Minterm. A Boolean expression generated by $x_1, x_2, \ldots, x_k$ that has the form*

$$\overset{k}{\underset{i=1}{\wedge}} y_i,$$

where each y_i may be either x_i or $\overline{x_i}$ is called a minterm generated by $x_1, x_2, \ldots, x_k$.

By a direct application of the Product Rule we see that there are 2^k different minterms generated by $x_1, \ldots, x_k$.

Definition: *Minterm Normal Form. A Boolean expression generated by $x_1, \ldots, x_k$ is in minterm normal form if it is the join of expressions of the form $a \wedge m$, where $a \in B$ and m is a minterm generated by $x_1, \ldots, x_k$. That is, it is of the form*

$$\overset{p}{\underset{j=1}{\vee}} \left(a_j \wedge m_j\right),$$

where $p = 2^k$ and $m_1, m_2, \ldots, m_p$ are the minterms generated by $x_1, \ldots, x_k$

If $B = B_2$, then each a_j in a minterm normal form is either 0 or 1. Therefore, $a_j \wedge m_j$ is either 0 or m_j.

Theorem 13.6.1. *Let $e(x_1, \ldots, x_k)$ be a Boolean expression over B. There exists a unique minterm normal form $M(x_1, \ldots, x_k)$ that is equivalent to $e(x_1, \ldots, x_k)$ in the sense that e and M define the same function from B^k into B.*

The uniqueness in this theorem does not include the possible ordering of the minterms in M (commonly referred to as "uniqueness up to the order of minterms"). The proof of this theorem would be quite lengthy, and not very instructive, so we will leave it to the interested reader to attempt. The implications of the theorem are very interesting, however.

If $|B| = 2^n$, then there are 2^n raised to the 2^k different minterm normal forms. Since each different minterm normal form defines a different function, there are a like number of Boolean functions from B^k into B. If $B = B_2$, there are as many Boolean functions (2 raised to the 2^k) as there are functions from B^k into B, since there are 2 raised to the 2^n functions from B^k into B. The significance of this result is that any desired function can be obtained using electronic circuits having 0 or 1 (off or on, positive or negative) values, but more complex, multivalued circuits would not have this flexibility.

We will close this section by examining minterm normal forms for expressions over B_2 , since they are a starting point for circuit economization.

Example 13.6.2. Consider the Boolean expression $f(x_1, x_2) = x_1 \vee \overline{x_2}$. One method of determining the minterm normal form of f is to think in terms of sets. Consider the diagram with the usual translation of notation in Figure 13.6.1. Then $f(x_1,\ x_2) = (\overline{x_1} \wedge \overline{x_2}) \bigvee (x_1 \wedge \overline{x_2}) \bigvee (x_1 \wedge x_2)$.

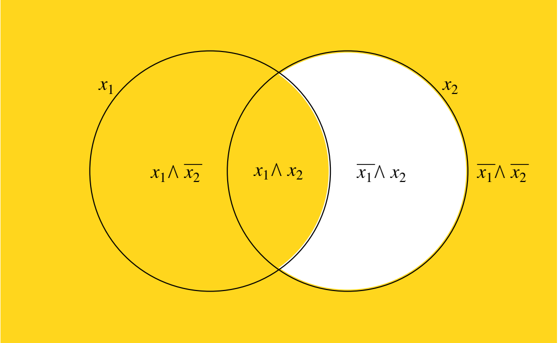

x_1
x_2
$x_1 \wedge \overline{x_2}$
$x_1 \wedge x_2$
$\overline{x_1} \wedge x_2$
$\overline{x_1} \wedge \overline{x_2}$

Figure 13.6.1

Example 13.6.3. Consider the function $f : B_2^3 \rightarrow B_2$ defined by Table 13.6.3. The minterm normal form for f can be obtained by taking the join of minterms that correspond to rows that have an image value of 1. If $f(a_1,\ a_2,\ a_3) = 1$, then include the minterm $y_1 \bigwedge y_2 \bigwedge y_3$ where

$$y_j = \begin{cases} x_j & \text{if } a_j = 1 \\ \overline{x_j} & \text{if } a_j = 0 \end{cases}$$

TABLE 13.6.3

Boolean Function of $f(a_1,\ a_2,\ a_3)$ Of Example 13.6.3

a_1	a_2	a_3	$f\ (a_1,\ a_2,\ a_3)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	0	1	0

Therefore,

$$f(x_1,\ x_2,\ x_3) = (\overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3}) \bigvee (\overline{x_1} \wedge x_2 \wedge x_3) \bigvee (x_1 \wedge x_2 \wedge \overline{x_3}).$$

The minterm normal form is a first step in obtaining an economical way of expressing a given Boolean function. For functions of more than three variables, the above set theory approach tends to be awkward. Other procedures are used to write the normal form. The most convenient is the Karnaugh map, a discussion of which can be found in any logical design/switching theory text (see, for example, Hill and Peterson).

EXERCISES FOR SECTION 13.6

A Exercises

1. (a) Write the 16 possible functions of Example 13.6.1. (*Hint:* Find all possible joins of minterms generated by x_1 and x_2 .)

(b) Write out the tables of several of the above Boolean functions to show that they are indeed different.

(c) Determine the minterm normal form of

$$f_1(x_1,\ x_2) = x_1 \vee x_2,$$

$$f_2(x_1,\ x_2) = \overline{x_1} \vee \overline{x_2}$$

$$f_3(x_1,\ x_2) = 0,\ f_4(x_1,\ x_2) = 1.$$

2. Consider the Boolean expression $f(x_1,\ x_2,\ x_3) = (\overline{x_3} \wedge x_2) \vee (\overline{x_1} \wedge x_3) \vee (x_2 \wedge x_3)$ on $[B_2;\ -,\ \bigvee,\ \bigwedge]$.

(a) Simplify this expression using basic Boolean algebra laws.

(b) Write this expression in minterm normal form.

(c) Write out the table for the given function defined by f and compare it to the tables of the functions in parts a and b.

(d) How many possible different functions in three variables on $[B_2; -, \vee, \wedge]$ are there?

B Exercise

3. Let $[B; -, \vee, \wedge]$ be a Boolean algebra of order 4, and let f be a Boolean function of two variables on B.

(a) How many elements are there in the domain of f ?

(b) How many different Boolean functions are there of two, variables? Three variables?

(c) Determine the minterm normal form of $f(x_1, x_2) = x_1 \vee x_2$.

(d) If $B = \{0, a, b, 1\}$, define a function from B^2 into B that is not a Boolean function.

13.7 A Brief Introduction to the Application of Boolean Algebra to Switching Theory

The algebra of switching theory is Boolean algebra. The standard notation used for Boolean algebra operations in most logic design/switching theory texts is + for ∨ and • for ∧. Complementation is as in this text. Therefore, $(x_1 \wedge \overline{x_2}) \vee (x_1 \wedge x_2) \vee (\overline{x_1} \wedge x_2)$ becomes $x_1 \bullet \overline{x_2} + x_1 \bullet x_2 + \overline{x_1} \bullet x_2$, or simply $x_1 \overline{x_2} + x_1 x_2 + \overline{x_1} x_2$. All concepts developed previously for Boolean algebras hold. The only change is purely notational. We make the change in this section solely to introduce the reader to another frequently used notation. Obviously, we could have continued the discussion with our previous notation.

The simplest switching device is the on-off switch. If the switch is closed, on, current will pass through it; if it is open, off, current will not pass through it. If we designate on by true or the logical, or Boolean, 1, and off by false, the logical, or Boolean, 0, we can describe electrical circuits containing switches by logical, or Boolean, expressions. The expression $x_1 \bullet x_2$ represents the situation in which a series of two switches appears in a circuit (see Figure 13.7. 1a). In order for current to flow through the circuit, both switches must be on, that is, have the value 1.

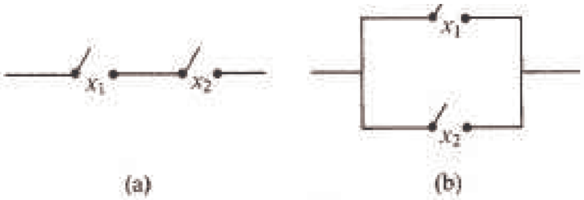
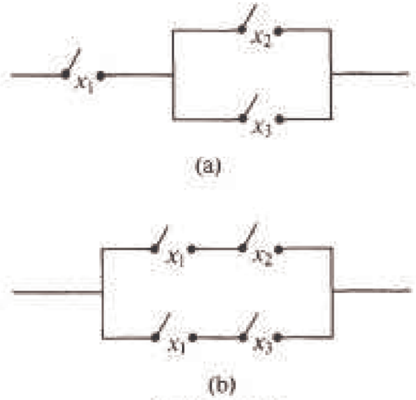


FIGURE 13.7.1

Similarly, a pair of parallel switches, as in Figure 13.7.1b, is described algebraically by $x_1 + x_2$. Many of the concepts in Boolean algebra can be thought of in terms of switching theory. For example, the distributive law in Boolean algebra (in +, • notation) is:$x_1 \bullet (x_2 + x_3) = x_1 \bullet x_2 + x_1 \bullet x_3$. Of course, this says the expression on the left is always equivalent to that on the right. The switching circuit analogue of the above statement is that Figure 13.7.2a is equivalent (as an electrical circuit) to Figure 13.7.2b.

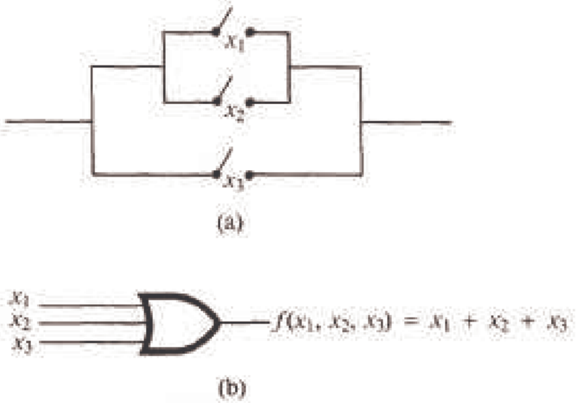
The circuits in a digital computer are composed of large quantities of switches that can be represented as in Figure 13.7.2 or can be thought of as boxes or gates with two or more inputs (except for the NOT gate) and one output. These are often drawn as in Figure 13.7.3. For example, the OR gate, as the name implies, is the logical/Boolean OR function. The on-off switch function in Figure 13.7.3a in gate notation is Figure 13.7.3b.



(a)

(b)

FIGURE 13.7.2



(a)

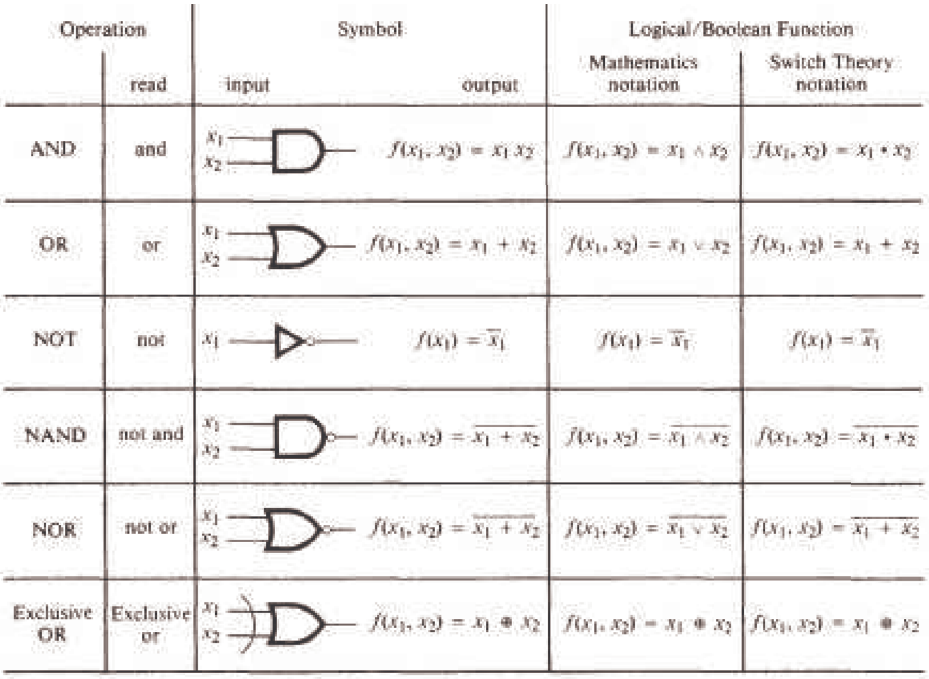
(b)

FIGURE 13.7.3

Either diagram indicates that the circuit will conduct current if and only if $f(x_1, x_2, x_3)$ is true, or 1. We list the gate symbols that are widely used in switching theory in Figure 13.7.4 with their names. The names mean, and are read, exactly as they appear. For example, NAND means "not x_1 and x_2" or algebraically, $\overline{x_1 \wedge x_2}$, or $\overline{x_1 \bullet x_2}$.

The circuit in Figure 13.7.5a can be described by gates. To do so, simply keep in mind that the Boolean function $f(x_1, x_2) = x_1 \bullet \overline{x_2}$ of this circuit contains two operations. The operation of complementation takes precedence over that of "and," so we have Figure 13.7.5b.

Example 13.7.1. The switching circuit in Figure 13.7.6a can be expressed through the logic, or gate, circuit in Figure 13.7.6b.



Operation		Symbol		Logical/Boolean Function	
	read	input	output	Mathematics notation	Switch Theory notation
AND	and	x_1 x_2	$f(x_1, x_2) = x_1 x_2$	$f(x_1, x_2) = x_1 \wedge x_2$	$f(x_1, x_2) = x_1 \bullet x_2$
OR	or	x_1 x_2	$f(x_1, x_2) = x_1 + x_2$	$f(x_1, x_2) = x_1 \vee x_2$	$f(x_1, x_2) = x_1 + x_2$
NOT	not	x_1	$f(x_1) = \overline{x_1}$	$f(x_1) = \overline{x_1}$	$f(x_1) = \overline{x_1}$
NAND	not and	x_1 x_2	$f(x_1, x_2) = \overline{x_1 + x_2}$	$f(x_1, x_2) = \overline{x_1 \wedge x_2}$	$f(x_1, x_2) = \overline{x_1 \bullet x_2}$
NOR	not or	x_1 x_2	$f(x_1, x_2) = \overline{x_1 + x_2}$	$f(x_1, x_2) = \overline{x_1 \vee x_2}$	$f(x_1, x_2) = \overline{x_1 + x_2}$
Exclusive OR	Exclusive or	x_1 x_2	$f(x_1, x_2) = x_1 \oplus x_2$	$f(x_1, x_2) = x_1 \oplus x_2$	$f(x_1, x_2) = x_1 \oplus x_2$

FIGURE 13.7.4

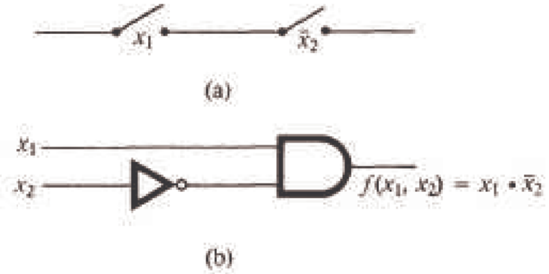
We leave it to the reader to analyze both figures and to convince him- or herself that they do describe the same circuit. The circuit can be described algebraically as

$$f(x_1,\ x_2,\ x_3) = ((x_1\ +\ x_2)\ +\ (x_1\ +\ x_3)) \bullet x_1 \bullet \overline{x_2}.$$

We can use basic Boolean algebra laws to simplify or minimize this Boolean function (circuit):

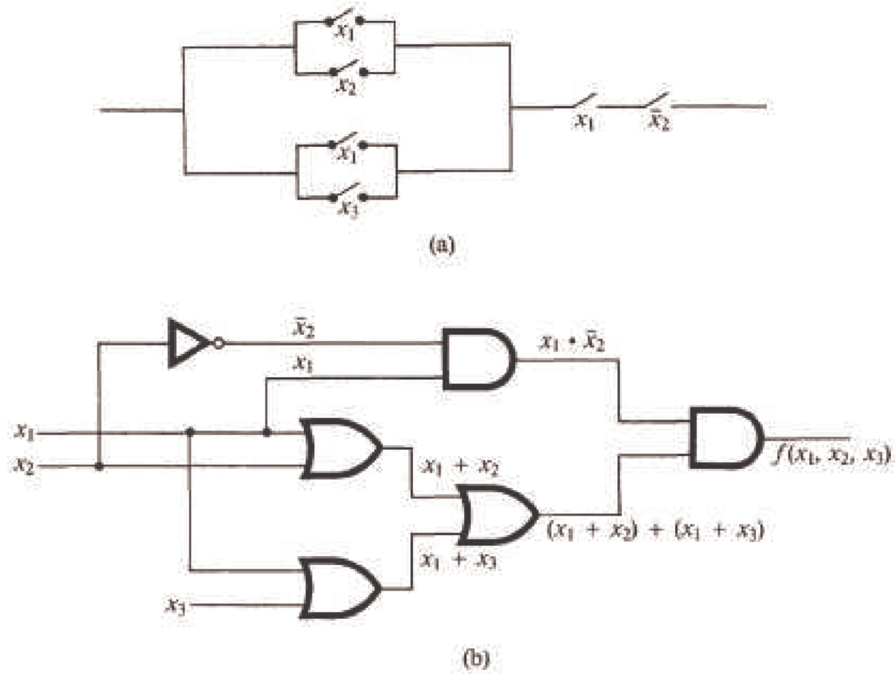
$$\begin{aligned} f(x_1,\ x_2,\ x_3) = ((x_1\ +\ x_2)\ +\ (x_1\ +\ x_3)) \bullet x_1 \bullet \overline{x_2} \\ &= (x_1 + x_2 + x_3) \bullet x_1 \bullet x_2 \\ &= (x_1 \bullet x_1 \bullet \overline{x_2} + x_2 \bullet x_1 \bullet \overline{x_2} + x_3 \bullet x_1 \bullet \overline{x_2} \\ &= x_1 \bullet \overline{x_2} + 0 \bullet x_1 + x_3 \bullet x_1 \bullet \overline{x_2} \\ &= x_1 \bullet \overline{x_2} + x_3 \bullet x_1 \bullet \overline{x_2} \\ &= x_1 \bullet (\overline{x_2} + \overline{x_2} \bullet x_3) \\ &= x_1 \bullet \overline{x_2} \bullet (1 + x_3) \\ &= x_1 \bullet \overline{x_2}. \end{aligned}$$

The circuit for *f* may be described as in Figure 13.7.5. This is a less expensive circuit since it involves considerably less hardware.


(a)

(b)

FIGURE 13.7.5


(a)

(b)

FIGURE 13.7.6

The table for *f* is:

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	0

The Venn diagram that represents *f* is the shaded portion in Figure 13.7.7. From this diagram, we can read off the minterm normal form of *f*:

$$f(x_1,\ x_2,\ x_3) = x_1 \bullet \overline{x_2} \bullet \overline{x_3}\ +\ x_1 \bullet \overline{x_2} \bullet x_3.$$

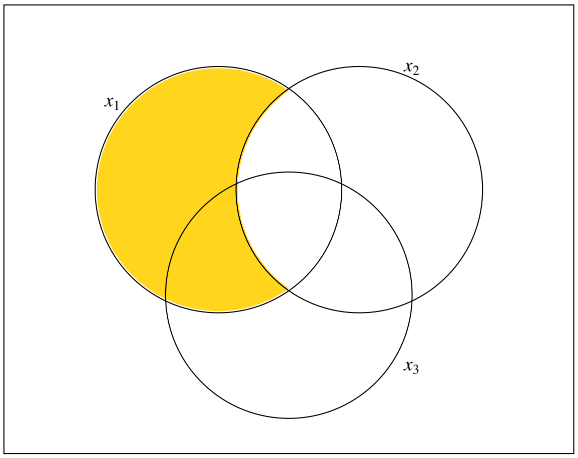


Figure 13.7.7

The circuit (gate) diagram appears in Figure 13.7.8.

How do we interpret this? We see that $f(x_1, x_2, x_3) = 1$ when $x_1 = 1$, $x_2 = 0$, and $x_3 = 0$ or $x_3 = 1$. Current will be conducted through the circuit when switch x_1 is on, switch x_2 is off, and when switch x_3 is either off or on.

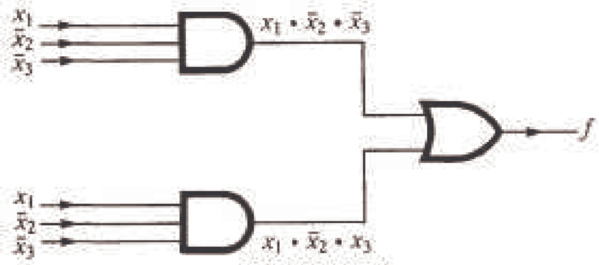

x_1
$\bar{x}_2$
$\bar{x}_3$
$x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
f
x_1
$\bar{x}_2$
x_3
$x_1 \cdot \bar{x}_2 \cdot x_3$

FIGURE 13.7.8

We close this section with a brief discussion of minimization, or reduction, techniques. We have discussed two in this text: algebraic (using basic Boolean rules) reduction and the minterm normal form technique. Other techniques are discussed in switching theory texts. When one reduces a given Boolean function, or circuit, it is possible to obtain a circuit that does not look simpler, but may be more cost effective, and is, therefore, simpler with respect to time. We illustrate with an example.

Example 13.7.2. Consider the Boolean function of Figure 13.7.9a is $f(x_1, x_2, x_3, x_4) = ((x_1 \bullet \overline{x_2)} \bullet \overline{x_3)} \bullet x_4$, which can also be diagrammed as in Figure 13.7.9b.

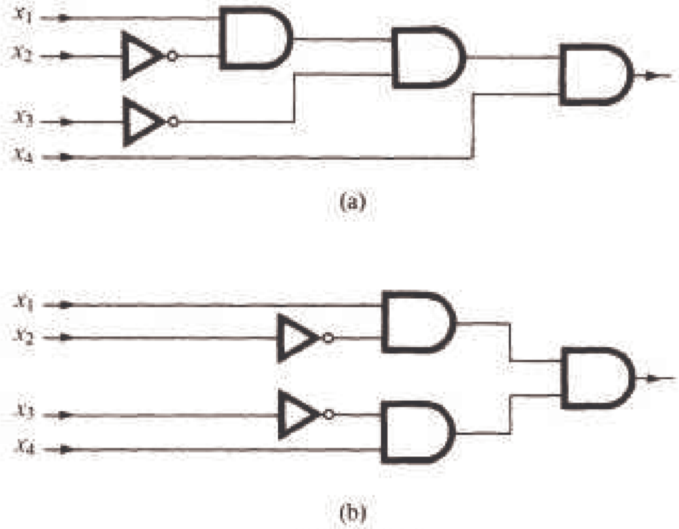


FIGURE 13.7.9

Is Circuit b simpler than Circuit a? Both circuits contain the same number of gates, so the hardware costs (per gate) would be the same. Hence, intuitively, we would guess that they are equivalent with respect to simplicity. However, the signals x_3 and x_4 in Circuit a pass through three levels of gating before reaching the output. All signals in Circuit b go through only two levels of gating (disregard the NOT gate when counting levels). Each level of logic (gates) adds to the time delay of the development of a signal at the output. In computers, we want the time delay to be as small as possible. Frequently, speed can be increased by decreasing the number of levels in a circuit. However, this frequently forces a larger number of gates to be used, thus increasing costs. One of the more difficult jobs of a design engineer is to balance off speed with hardware costs (number of gates).

One final remark on notation: The circuit in Figure 13.7.10a can be written as in Figure 13.7.10b, or simply as in Figure 13.7.10c.

EXERCISES FOR SECTION 13.7

A Exercises

1. (a) Write all inputs and outputs from Figure 13.7.11 and show that its Boolean function is $f(x_1,\ x_2,\ x_3)\ = \overline{((x_1\ +\ x_2)\bullet x_3)}\bullet(x_1\ +\ x_2)$.

(b) Simplify f algebraically.

(c) Find the minterm normal form of f.

(d) Draw and compare the circuit (gate) diagram of parts b and c above.

(e) Draw the on-off switching diagram of f in part a.

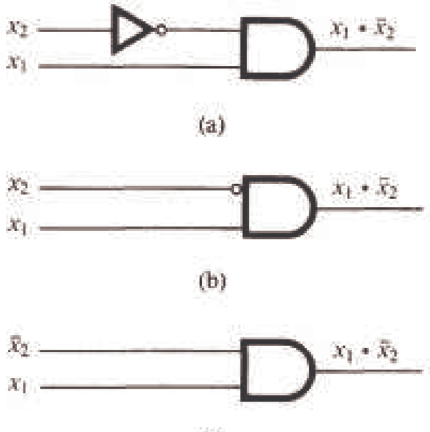


FIGURE 13.7.10

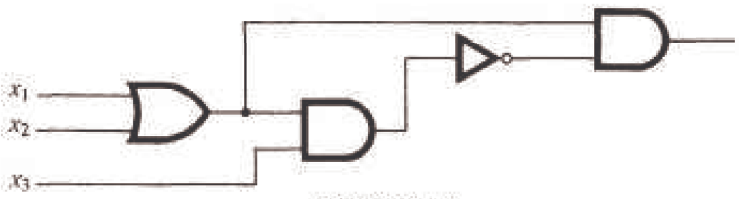


FIGURE 13.7.11

(f) Write the table of the Boolean function *f* in part a and interpret the results.

2. Given Figure 13.7.12:

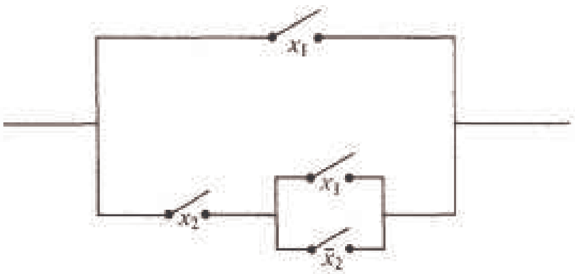


FIGURE 13.7.12

(a) Write the Boolean function that represents the given on-off circuit.

(b) Show that the Boolean function obtained in answer to part a can be reduced to $f(x_1, x_2) = x_1$. Draw the on-off circuit diagram of this simplified representation.

(c) Draw the circuit (gate) diagram of the given on-off circuit diagram.

(d) Determine the minterm normal of the Boolean function found in the answer to part a or given in part b; they are equivalent.

(e) Discuss the relative simplicity and advantages of the circuit gate diagrams found in answer to parts c and d.

3. (a) Write the circuit (gate) diagram of

$f(x_1, x_2, x_3) = (x_1 \bullet x_2 + x_3) \bullet (x_2 + x_3) + x_3$.

(b) Simplify the function in part a by using basic Boolean algebra laws.

(c) Write the circuit (gate) diagram of the result obtained in part b.

(d) Draw the on-off switch diagrams of parts a and b.

4. Consider the Boolean function

$$f(x_1, x_2, x_3, x_4) = x_1 + (x_2 \bullet (\overline{x_1} + x_4) + x_3 \bullet (\overline{x_2} + \overline{x_4})).$$

(a) Simplify *f* algebraically.

(b) Draw the switching (on-off) circuit of *f* and the reduction of *f* obtained in part a.

(c) Draw the circuit (gate) diagram of *f* and the reduction of *f* obtained in answer to part a.

SUPPLEMENTARY EXERCISES FOR CHAPTER 13

Section 13.1

1. (a) Draw the Hasse diagram of the relation divides on the set $A = \{1, 2, 3, \ldots, 12\}$.

(b) For the same set A draw the Hasse diagram for the relation $\leq$ on A.

2. (a) For the poset $A = \{1, 2, 3, \ldots, 12\}$ under the relation divides find the *lub* and *glb* of the following pairs of numbers if possible: 4 and 6, 2 and 3, 10 and 4, 6 and 9.

(b) Repeat part a for the set A, but use the relation $\leq$.

Section 13.2

3. Consider the poset $\mathbb{P}$ under the relation "divides."

(a) Compute: $4 \vee 8, 3 \vee 15, 3 \vee 5, 4 \wedge 8, 3 \wedge 15, 3 \wedge 5$ for $[\mathbb{P}, \vee, \wedge]$.

(b) Is $[\mathbb{P}, \vee, \wedge]$ a distributive lattice? Explain.

(c) Does $[\mathbb{P}, \vee, \wedge]$ have a least element? Does it have a greatest element? If so, what are they?

4. Let $[L, \vee . \wedge]$ be a lattice and $a, b \in L$. Prove:

(a) $a \vee b = b$ if and only if $a \leq b$.

(b) $a \wedge b = a$ if and only if $a \leq b$.

5. Let $L = \{0, 1\}$ and define $\leq$ on L by $0 \leq 0 \leq 1 \leq 1$.

(a) Draw the Hasse diagram of this poset.

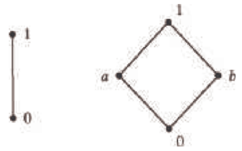
(b) Write out the operation table for $\vee$ and $\wedge$ on L observing that they are essentially the standard logical connectives.

(c) Define the operations on L^2 componentwise and draw the Hasse diagram for L^2 .

(d) Repeat part (c) for L^3.

6. (a) Let $[L_1, \vee, \wedge]$ and $[L_2, \vee, \wedge]$ be lattices. Prove that $[L_1 \times L_2, \vee, \wedge]$ is a lattice when the operations are defined componentwise as we did for algebraic systems in Section 11.6.

(b) Let L_1 and L_2 be lattices whose posets have the following Hasse diagrams respectively. List the elements in the lattice $L_1 \times L_2$.



(c) Compute:

$(0, a) \vee (0, b)$

$(0, a) \wedge (0, b)$

$(1, a) \vee (1, b)$

$(1, a) \wedge (1, b)$

$(0, 1) \vee (1, 0)$

and $(0, 1) \wedge (1, 0)$.

Use this information as an aid to draw the Hasse diagram for $L_1 \times L_2$.

7. (a) Is $A = \{1, 2, 3, \ldots, 12\}$ a lattice under the relation “divides”? Explain.

(b) Is the set A above a lattice under the relation “less than or equal to”? Explain.

Section 13.3

8. Using the rules of Boolean algebra, reduce the expression $\overline{(x_1 \lor x_2)} \bigvee (\overline{x_1} \land x_2) \bigvee (x_1 \land x_2)$ to the equivalent expression $\overline{x_1} \lor x_2$. Justify each step.

9. Using the rules of Boolean algebra, reduce the expression $(x + y) \cdot (x + \overline{y})$ to a simpler expression.

10. Even a cursory examination of the basic laws for Boolean algebra (Table 13.3.1), for logic (Table 3.4.1), and for sets (Section 4.2) will indicate that they are the same in three different languages: they are isomorphic to one another as Boolean algebras.

(a) Fill out the following table to illustrate the above concept:

	comparable connectives			
Sets	$\bigcup$			
Logic			$\bigwedge$	$\neg$
Boolean Algebraa		$\leq$		

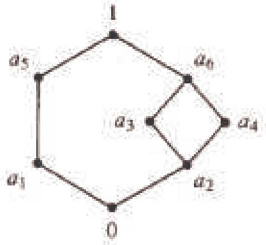
(b) Since the above algebras are isomorphic as Boolean algebras, any theorem true in one is true in the other two. Translate each of the following statements into the language of the other two.

(i) $p \to q$ if and only if $\neg q \to \neg p$.

(ii) If $A \subseteq B$ and $A \subseteq C$ then $A \subseteq B \bigcap C$

(iii) If $a \geq b$ and $a \geq c$ then $a \geq b \bigvee c$.

11. (a) Determine the complements of each element described by the following Hasse diagram:



(b) Is the above lattice a Boolean algebra?

12. (a) Determine the complement of each element in the lattice D_{50}.

(b) Is D_{50} a Boolean algebra? Explain.

Section 13.4

13. (a) Use the Theorem 13.4.2 and its Corollaries to determine which of the following are Boolean algebras:

(a) D_{20} (b) D_{27} (c) D_{35} (d) D_{210}

(b) Notice that D_n is a Boolean algebra if and only if n is a product of distinct primes. Such an integer is called *square free*. What are the atoms of D_n if n is square free?

14. Let $[B, -, \lor . \land]$ be any Boolean algebra of order 8. Find a Boolean algebra of sets that is isomorphic to B. How many atoms must B have?

Section 13.5

15. (a) List all sub-Boolean algebras of order 4 in ${B_2}^3$

(b) How many sub-Boolean algebras of order 4 are there in ${B_2}^n$, $n \geq 4$?

(c) Discuss how the selection of atoms in a sub-Boolean algebra can be used to answer questions such as the one in part (b).

16. Prove that Boolean algebras ${B_2}^m \times {B_2}^n$ and ${B_2}^{m+n}$ are isomorphic.

Section 13.6

17 Find the minterm normal form of the Boolean expression $(\overline{x_1} \lor x_2) \bigwedge x_3$

18. Find the minterm normal form of the Boolean expression

$$x_4 \wedge (x_3 \vee x_2 \vee x_1) \vee x_3 \wedge (x_2 \vee x_1) \vee x_2 \wedge x_1$$

19. Let B be a Boolean algebra of order 2.

(a) How many rows are there in the table of a Boolean function of 3 variables? Of n variables?

(b) How many different Boolean functions of 3 variables and of n variables are there?

20. Let B be a Boolean algebra of order 2.

(a) How many different minterm normal forms are there for Boolean expressions of 2 variables over B? List them.

(b) How many different minterm normal forms are there for Boolean expressions of 3 variables over B?

Section 13.7

21. Consider the following Boolean expression:

$$f(x_1, x_2, x_3) = ((x_1 + x_2 + x_3)\cdot\overline{x_1} + x_1 + \overline{x_2})\cdot x_1 \cdot \overline{x_3}$$

(a) Draw the switching circuit of f.

(b) Draw the gate diagram of f.

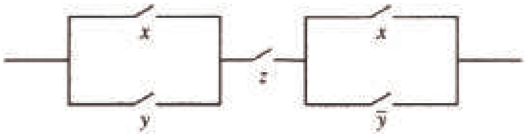
(c) Simplify f algebraically and draw the switching circuit and gate diagrams of this simplified version of f.

22. Assume that each of the three members of a committee votes *yes* or *no* on a proposal by pressing a button that closes a switch for *yes* and does nothing for *no*. Devise as simple a switching-circuit as you can that will allow current to pass when and only when at least two of the members vote in the affirmative.

23. (a) Find the Boolean function of this network:

(b) Draw an equivalent

24. Given the switching circuit

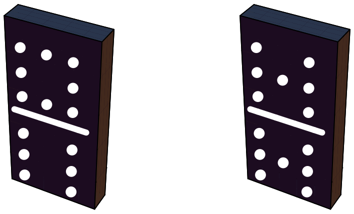


(a) Express the switching circuit algebraically.

(b) Draw the gate diagram of the expression obtained in part a.

(c) Simplify the expression in part a and draw the switching-circuit and gate diagram for the simplified expression.

chapter 14



Monoids and Automata

GOALS

At first glance, the two topics that we will discuss in this chapter seem totally unrelated. The first is monoid theory, which we touched upon in Chapter 11. The second is automata theory, in which computers and other machines are described in abstract terms. After short independent discussions of these topics, we will describe how the two are related in the sense that each monoid can be viewed as a machine and each machine has a monoid associated with it.

14.1 Monoids

Recall the definition of a monoid:

> ***Definition:*** *Monoid. A monoid is a set M together with a binary operation * with the properties*
> *(a) $*$ is associative: $(a*b)*c = a*(b*c)$ for all $a, b, c \in M$, and*
> *(b) $*$ has an identity: there exists $e \in M$ such that for all $a \in M$, $a*e = e*a = a$.*

Note: Since the requirements for a group contain the requirements for a monoid, every group is a monoid.

Example 14.1.1.

(a) The power set of any set together with any one of the operations intersection, union, or symmetric difference is a monoid.

(b) The set of integers, $\mathbb{Z}$, with multiplication, is a monoid. With addition, $\mathbb{Z}$ is also a monoid.

(c) The set of $n\times n$ matrices over the integers, $M_n(\mathbb{Z})$, $n \geq 2$, with matrix multiplication, is a monoid. This follows from the fact that matrix multiplication is associative and has an identity, I_n. This is an example of a noncommutative monoid since there are matrices, A and B, for which $A B \neq B A$.

(d) $[\mathbb{Z}_n, \times_n]$, $n \geqslant 2$, is a monoid with identity 1.

(e) Let X be a nonempty set. The set of all functions from X into X, often denoted X^X , is a monoid over function composition. In Chapter 7, we saw that function composition is associative. The function $i : X \to X$ defined by $i(a) = a$ is the identity element for this system. This is another example of a noncommutative monoid, provided $|X|$ is greater than 1.

If X is finite, $|X^X| = |X|^{|X|}$. For example, if $B = \{0, 1\}$, $|B^B| = 4$. The functions z, u, i, and t, defined by the graphs in Figure 14.1.1, are the elements of B^B . This monoid is not a group. Do you know why?

One reason that B^B is noncommutative is that $tz \neq zt$, since $(tz)(0) = 1$ and $(zt)(0) = 0$.

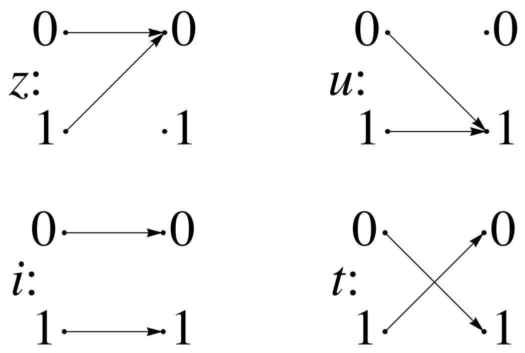


Figure 14.1.1
The four elements of B^B

GENERAL CONCEPTS AND PROPERTIES OF MONOIDS

Virtually all of the group concepts that were discussed in Chapter 11 are applicable to monoids. When we introduced subsystems, we saw that a submonoid of monoid M is a subset of M —that is, it itself is a monoid with the operation of M. To prove that a subset is a submonoid, you can apply the following algorithm.

Theorem/Algorithm 14.1.1. *Let $[M; *]$ be a monoid and K is a nonempty subset of M, K is a submonoid of M if and only if:*
(a) If $a, b \in K$, then $a * b \in K$ (i.e., K is closed under $*$), and
(b) the identity of M belongs to K.

Often we will want to discuss the smallest submonoid that includes a certain subset S of a monoid M. This submonoid can be defined recursively by the following definition.

Definition: Submonoid Generated by a Set. *If S is a subset of monoid $[M; *]$, the submonoid generated by S, $\langle S \rangle$, is defined by:*

(a) (Basis) (i) $a \in S \Rightarrow a \in \langle S \rangle$, and (ii) the identity of M belongs to $\langle S \rangle$;

(b) (Recursion), $a, b \in \langle S \rangle \Rightarrow a * b \in \langle S \rangle$.

Note: If $S = \{a_1, a_2, \ldots, a_n\}$, we write $\langle a_1, a_2, \ldots, a_n \rangle$ in place of $\langle \{a_1, a_2, \ldots, a_n\} \rangle$.

Example 14.1.2.

(a) In $[\mathbb{Z}; +]$, $\langle 2 \rangle = \{0, 2, 4, 6, 8, \ldots\}$.

(b) The power set of $\mathbb{Z}$, $\mathcal{P}(\mathbb{Z})$, over union is a monoid with identity $\emptyset$. If $S = \{\{1\}, \{2\}, \{3\}\}$, then $\langle S \rangle$ is the power set of $\{1, 2, 3\}$. If $S = \{\{n\} : n \in \mathbb{Z}\}$, then $\langle S \rangle$ is the set of finite subsets of the integers.

MONOID ISOMORPHISMS

Two monoids are *isomorphic* if and only if there exists a translation rule between them so that any true proposition in one monoid is translated to a true proposition in the other.

Example 14.1.3. $M = [\mathcal{P}\{1, 2, 3\}, \bigcap]$ is isomorphic to $M_2 = [\mathbb{Z}_2^3; \cdot]$, where the operation in M_2 is componentwise *mod 2* multiplication. A translation rule is that if $A \subseteq \{1, 2, 3\}$, then it is translated to (d_1, d_2, d_3) where $d_i = \begin{cases} 1 & \text{if } i \in A \\ 0 & \text{if } i \notin A \end{cases}$. Two cases of how this translation rule works are:

$$\begin{array}{lllcccc}
\{1, 2, 3\} \text{ is the identity for } M_1, & \text{and} & \{1, 2\} & \bigcap & \{2, 3\} & = & \{2\} \\
\updownarrow & & \updownarrow & \updownarrow & \updownarrow & & \updownarrow \\
(1, 1, 1) \text{ is the identity for } M_2, & \text{and} & (1, 1, 0) & \bullet & (0, 1, 1) & = & (0, 1, 0).
\end{array}$$

A more precise definition of a monoid isomorphism is identical to the definition of a group isomorphism (see Section 11.7).

EXERCISES FOR SECTION 14.1

A Exercises

1. For each of the subsets of the indicated monoid, determine whether the subset is a sub monoid.

(a) $S_1 = \{0, 2, 4, 6\}$ and $S_2 = \{1, 3, 5, 7\}$ in $[\mathbb{Z}_8; \times_8]$.

(b) $\{f \in \mathbb{N}^{\mathbb{N}} : f(n) \leqslant n, \forall_n \in \mathbb{N}\}$ and $\{f \in \mathbb{N}^{\mathbb{N}} : f(1) = 2\}$ in $\mathbb{N}^{\mathbb{N}}$.

(c) $\{A \subseteq \mathbb{Z} : A \text{ is finite}\}$ and $\{A \subseteq \mathbb{Z} : A^c \text{ is finite}\}$ in $[\mathcal{P}(\mathbb{Z}); \bigcup]$.

2. For each subset, describe the submonoid that it generates.

(a) $\{3\}$ and $\{0\}$ in $[\mathbb{Z}_{12}; \times_{12}]$

(b) $\{5\}$ in $[\mathbb{Z}_{25}; \times_{25}]$

(c) the set of prime numbers and $\{2\}$ in $[\mathbb{P}; \cdot]$

(d) $\{3, 5\}$ in $[\mathbb{N}; +]$

B Exercises

3. Definition: Stochastic Matrix. *An $n \times n$ matrix of real numbers is called stochastic if and only if each entry is nonnegative and the sum of entries in each column is* 1. Prove that the set of stochastic matrices is a monoid over matrix multiplication.

4. Prove Theorem 14.1.1.

14.2 Free Monoids and Languages

In this section, we will introduce the concept of a language. Languages are subsets of a certain type of monoid, the free monoid over an alphabet. After defining a free monoid, we will discuss languages and some of the basic problems relating to them. We will also discuss the common ways in which languages are defined.

Let A be a nonempty set, which we will call an *alphabet*. Our primary interest will be in the case where A is finite; however, A could be infinite for most of the situations that we will describe. The elements of A are called *letters or symbols*. Among the alphabets that we will use are $B = \{0, 1\}$, ASCII = the set of ASCII characters, and PAS = the Pascal character set (whichever one you use).

Definition: *Strings over an Alphabet. A string of length n, $n \geqslant 1$, over A is a sequence of n letters from A : $a_1 a_2 \ldots a_n$. The null string, λ, is defined as the string of length zero containing no letters. The set of strings of length n over A is denoted by A^n. The set of all strings over A. is denoted A^*.*

Notes:

(a) If the length of string s is n, we write $|s| = n$.

(b) The null string is not the same as the empty set, although they are similar in many ways.

(c) $A^* = A^0 \bigcup A^1 \bigcup A^2 \bigcup A^3 \bigcup \cdots$ and if $i \neq j$, $A^i \bigcap A^j = \emptyset$; that is, $\{A^0, A^1, A^2, A^3, \ldots\}$ is *a* partition of A^*.

(d) An element of A can appear any number of times in a string.

Theorem 14.2.1. *If A is countable, then A* is countable.*

Proof: Case 1. Given the alphabet $B = \{0, 1\}$, we can define a bijection from the positive integers into B^*. Each positive integer has a binary expansion $d_k d_{k-1} \cdots d_1 d_0$, where each d_j is 0 or 1 and $d_k = 1$. If n has such a binary expansion, then $2^k \leqslant n < 2^{k+1}$. We define $f : P \to B^*$ by $f(n) = f(d_k d_{k-1} \cdots d_1 d_0) = d_{k-1} \cdots d_1 d_0$, where $f(1) = \lambda$. Every one of the 2^k strings of length k are the images of exactly one of the integers between 2^k and $2^{k+1} - 1$. From its definition, f is clearly a bijection; therefore, B^* is countable.

Case 2: A is Finite. We will describe how this case is handled with an example first and then give the general proof. If $A = \{a, b, c, d, e)$, then we can code the letters in A into strings from B^3. One of the coding schemes (there are many) is $a \leftrightarrow 000$, $b \leftrightarrow 001$, $c \leftrightarrow 010$, $d \leftrightarrow 011$, and $e \leftrightarrow 100$. Now every string in A^* corresponds to a different string in B^*; for example, *ace* would correspond with 000 010 100. The cardinality of A^* is equal to the cardinality of the set of strings that can be obtained from this encoding system. The possible coded strings must be countable, since they are a subset of a countable set (B^*); therefore, A^* is countable.

If $|A| = m$, then the letters in A can be coded using a set of fixed-length strings from B^*. If $2^{k-1} < m \leqslant 2^k$, then there are at least as many strings of length k in B^k as there are letters in A. Now we can associate each letter in A with an element of B^k. Then any string in A^* corresponds to a string in B^*. By the same reasoning as in the example above, A^* is countable.

Case 3: A is Countably Infinite. We will leave this case as an exercise. ■

FREE MONOIDS OVER AN ALPHABET

The set of strings over any alphabet is a monoid under concatenation.

Definition: Concatenation. *Let $a = a_1 a_2 \cdots a_m$ and $b = b_1 b_2 \cdots b_n$ be strings of length m and n, respectively. The concatenation of a with b, a <> b, is the string of length $m + n$: $a_1 a_2 \cdots a_m b_1 b_2 \cdots b_n$.*

Notes:

(a) The null string is the identity element of [A^*; concatenation]. Henceforth, we will denote the monoid of strings over A by A^*.

(b) Concatenation is noncommutative, provided $|A| > 1$.

(c) If $|A_1| = |A_2|$, then the monoids A_1^* and A_2^* are isomorphic. An isomorphism can be defined using any bijection $f : A_1 \to A_2$. If $a = a_1 a_2 \cdots a_n \in A_1^*$, $f^*(a) = f(a_1) f(a_2) \cdots f(a_n)$ defines a bijection from A_1^* into A_2^*. We will leave it to the reader to convince him or herself that for all $a, b, \in A_1^*$, $f^*(a <> b) = f^*(a) <> f^*(b)$.

LANGUAGES

The languages of the world—English, German, Russian, Chinese, and so forth—are called natural languages. In order to communicate in writing in any one of them, you must first know the letters of the alphabet and then know how to combine the letters in meaningful ways. A *formal language* is an abstraction of this situation.

Definition: Formal Language. *If A is an alphabet, a formal language over A is a subset of A*.*

Example 14.2.1.

(a) English can be thought of as a language over the set of letters $A, B, \cdots Z$ (upper and lower case) and other special symbols, such as punctuation marks and the blank. Exactly what subset of the strings over this alphabet defines the English language is difficult to pin down exactly. This is a characteristic of natural languages that we try to avoid with formal languages.

(b) The set of all ASCII stream files can be defined in terms of a language over ASCII. An ASCII stream file is a sequence of zero or more lines followed by an end-of-file symbol. A line is defined as a sequence of ASCII characters that ends with the two characters CR (carriage return) and LF (line feed). The end-of-file symbol is system-dependent; for example, CTRL/C is a common one.

(c) The set of all syntactically correct expressions in *Mathematica* is a language over the set of ASCII strings.

(d) A few languages over B are

$L_1 = \{s \in B^* \mid s \text{ has exactly as many } 1's \text{ as it has } 0's\}$,

$L_2 = \{1 <> s <> 0 : s \in B^*\}$, and

$L_3 = \langle 0, 01 \rangle$ = the submonoid of B^* generated by $\{0, 01\}$.

TWO FUNDAMENTAL PROBLEMS: RECOGNITION AND GENERATION

The generation and recognition problems are basic to computer programming. Given a language, L, the programmer must know how to write (or generate) a syntactically correct program that solves a problem. On the other hand, the compiler must be written to recognize whether a program contains any syntax errors.

The Recognition Problem: Design an algorithm that determines the truth of $s \in L$ in a finite number of steps for all $a \in A^*$. Any such algorithm is called a *recognition algorithm*.

Definition: *Recursive Language. A language is recursive if there exists a recognition algorithm for it.*

Example 14.2.2.

(a) The language of syntactically correct *Mathematica* expressions is recursive.

(b) The three languages in Example 14.2.1 (d) are all recursive. Recognition algorithms for L_1 and L_2 should be easy for you to imagine. The reason a recognition algorithm for L_3 might not be obvious is that $L_3's$ definition is more cryptic. It doesn't tell us what belongs to L_3, just what can be used to create strings in L_3. This is how many languages are defined. With a second description of L_3, we can easily design a recognition algorithm. $L_3 = \{s \in B^*;\ s = \lambda$ or s starts with a 0 and has no consecutive 1's$\}$.

Algorithm 14.2.1: Recognition Algorithm for L_3. Let $s = s_1 s_2 \cdots s_n \in B^*$. This algorithm determines the truth value of $s \in L_3$. The truth value is returned as the value of Word.

```
(1) Word := true
(2) If $n > 0$ then
        If $s_1 = 1$ then Word := false
                else for $i := 3$ to $n$
                        if $s_{i-1} = 1$ and $s_i = 1$ then Word := false
```

The Generation Problem. Design an algorithm that generates or produces any string in L. Here we presume that A is either finite or countably infinite; hence, A^* is countable by Theorem 14.2.1, and $L \subseteq A^*$ must be countable. Therefore, the generation of L amounts to creating a list of strings in L. The list may be either finite or infinite, and you must be able to show that every string in L appears somewhere in the list.

Theorem 14.2.2.

(a) If A is countable, then there exists a generating algorithm for A.*

(b) If L is a recursive language over a countable alphabet, then there exists a generating algorithm for L.

Proof:

(a) Part a follows from the fact that A^* is countable; therefore, there exists a complete list of strings in A^*.

(b) To generate all strings of L, start with a list of all strings in A^* and an empty list, W, of strings in L. For each string s, use a recognition algorithm (one exists since L is recursive) to determine whether $s \in L$. If s is in L, add it to W; otherwise "throw it out." Then go to the next string in the list of A^*. ■

Example 14.2.3. Since all of the languages in Example 14.2.2 are recursive, they must have generating algorithms. The one given in the proof of Theorem 14.2.2 is not generally the most efficient. You could probably design more efficient generating algorithms for L_2 and L_3; however, a better generating algorithm for L_1 is not quite so obvious.

The recognition and generation problems can vary in difficulty depending on how a language is defined and what sort of algorithms we allow ourselves to use. This is not to say that the means by which a language is defined determines whether it is recursive. It just means that the truth of "L is recursive" may be more difficult to determine with one definition than with another. We will close this section with a discussion of grammars, which are standard forms of definition for a language. When we restrict ourselves to only certain types of algorithms, we can affect our ability to determine whether $s \in L$ is true. In defining a recursive language, we do not restrict ourselves in any way in regard to the type of algorithm that will be used. In Section 14.3, we will consider machines called *finite automata*, which can only perform simple algorithms.

PHRASE STRUCTURE GRAMMARS AND LANGUAGES

One common way of defining a language is by means of a *phrase structure grammar* (or grammar, for short). The set of strings that can be produced using the grammar rules is called the *phrase structure language* (of the grammar).

Example 14.2.4. We can define the set of all strings over B for which all 0s precede all 1s as follows. Define the starting symbol S and establish rules that S can be replaced with any of the following: λ, 0S, or S1. These replacement rules are usually called *production* (or *rewriting*) *rules* and are usually written in the format $S \to \lambda$, $S \to 0\,S$, and $S \to$ S1. Now define L to be the set of all strings that can be produced by starting with S and applying the production rules until S no longer appears. The strings in L are exactly the ones that are described above.

Definition: *Phrase Structure Grammar. A phrase structure grammar consists of four components:*

(1) A nonempty finite set of terminal characters, T. If the grammar is defining a language over A, T is a subset of A.*
(2) A finite set of nonterminal characters, N.
(3) A starting symbol, $S \in N$.
(4) A finite set of production rules, each of the form $X \to Y$, where X and Y are strings over $A \bigcup N$ such that $X \neq Y$ and X contains at least one nonterminal symbol.

If G is a phrase structure grammar, $L(G)$ is the set of strings that can be obtained by starting with S and applying the production rules a finite number of times until no nonterminal characters remain. If a language can be defined by a phrase structure grammar, then it is called a *phrase structure language*.

Example 14.2.5. The language over B consisting of strings of alternating 0s and 1s is a phrase structure language. It can be defined by the following grammar:

(1) Terminal characters: λ, 0, and 1,

(2) Nonterminal characters: S, T, and U,

(3) Starting symbol: S,

(4) Production rules:

$$S \to T,\ S \to U,\ S \to \lambda,\ S \to 0,\ S \to 1,\ S \to 0\,T,$$
$$S \to 1\,U,\ T \to 10\,T,\ T \to 10,\ U \to 01\,U,\ U \to 01$$

These rules can be visualized more easily with a graph:

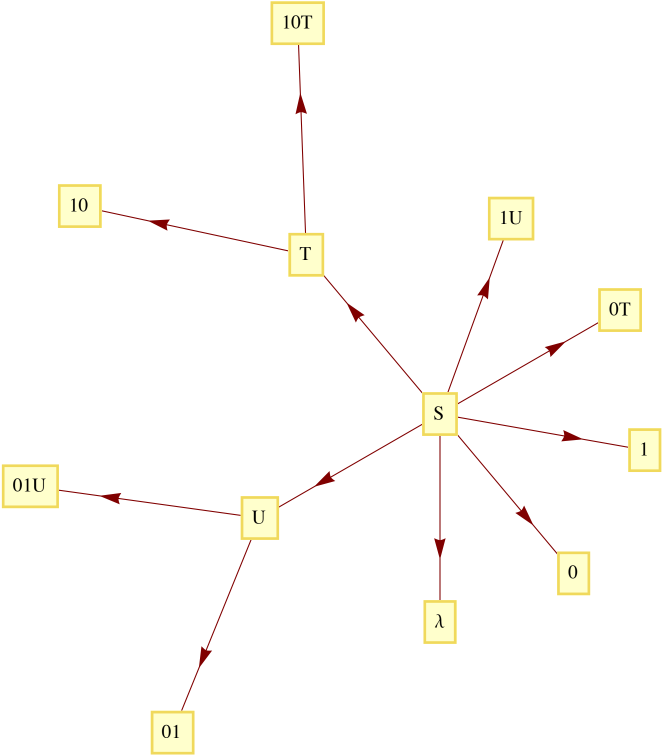


Figure 14.2.1
Production rules for the language of alternating 0's and 1's.

We can verify that a string such as 10101 belongs to the language by starting with S and producing 10101 using the production rules a finite number of times: $S \to 1\,U \to 101\,U \to 10\,101$.

Example 14.2.6. Let G be the grammar with components:

(1) Terminal symbols = all letters of the alphabet (both upper and lower case) and the digits 0 through 9,

(2) Nonterminal symbols $=\{I, X\}$,

(3) Starting symbol: I

(4) Production rules: $I \to \alpha$, where α is any letter, $I \to \alpha$X for any letter α, $X \to \beta$X for any letter or digit β, and $X \to \beta$ for any letter or digit β.

There are a total of 176 production rules for this grammar. The language $L\,(G)$ consists of all valid *Mathematica* names.

Backus-Naur form (BNF), A popular alternate form of defining the production rules in a grammar is BNF. If the production rules $A \to B_1,\ A \to B_2,\ \ldots A \to B_n$ are part of a grammar, they would be written in BNF as $A :: = B_1\,|B_2| \cdots |B_n$. The symbol | in BNF is read as "or," while the :: = is read as "is defined as." Additional notations of BNF are that $\{x\}$, represents zero or more repetitions of x and $[y]$ means that y is optional.

Example 14.2.7. A BNF version of the production rules for a *Mathematica* name is

$$\text{letter } :: \ = a\,|b\,|c \cdots \ |\, z \,|\, A \,|\, B \,|\, \cdots \,|\, Z$$

$$\text{digit} :: = 0 \,|\, 1 \,|\, \cdots \,|\, 9$$

$$I :: \ = \ \text{letter}\,\{\text{letter} \ | \ \text{digit}\}$$

Example 14.2.8. An arithmetic expression can be defined in BNF. For simplicity, we will consider only expressions obtained using addition and multiplication of integers. The terminal symbols are (,), +, $*$, −, and the digits 0 through 9. The nonterminal symbols are E (for expression), T (term), F (factor), and N (number). The starting symbol is E.

$$E \ :: = E + T \,|\, T$$

$$T ::= T * F \mid F$$

$$F ::= (E) \mid N$$

$$N ::= [-] \text{ digit } \{\text{digit}\}.$$

One particularly simple type of phrase structure grammar is the regular grammar.

Definition: Regular Grammar. *A regular (right-hand form) grammar is a grammar whose production rules are all of the form $A \to t$ and $A \to tB$, where A and B are nonterminal and t is terminal. A left-hand form grammar allows only $A \to t$ and $A \to Bt$, A language that has a regular phrase structure language is called a regular language.*

Example 14.2.9.

(a) The set of *Mathematica* names is a regular language since the grammar by which we defined the set is a regular grammar.

(b) The language of all strings for which all 0s precede all 1s (Example 14.2.4) is regular; however, the grammar by which we defined this set is not regular. Can you define these strings with a regular grammar?

(c) The language of arithmetic expressions is not regular.

EXERCISES FOR SECTION 14.2

A Exercises

1. (a) If a computer is being designed to operate with a character set of 350 symbols, how many bits must be reserved for each character? Assume each character will use the same number of bits.

(b) Do the same for 3,500 symbols.

2. It was pointed out in the text that the null string and the null set are different. The former is a string and the latter is a set, two different kinds of objects. Discuss how the two are similar.

3. What sets of strings are defined by the following grammar?

(a) Terminal symbols: λ, 0 and 1

(b) Nonterminal symbols: S and E

(c) Starting symbol: S

(d) Production rules: $S \to 0\,S0,\ S \to 1\,S1,\ S \to E,\ E \to \lambda,\ E \to 0,\ E \to 1.$

4. What sets of strings are defined by the following grammar?

(a) Terminal symbols: λ, a, b, and c

(b) Nonterminal symbols: S, T, U and E

(c) Starting symbol: S

(d) Production rules: $S \to aS,\ S \to T,\ T \to bT,\ T \to U,\ U \to cU,\ U \to E,\ E \to \lambda.$

5. Define the following languages over B with phrase structure grammars.

Which of these languages are regular?

(a) The strings with an odd number of characters.

(b) The strings of length 4 or less.

(c) The palindromes, strings that are the same backwards as forwards.

6. Define the following languages over B with phrase structure grammars. Which of these languages are regular?

(a) The strings with more 0s than 1s.

(b) The strings with an even number of 1s.

(c) The strings for which all 0s precede all 1s.

7. Prove that if a language over A is recursive, then its complement is also recursive.

8. Use BNF to define the grammars in Exercises 3 and 4.

B Exercise

9. (a)Prove that if $X_1,\ X_2,\ \ldots$ is a countable sequence of countable sets, the union of these sets, $\bigcup_{i=1}^{\infty} X_i$, is countable.

(b) Using the fact that the countable union of countable sets is countable, prove that if A is countable, then A^* is countable.

14.3 Automata, Finite-State Machines

In this section, we will introduce the concept of an abstract machine. The machines we will examine will (in theory) be capable of performing many of the tasks associated with digital computers. One such task is solving the recognition problem for a language. We will concentrate on one class of machines, finite-state machines (finite automata). And we will see that they are precisely the machines that are capable of recognizing strings in a regular grammar.

Given an alphabet X, we will imagine a string in X^* to be encoded on a tape that we will call an *input tape*. When we refer to a tape, we might imagine a strip of material that is divided into segments, each of which can contain either a letter or a blank.

The typical abstract machine includes an input device, the *read head*, which is capable of reading the symbol from the segment of the input tape that is currently in the read head. Some more advanced machines have a read/write head that can also write symbols onto the tape. The movement of the input tape after reading a symbol depends on the machine. With a finite-state machine, the next segment of the input tape is always moved into the read head after a symbol has been read. Most machines (including finite-state machines) also have a separate output tape that is written on with a *write head*. The output symbols come from an output alphabet, Z, that may or may not be equal to the input alphabet. The most significant component of an abstract machine is its *memory structure*. This structure can range from a finite number of bits of memory (as in a finite-state machine) to an infinite amount of memory that can be sorted in the form of a tape that can be read from and written on (as in a Turing machine).

Definition: *Finite-State Machine. A finite-state machine is defined by a quintet* $(S,\ X,\ Z,\ w,\ t)$ *where*

(1) $S = \{s_1,\ s_2,\ \ldots,\ s_r\}$ *is the state set, a finite set that corresponds to the set of memory configurations that the machines can have at any time.*

(2) $X = \{x_1,\ x_2,\ \ldots, x_m\}$ *is the input alphabet.*

(3) $Z = \{z_1, z_2,\ \ldots, z_n\}$ *is the output alphabet.*

(4) $w : X \times S \to Z$ *is the output function, which specifies which output symbol* $w(x,\ s)\ \in Z$ *is written onto the output tape when the machine is in state s and the input symbol x is read.*

(5) $t : X \times S \to S$ *is the next-state (or transition) function, which specifies which state*$t(x,\ s)\ \in S$ *the machine should enter when it is in state s and it reads the symbol x.*

Example 14.3.1. Many mechanical devices, such as simple vending machines, can be thought of as finite-state machines. For simplicity, assume that a vending machine dispenses packets of gum, spearmint *(S)*, peppermint *(P)*, and bubble *(B)*, for 25¢ each. We can define the input alphabet to be {deposit 25 ¢, press S, press P, press B} and the state set to be {Locked, Select}, where the deposit of a quarter unlocks the release mechanism of the machine and allows you to select a flavor of gum. We will leave it to the reader to imagine what the output alphabet, output function, and next-state function would be. You are also invited to let your imagination run wild and include such features as a coin-return lever and change maker.

Example 14.3.2. The following machine is called a *parity checker*. It recognizes whether or not a string in B^* contains an even number of 1s. The memory structure of this machine reflects the fact that in order to check the parity of a string, we need only keep track of whether an odd or even number of 1s has been detected.

(1) The input alphabet is $B = \{0,\ 1\}$.

(2) The output alphabet is also B.

(3) The state set is {even, odd}.

(4, 5) The following table defines the output and next-state functions:

x	s	$w(x,\ s)$	$t(x,\ s)$
0	even	0	even
0	odd	1	odd
1	even	1	odd
1	odd	0	even

Note how the value of the most recent output at any time is an indication of the current state of the machine. Therefore, if we start in the even state and read any finite input tape, the last output corresponds to the final state of the parity checker and tells us the parity of the string on the input tape. For example, if the string 11001010 is read from left to right, the output tape, also from left to right, will be 10001100. Since the last character is a 0, we know that the input string has even parity.

An alternate method for defining a finite-state machine is with a transition diagram. A *transition diagram* is a directed graph that contains a node for each state and edges that indicate the transition and output functions. An edge $\left(s_i,\ s_j\right)$ that is labeled x/z indicates that in state s_i the input x results in an output of z and the next state is s_j. That is, $w(x, s_i) = z$ and $t(x, s_i) = s_j$. The transition diagram for the parity checker appears in Figure 14.3.1. In later examples, we will see that if different inputs, x_i and x_j, while in the same state, result in the same transitions and outputs, we label a single edge $x_i, x_j/z$ instead of drawing two edges with labels x_i/z and x_j/z.

One of the most significant features of a finite-state machine is that it retains no information about its past states that can be accessed by the machine itself. For example, after we input a tape encoded with the symbols 01101010 into the parity checker, the current state will be even, but we have no indication within the machine whether or not it has always been in even state. Note how the output tape is not considered part of the machine's memory. In this case, the output tape does contain a "history" of the parity checker's past states. We assume that the finite-state machine has no way of recovering the output sequence for later use.

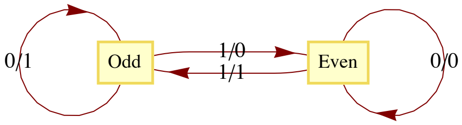


Figure 14.3.1
Transition Diagram for a parity checker

Example 14.3.3. Consider the following simplified version of the game of baseball. To be precise, this machine describes one half-inning of a simplified baseball game. Suppose that in addition to home plate, there is only one base instead of the usual three bases. Also, assume that there are only two outs per inning instead of the usual three. Our input alphabet will consist of the types of hits that the batter could have: out (O), double play (DP), single (S), and home run (HR). The input DP is meant to represent a batted ball that would result in a double play (two outs), if possible. The input DP can then occur at any time. The output alphabet is the numbers 0, 1, and 2 for the number of runs that can be scored as a result of any input. The state set contains the current situation in the inning, the number of outs, and whether a base runner is currently on the base. The list of possible states is then 00 (for 0 outs and 0 runners), 01, 10, 11, and end (when the half-inning is over). The transition diagram for this machine appears in Figure 14.3.2.

Let's concentrate on one state. If the current state is 01, 0 outs and 1 runner on base, each input results in a different combination of output and next-state. If the batter hits the ball poorly (a double play) the output is zero runs and the inning is over (the limit of two outs has been made). A simple out also results in an output of 0 runs and the next state is 11, one out and one runner on base. If the batter hits a single, one run scores (output = 1) while the state remains 01. If a home run is hit, two runs are scored (output = 2) and the next state is 00. If we had allowed three outs per inning, this graph would only be marginally more complicated. The usual game with three bases would be quite a bit more complicated, however.

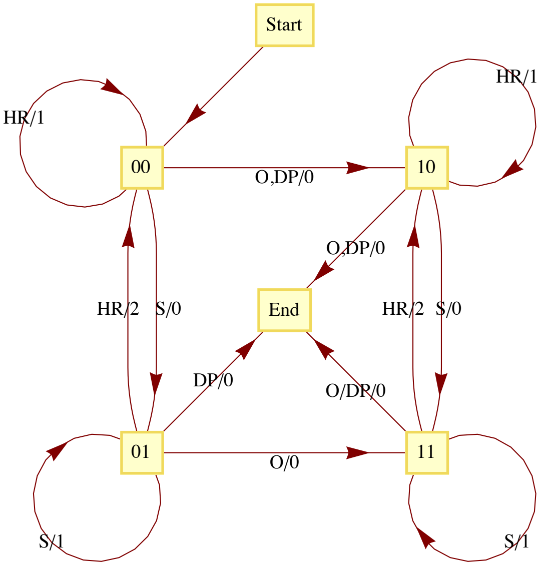


Figure 14.3.2
Transition Diagram for a simplified game of baseball

RECOGNITION IN REGULAR LANGUAGES

As we mentioned at the outset of this section, finite-state machines can recognize strings in a regular language. Consider the language L over $\{a, b, c\}$ that contains the strings of positive length in which each a is followed by b and each b is followed by c. One such string is $bccabcbc$. This language is regular. A grammar for the language would be nonterminal symbols $\{A, B, C\}$ with starting symbol C and production rules

$A \to \mathrm{bB},\ \mathrm{cC},\ C \to aA,\ C \to cC$ and $C \to c$. A finite-state machine (Figure 14.3.3) that recognizes this language can be constructed with one state for each nonterminal symbol and an additional state (Reject) that is entered if any invalid production takes place. At the end of an input tape that encodes a string in $\{a, b, c\}^*$, we will know when the string belongs to L based on the final output. If the final output is 1, the string belongs to L and if it is 0, the string does not belong to L. In addition, recognition can be accomplished by examining the final state of the machine. The input string belongs to the language if and only if the final state is C.

The construction of this machine is quite easy: note how each production rule translates into an edge between states other than Reject. For example, $C \to b\mathrm{B}$ indicates that in State C, an input of b places the machine into State B. Not all sets of production rules can be as easily translated to a finite-state machine. Another set of production rules for L is $A \to \mathrm{aB},\ B \to bC,\ C \to \mathrm{cA},\ C \to \mathrm{cB},\ C \to cC$ and $C \to c$. Techniques for constructing finite-state machines from production rules is not our objective here. Hence we will only expect you to experiment with production rules until appropriate ones are found.

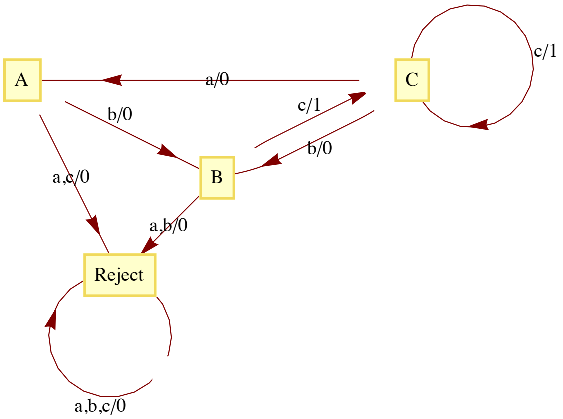


Figure 14.3.3

Example 14.3.4. A finite-state machine can be designed to add positive integers of any size. Given two integers in binary form, $a = a_n\, a_{n-1} \cdots a_1\, a_0$ and $b = b_n\, b_{n-1} \cdots b_1\, b_0$, the machine will read the input sequence, which is obtained from the digits of a and b reading from right to left,

$$a_0\, b_0(a_0 +_2 b_0)\,,\ \ldots,\ a_n\, b_n(a_n +_2 b_n),$$

followed by the special input 111. Note how all possible inputs except the last one must even parity (contain an even number of ones). The output sequence is the sum of a and b, starting with the units digit, and comes from the set $\{0, 1, \lambda\}$. The transition diagram for this machine appears in Figure 14.3.4.

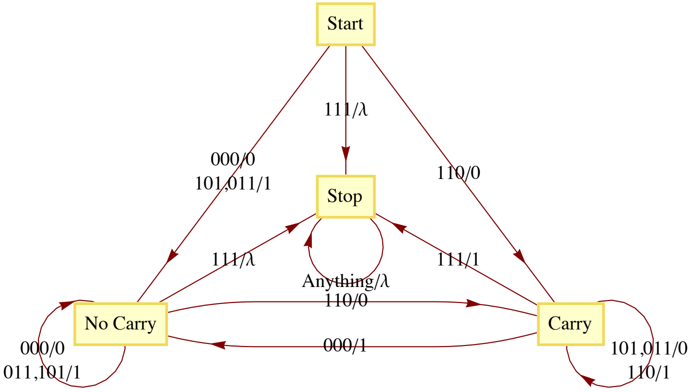


Figure 14.3.4
Transition Diagram for a binary adder

EXERCISES FOR SECTION 14.3

A Exercises

1. Draw a transition diagram for the vending machine described in Example

14.3.1.

2. Construct finite-state machines that recognize the regular languages that you identified in Section 14.2.

3. What is the input set for the machine in Example 14.3.4?

4. What input sequence would be used to compute the sum of 1101 and 0111 (binary integers)? What would the output sequence be?

B Exercise

5. *The Gray Code Decoder*. The finite-state machine defined by the following figure has an interesting connection with the Gray Code (Section 9.4).

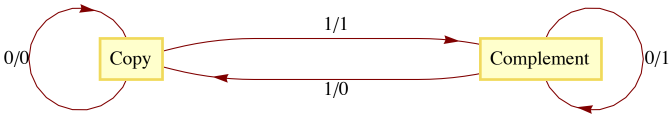


Figure 14.3.5
Gray Code Decoder

Given a string $x = x_1\, x_2 \cdots x_n \in B^n$, we may ask where x appears in G_n. Starting in Copy state, the input string x will result in an output string $z \in B^n$, which is the binary form of the position of x in G_n Positions are numbered from 0 to $2^n - 1$.

(a) In what positions $(0 - 31)$ do $10110, 00100$, and 11111 appear in G_5?

(b) Prove that the Gray Code Decoder always works.

14.4 The Monoid of a Finite-State Machine

In this section, we will see how every finite-state machine has a monoid associated with it. For any finite-state machine, the elements of its associated monoid correspond to certain input sequences. Because only a finite number of combinations of states and inputs is possible for a finite-state machine there is only a finite number of input sequences that summarize the machine This idea is illustrated best with a few examples.

Example 14.4.1. Consider the parity checker. The following table summarizes the effect on the parity checker of strings in B^1 and B^2 . The row labeled "Even" contains the final state and final output as a result of each input string in B^1 and B^2 when the machine starts in the even state. Similarly, the row labeled "Odd" contains the same information for input sequences when the machine starts in the odd state.

Input String	0	1	00	01	10	11
Even	(Even, 0)	(Odd, 1)	(Even, 0)	(Odd, 1)	(Odd, 1)	(Even, 0)
Odd	(Odd, 1)	(Even, 1)	(Odd, 1)	(Even, 1)	(Even, 0)	(Odd, 1)
Same Effect as			0	1	1	0

Note how, as indicated in the last row, the strings in B^2 have the same effect as certain strings in B^1. For this reason, we can summarize the machine in terms of how it is affected by strings of length 1. The actual monoid that we will now describe consists of a set of functions, and the operation on the functions will be based on the concatenation operation.

Let T_0 be the final effect (state and output) on the parity checker of the input 0. Similarly, T_1 is defined as the final effect on the parity checker of the input 1. More precisely,

$T_0(\text{even}) = (\text{even}, 0)$ and $T_0(\text{odd}) = (\text{odd}, 1)$,

while

$T_1(\text{even}) = (\text{odd}, 1)$ and $T_1(\text{odd}) = (\text{even}, 0)$.

In general, we define the operation on a set of such functions as follows: if s, t are input sequences and T_s and T_t, are functions as above, then $T_s * T_t = T_{st}$, that is, the result of the function that summarizes the effect on the machine by the concatenation of s with t. Since, for example, 01 has the same effect on the parity checker as 1, $T_0 * T_1 = T_{01} = T_1$. We don't stop our calculation at T_{01} because we want to use the shortest string of inputs to describe the final result. A complete table for the monoid of the parity checker is

$*$	T_0	T_1
T_0	T_0	T_1
T_1	T_1	T_0

What is the identify of this monoid? The monoid of the parity checker is isomorphic to the monoid $[\mathbb{Z}_2, +_2]$.

This operation may remind you of the composition operation on functions, but there are two principal differences. The domain of T_s is not the codomain of T_t and the functions are read from left to right unlike in composition, where they are normally read from right to left.

You may have noticed that the output of the parity checker echoes the state of the machine and that we could have looked only at the effect on the machine as the final state. The following example has the same property, hence we will only consider the final state.

Example 14.4.2. The transition diagram for the machine that recognizes strings in B^* that have no consecutive 1's appears in Figure

14.4.1. Note how it is similar to the graph in Figure 9.1.1. Only a "reject state" has been added, for the case when an input of 1 occurs while in State a. We construct a similar table to the one in the previous example to study the effect of certain strings on this machine. This time, we must include strings of length 3 before we recognize that no "new effects" can be found.

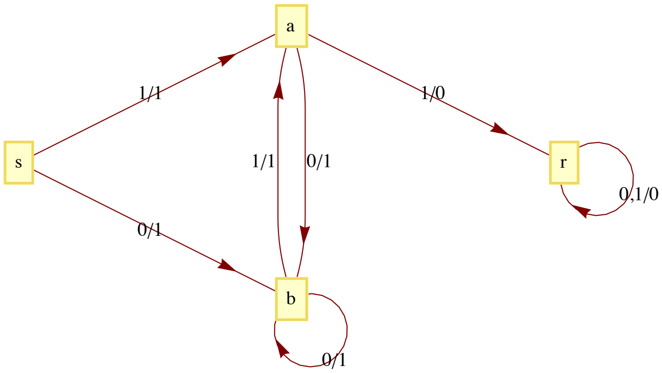


Figure 14.4.1

Inputs	0	1	00	01	10	11	000	001	010	011	100	101	110	111
s	b	a	b	a	b	r	b	a	b	r	b	a	r	r
a	b	r	b	a	r	r	b	a	b	r	r	r	r	r
b	b	a	b	a	b	r	b	a	b	r	b	a	r	r
r	r	r	r	r	r	r	r	r	r	r	r	r	r	r
Same as			0				0	01	0	11	10	1	11	11

The following table summarizes how combinations of the strings 0, 1, 01, 10, and 11 affect this machine.

$*$	T_0	T_1	T_{01}	T_{10}	T_{11}
T_0	T_0	T_1	T_{01}	T_{10}	T_{11}
T_1	T_{10}	T_{11}	T_1	T_{11}	T_{11}
T_{01}	T_0	T_{11}	T_{01}	T_{11}	T_{11}
T_{10}	T_{10}	T_1	T_1	T_{10}	T_{11}
T_{11}	T_{11}	T_{11}	T_{11}	T_{11}	T_{11}

All the results in this table can be obtained using the previous table. For example,

$$T_{10} * T_{01} = T_{1001} = T_{100} * T_1 = T_{10} * T_1 = T_{101} = T_1$$

and

$$T_{01} * T_{01} = T_{0101} = T_{010}\, T_1 = T_0\, T_1 = T_{01}.$$

Note that none of the elements that we have listed in this table serves as the identity for our operation. This problem can always be remedied by including the function that corresponds to the input of the null string, T_λ. Since the null string is the identity for concatenation of strings, $T_s\, T_\lambda = T_\lambda\, T_s = T_s$ for all input strings s.

Example 14.4.3. A finite-state machine called the unit-time delay machine does not echo its current state, but prints its previous state. For this reason, when we find the monoid of the unit-time delay machine, we must consider both state and output. The transition diagram of this machine appears in Figure 14.4.2.

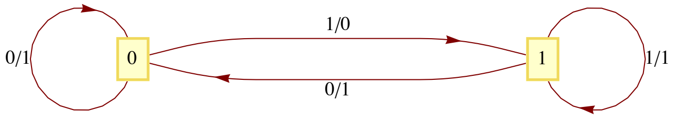


Figure 14.4.2

Input	0	1	00	01	10	11	100 or 000	101 or 001	110 or 101	111 or 011
0	(0, 0)	(1, 0)	(0, 0)	(1, 0)	(0, 1)	(1, 1)	(0, 0)	(1, 0)	(0, 1)	(1, 1)
1	(0, 1)	(1, 1)	(0, 0)	(1, 0)	(0, 1)	(1, 1)	(0, 0)	(1, 0)	(0, 1)	(1, 1)
Same as							00	01	10	11

Again, since no new outcomes were obtained from strings of length 3, only strings of length 2 or less contribute to the monoid of the machine. The table for the strings of positive length shows that we must add T_λ to obtain a monoid.

$*$	T_0	T_1	T_{00}	T_{01}	T_{10}	T_{11}
T_0	T_{00}	T_{01}	T_{00}	T_{01}	T_{10}	T_{11}
T_1	T_{10}	T_{11}	T_{00}	T_{01}	T_{10}	T_{11}
T_{00}	T_{00}	T_{01}	T_{00}	T_{01}	T_{10}	T_{11}
T_{01}	T_{10}	T_{11}	T_{00}	T_{01}	T_{10}	T_{11}
T_{10}	T_{00}	T_{01}	T_{00}	T_{01}	T_{10}	T_{11}
T_{11}	T_{10}	T_{11}	T_{00}	T_{01}	T_{10}	T_{11}

EXERCISES FOR SECTION 14.4

A Exercise

1. For each of the transition diagrams in Figure 14.4.3, write out tables for their associated monoids. Identify the identity in terms of a string of positive length, if possible. (*Hint*: Where the output echoes the current state, the output can be ignored.)

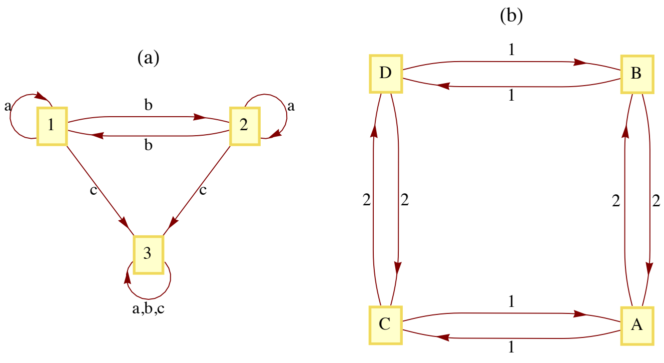


Figure 14.4.3

B Exercise

2. What common monoids are isomorphic to the monoids obtained in the previous exercise?

C Exercise

3. Can two finite-state machines with nonisomorphic transition diagrams have isomorphic monoids?

14.5 The Machine of a Monoid

Any finite monoid $[M, *]$ can be represented in the form of a finite-state machine with input and state sets equal to M. The output of the machine will be ignored here, since it would echo the current state of the machine. Machines of this type are called *state machines*. It can be shown that whatever can be done with a finite-state machine can be done with a state machine; however, there is a trade-off. Usually, state machines that perform a specific function are more complex than general finite-state machines.

Definition: Machine of a Monoid. *If* $[M, *]$ *is a finite monoid, then the machine of M, denoted m(M), is the state machine with state set M, input set M, and next-state function* $t : M \times M \to M$ *defined by* $t(s, x) = s * x$.

Example 14.5.1. We will construct the machine of the monoid $[\mathbb{Z}_2; +_2]$. As mentioned above, the state set and the input set are both $\mathbb{Z}_2$. The next state function is defined by $t(s, x) = s +_2 x$. The transition diagram for $m(\mathbb{Z}_2)$ appears in Figure 14.5.1. Note how it is identical to the transition diagram of the parity checker, which has an associated monoid that was isomorphic to $[\mathbb{Z}_2, +_2]$.

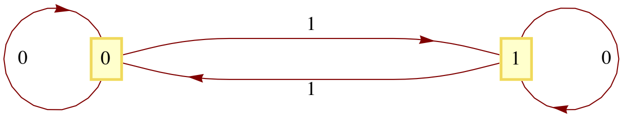


Figure 14.5.1

Example 14.5.2. The transition diagram of the monoids $[\mathbb{Z}_2, \times_2]$ and $[\mathbb{Z}_3, \times_3]$ appear in Figure 14.5.2.

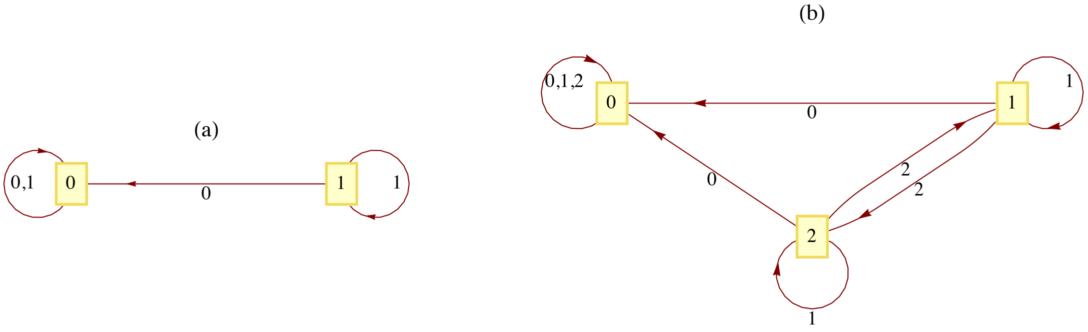


Figure 14.5.2

Example 14.5.3. Let U be the monoid that we obtained from the unit-time delay machine (Example 14.4.3). We have seen that the machine of the monoid of the parity checker is essentially the parity checker. Will we obtain a unit-time delay machine when we construct the machine of U? We can't expect to get exactly the same machine because the unit-time delay machine is not a state machine and the machine of a monoid is a state machine. However, we will see that our new machine is capable of telling us what input was received in the previous time period. The operation table for the monoid serves as a table to define the transition function for the machine. The row headings are the state values, while the column headings are the inputs. If we were to draw a transition diagram with all possible inputs, the diagram would be too difficult to read. Since U is generated by the two elements, T_0 and T_1, we will include only those inputs. Suppose that we wanted to read the transition function for the input T_{01}. Since $T_{01} = T_0 T_1$, in any state s, $t(s, T_{01}) = t(t(s, T_0), T_1)$. The transition diagram appears in Figure 14.5.3.

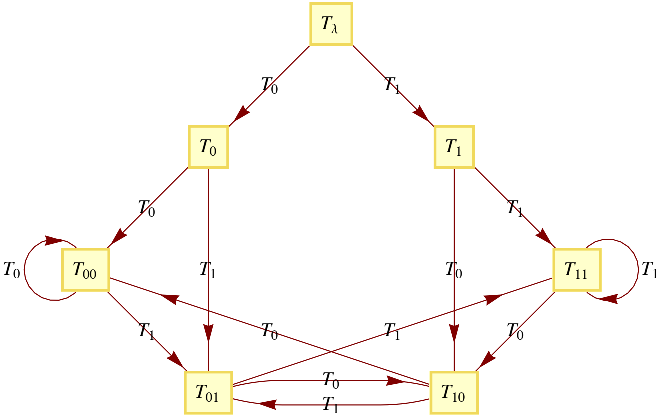


Figure 14.5.3

If we start reading a string of 0s and 1s while in state T_λ and are in state T_{ab} at any one time, the input from the previous time period (not the input that sent us into T_{ab}, the one before that) is a. In states T_λ, T_0 and T_1, no previous input exists.

EXERCISES FOR SECTION 14.5

A Exercise

1. Draw the transition diagrams for the machines of the following monoids:

(a) $[\mathbb{Z}_4; +_4]$

(b) The direct product of $[\mathbb{Z}_2; \times_2]$ with itself.

B Exercise

2. Even though a monoid may be infinite, we can visualize it as an infinite-state machine provided that it is generated by a finite number of elements. For example, the monoid B^* is generated by 0 and 1. A section of its transition diagram can be obtained by allowing input only from the generating set (Figure 14.5.4a). The monoid of integers under addition is generated by the set {-1, 1}. The transition diagram for this monoid can be visualized by drawing a small portion of it, as in Figure 14.5.4b.

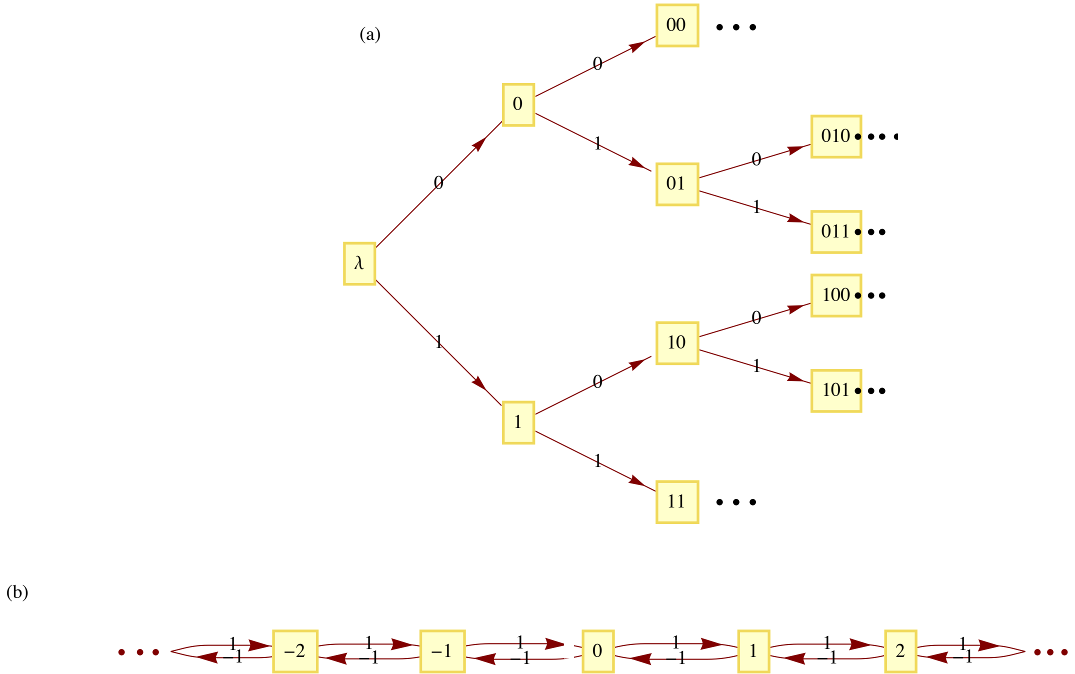


Figure 14.5.4

(a) Draw a transition diagram for $\{a, b, c\}^*$.

(b) Draw a transition diagram for $[\mathbb{Z} \times \mathbb{Z}$, componentwise addition$]$.

SUPPLEMENTARY EXERCISES FOR CHAPTER 14

Section 14,1

1. Let B be a Boolean algebra and M the set of all Boolean functions on B. Let $*$ be defined on M by $(f * g)(a) = f(a) \wedge g(a)$. Prove that $[M, *]$ is a monoid. Construct the operation table of $[M, *]$ for the case of $B = B_2$.

2. A semigroup is an algebraic system $[S, *]$ with the only axiom that $*$ be associative on S. Prove that if S is a finite set, then there must exist an idempotent element, that is, an $a \in S$ such that $a * a = a$.

Section 14.2

3. What language does the following grammar define? The start symbol is S, the terminal symbols are a and b, and the nonterminal symbols are S and B. The production rules are $S \to a, S \to b B, B \to b,\ B \to b S$.

4. What language does the following grammar define? Start symbol = S. nonterminal symbols: T, R. Production rules: $S \to T$, $S \to R$, $T \to b R, R \to a T, T \to b, R \to a$.

5. Write a regular grammar for the language L over the alphabet $\{a, b\}$ where L is the set of all strings with exactly two b's.

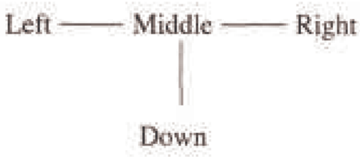
6. Write a regular grammar to describe the strings of 0's and 1's that consist of a positive number of 0's surrounded by single 1's. For example, 100001 is one such string.

Section 14.3

7. Draw a finite-state machine to recognize the language in Exercise 5. Have the last output be 1 if the input word is in L, and 0 it is not in L.

8. Draw a transition diagram for a finite-state machine that recognizes strings in the language of Exercise 6.

9. A finite-state machine moves once every time unit between one of four states called Right, Middle, Left, and Down. The input alphabet is $X = \{00, 01, 10, 11\}$ and the output alphabet is $Y = \{1, 0\}$.



(i) If the machine is in the Middle, Right, or Left, 00 means that it stays where it is; 01 means that it moves one state to the right (e.g. Left to Middle.)—if it can't move any farther to the right, it stays where it is;

10 means that it moves one state to the left.

(ii) Input of 11 means that the machine stays where it is except if it is in the Middle, in which case it enters the Down state.

(iii) If the machine is in the Down state, it stays in that state forever.

(iv) Output is 1 if the state of the machine changes, 0 otherwise.

(a) Construct the transition diagram for this finite-state machine.

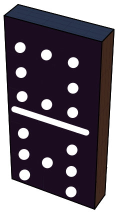
(b) If $s(0) = $ Middle and $s(3) = $ Down, list the possible output sequences that could have occurred for $t = 0, 1, 2$.

Section 14.4

10. Write out the operation table for the monoid of the machine in Exercise 9. Section 14.5

11. Draw the transition diagram of the machine of $[M, *]$ in Exercise 1 of these supplementary exercises.

Chapter 15



GROUP THEORY AND APPLICATIONS

Abelian Group

In Abelian groups, when computing,
With operands there's no refuting:
The expression bc
Is the same as cb.
Not en route to your job, yet commuting.

- limerick by Howard Spindel in *The Omnificent English Dictionary In Limerick Form*

GOALS

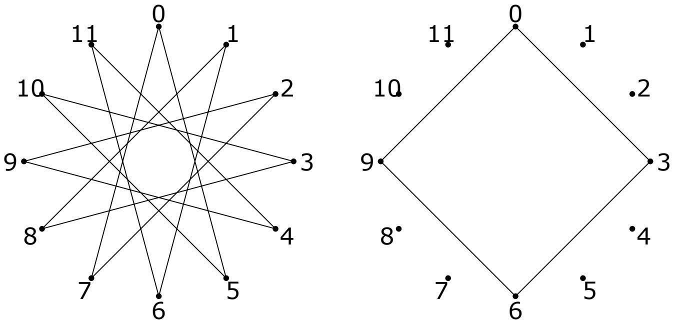
In Chapter 11, groups were introduced as a typical algebraic system. The associated concepts of subgroup, group isomorphism, and direct products of groups were also introduced. Groups were chosen for that chapter because they are among the simplest types of algebraic systems. Despite this simplicity, group theory abounds with interesting applications, many of which are of interest to the computer scientist. In this chapter we will introduce some more important concepts in elementary group theory, and some of their applications.

15.1 Cyclic Groups

Groups are classified according to their size and structure. A group's structure is revealed by a study of its subgroups and other properties (e.g., whether it is abelian) that might give an overview of it. Cyclic groups have the simplest structure of all groups.

Definitions: Cyclic Group, Generator. *Group G is cyclic if there exists $a \in G$ such that the cyclic subgroup generated by a, (a), equals all of G. That is, $G = \{n a \mid n \in \mathbb{Z}\}$, in which case a is called a generator of G. The reader should note that additive notation is used for G.*

Example 15.1.1. $\mathbb{Z}_{12} = [\mathbb{Z}_{12}, +_{12}]$, where $+_{12}$ is addition modulo 12, is a cyclic group. To verify this statement, all we need to do is demonstrate that some element of $\mathbb{Z}_{12}$ is a generator. One such element is 5; that is, $(5) = \mathbb{Z}_{12}$. One more obvious generator is 1. In fact, 1 is a generator of every $[\mathbb{Z}_n; +_n]$. The reader is asked to prove that if an element is a generator, then its inverse is also a generator. Thus, -5 = 7 and -1 = 11 are the other generators of $\mathbb{Z}_{12}$.



(a) (b)

Figure 15.1.1
Examples of "string art"

Figure 15.1.1(a) is an example of "string art" that illustrates how 5 generates $\mathbb{Z}_{12}$. Twelve tacks are placed along a circle and numbered. A string is tied to tack 0, and is then looped around every fifth tack. As a result, the numbers of the tacks that are reached are exactly the ordered multiples of 5 modulo 12: 5, 10, 3, ... , 7, 0. Note that if every seventh tack were used, the same artwork would be obtained. If every third tack were connected, as in Figure 15.1.1(b), the resulting loop would only use four tacks; thus 3 does not generate $\mathbb{Z}_{12}$.

Example 15.1.2. The group of additive integers, $[\mathbb{Z}; +]$, is cyclic:

$$\mathbb{Z} = (1) = \{n \cdot 1 \mid n \in \mathbb{Z}\}.$$

This observation does not mean that every integer is the product of an integer times 1. It means that

$$\mathbb{Z} = \{0\} \cup \left\{1 + \overbrace{1 + \cdots}^{n\text{ terms}} + 1 \mid n \in \mathbb{P}\right\} \cup \left\{(-1) + \overbrace{(-1) + \cdots}^{n\text{ terms}} + (-1) \mid n \in \mathbb{P}\right\}$$

Theorem 15.1.1. *If $[G *]$ is cyclic, then it is abelian.*

Proof: Let a be any generator of G and let $b, c \in G$. By the definition of the generator of a group, there exists integers m and n such that $b = m a$ and $c = n a$. Thus

$$\begin{aligned} b * c &= (m a) * (n a) \\ &= (m + n) a \quad \text{by Theorem 11.3.7(ii)} \\ &= (n + m) a \\ &= (n a) * (n b) \\ &= c * b \quad \blacksquare \end{aligned}$$

One of the first steps in proving a property of cyclic groups is to use the fact that there exists a generator. Then every element of the group can be expressed as some multiple of the generator. Take special note of how this is used in theorems of this section.

Up to now we have used only additive notation to discuss cyclic groups. Theorem 15.1.1 actually justifies this practice since it is customary to use additive notation when discussing abelian groups. Of course, some concrete groups for which we employ multiplicative notation are cyclic. If one of its elements, a, is a generator,

$$(a) = \{a^n \mid n \in \mathbb{Z}\}$$

Example 15.1.3. The group of positive integers modulo 11 with modulo 11 multiplication, $[\mathbb{Z}_{11}{}^*; \times_{11}]$, is cyclic. One of its generators is 6: $6^1 = 6, 6^2 = 3, 6^3 = 7, \ldots, 6^9 = 2$, and $6^{10} = 1$, the identity of the group.

Example 15.1.4. The real numbers with addition, $[\mathbb{R}; +]$ is a noncyclic group. The proof of this statement requires a bit more generality since we are saying that for all $r \in \mathbb{R}$, (r) is a proper subset of $\mathbb{R}$. If r is nonzero, the multiples of r are distributed over the real line, as in Figure 15.1.2. It is clear then that there are many real numbers, like $r/2$, that are not in (r).

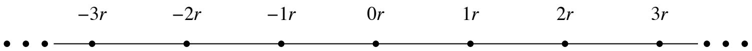


Figure 15.1.2
Elements of (r), $r > 0$

The following theorem shows that a cyclic group can never be very complicated.

Theorem 15.1.2. *If G is a cyclic group, then G is either finite or countably infinite. If G is finite and $|G| = n$, it is isomorphic to $[\mathbb{Z}_n, +_n]$. If G is infinite, it is isomorphic to $[\mathbb{Z}, +]$.*

Proof: Case 1: $|G| < \infty$. If a is a generator of G and $|G| = n$, define $\phi : \mathbb{Z}_n \to G$ by

$$\phi(k) = k\,a \quad \text{for all } k \in \mathbb{Z}_n$$

Since (a) is finite, we can use the fact that the elements of (a) are the first n nonnegative multiples of a. From this observation, we see that ϕ is a surjection. A surjection between finite sets of the same cardinality must be a bijection. Finally, if $p, q \in \mathbb{Z}_n$,

$$\begin{aligned} \phi(p) + \phi(q) &= p\,a + q\,a \\ &= (p + q)\,a \\ &= (p +_n q)\,a \quad \text{see exercise 10} \\ &= \phi(p +_n q) \end{aligned}$$

Therefore ϕ is an isomorphism.

Case 2; $|G| = \infty$. We will leave this case as an exercise. ■

The proof of the next theorem makes use of the division property for integers, which was introduced in Section 11.4: If m, n are integers, $m > 0$, there exist unique integers q (quotient) and r (remainder) such that $n = \text{qm} + r$ and $0 \leq r < m$.

Theorem 15.1.3. *Every subgroup of a cyclic group is cyclic.*

Proof: Let G be cyclic with generator a and let $H \leq G$. If $H = \{e\}$, H has e as a generator. We may now assume that $|H| \geq 2$ and $a \neq e$. Let m be the least positive integer such that $m\,a$ belongs to H. (This is the key step. It lets us get our hands on a generator of H.) We will now show that $c = m\,a$ generates H. Suppose that $(c) \neq H$. Then there exists $b \in H$ such that $b \notin (c)$. Now, since b is in G, there exists $n \in \mathbb{Z}$ such that $b = n\,a$. We now apply the division property and divide n by m.

$$b = n\,a = (q\,m + r)\,a = (q\,m)\,a + r\,a,$$

where $0 \leq r < m$. We note that r cannot be zero for otherwise we would have $b = n\,a = q(m\,a) = q\,c \in (c)$. Therefore,

$$r\,a = n\,a - (q\,m)\,a \in H$$

This contradicts our choice of m because $0 < r < m$. ■

Example 15.1.5. The only proper subgroups of $\mathbb{Z}_{10}$ are $H_1 = \{0, 5\}$ and $H_2 = \{0, 2, 4, 6, 8\}$. They are both cyclic: $H_1 = (5)$, while $H_2 = (2) = (4) = (6) = (8)$. The generators of $\mathbb{Z}_{10}$ are 1, 3, 7, and 9.

Example 15.1.6. With the exception of $\{0\}$, all subgroups of $\mathbb{Z}$ are isomorphic to $\mathbb{Z}$. If $H \leq \mathbb{Z}$, then H is the cyclic subgroup generated by the least positive element of H. It is infinite and so by theorem 15.1.2 it is isomorphic to $\mathbb{Z}$.

We now cite a useful theorem for computing the order of cyclic subgroups of a cyclic group:

Theorem 15.1.4. *If G is a cyclic group of order n and a is a generator of G, the order of $k\,a$ is n/d, where d is the greatest common divisor of n and k.*

The proof of this theorem is left to the reader.

Example 15.1.7. To compute the order of (18) in $\mathbb{Z}_{30}$, we first observe that 1 is a generator of $\mathbb{Z}_{30}$ and 18 = 18(1). The greatest common divisor of 18 and 30 is 6. Hence, the order of (18) is 30/6, or 5.

APPLICATION: FAST ADDERS

At this point, we will introduce the idea of a fast adder, a relatively modern application (Winograd, 1965) to an ancient theorem, the Chinese Remainder Theorem. We will present only an overview of the theory and rely primarily on examples. The interested reader can refer to Dornhoff and Hohn for details.

Out of necessity, integer addition with a computer is addition modulo n, for n some larger number. Consider the case where n is small, like 64. Then addition involves the addition of six-digit binary numbers. Consider the process of adding 31 and 1. Assume the computer's adder takes as input two bit strings $a = \{a_0, a_1, a_2, a_3, a_4, a_5\}$ and $b = \{b_0, b_1, b_2, b_3, b_4, b_5\}$ and outputs $s = \{s_0, s_1, s_2, s_3, s_4, s_5\}$, the sum of a and b. Then, if $a = 31 = (1, 1, 1, 1, 1, 0)$ and $b = 1 = (1, 0, 0, 0, 0, 0)$, s will be $(0, 0, 0, 0, 0, 1)$, or 32. The output $s_5 = 1$ cannot be determined until all other outputs have been determined. If addition is done with a finite-state machine, as in Example 14.3.5, the time required to obtain s will be six time units, where one time unit is the time it takes to get one output from the machine. In general, the time required to obtain s will be proportional to the number of bits Theoretically, this time can be decreased, but the explanation would require a long digression and our relative results would not change that much. We will use the rule that the number of time units needed to perform addition modulo

n is proportional to $\lceil \log_2 n \rceil$.

Now we will introduce a hypothetical problem that we will use to illustrate the idea of a fast adder. Suppose that we had to add many numbers modulo $27\,720 = 8 \cdot 9 \cdot 5 \cdot 7 \cdot 11$. By the rule above, since $2^{14} < 27\,720 < 2^{15}$, each addition would take 15 time units. If the sum is initialized to zero, 1,000 additions would be needed; thus, 15,000 time units would be needed to do the additions. We can improve this time dramatically by applying the Chinese Remainder Theorem.

The Chinese Remainder Theorem (CRT). *Let $n_1, n_2, \ldots, n_p$ be integers that have no common factor greater than one between any pair of them; i. e., they are relatively prime. Let $n = n_1 n_2 \cdots n_p$. Define*

$$\theta : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_p}$$

by

$$\theta(k) = (k_1, k_2, \ldots, k_p)$$

where for $1 \leq i \leq p$, $0 \leq k_i < n_i$ and $k \equiv k_i (\mathrm{mod}\, n_i)$. Then θ is an isomorphism from $\mathbb{Z}_n$ into $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_p}$.

This theorem can be stated in several different forms, and its proof can be found in many abstract algebra texts.

Example 15.1.8. As we saw in Chapter 11, $\mathbb{Z}_6$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$. This is the smallest case to which the CRT can be applied. An isomorphism between $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$ is

$\theta(0) = (0, 0)$ $\quad$ $\theta(3) = (1, 0)$

$\theta(1) = (1, 1)$ $\quad$ $\theta(4) = (0, 1)$

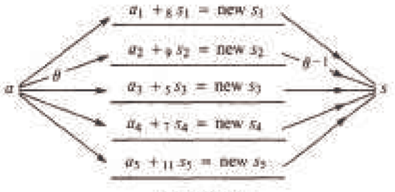
$\theta(2) = (0, 2)$ $\quad$ $\theta(5) = (1, 2)$

Let's consider a somewhat larger case. We start by selecting a modulus that can be factored into a produce to relatively prime integers.

```
n = 2^5 3^3 5^2
```

```
21 600
```

In this case the factors are $2^5 = 32$, $3^3 = 27$, and $5^2 = 25$. They need not be powers of primes, but it is easy to break the factors into this form to assure relatively prime numbers. To add in $\mathbb{Z}_n$, we need $\lceil \log_2 n \rceil = 15$ time units. Let $G = \mathbb{Z}_{32} \times \mathbb{Z}_{27} \times \mathbb{Z}_{25}$. The CRT gives us an isomorphism between $\mathbb{Z}_{21\,600}$ and G. The basic idea behind the fast adder, illustrated in Figure 15.1.3, is to make use of this isomorphism.



a
θ
$a_1 +_8 s_1 = \text{new } s_1$
$a_2 +_9 s_2 = \text{new } s_2$
$a_3 +_5 s_3 = \text{new } s_3$
$a_4 +_7 s_4 = \text{new } s_4$
$a_5 +_{11} s_5 = \text{new } s_5$
θ^{-1}
s

FIGURE 15.1.3

Assume we have several integers $a_1, \ldots, a_m$ to be added. Here, we assume $m = 20$.

```
a = {1878, 1384, 84, 2021, 784, 1509, 1740, 1201,
   2363, 1774, 1865, 33, 1477, 894, 690, 520, 198, 1349, 1278, 650};
```

After each of the s_i's is initialized to zero, each summand t is decomposed into a triple $\theta(t) = (t_1, t_2, t_3) \in G$. For our example we first define θ as a *Mathematica* function and then map it over the list of summands.

```
θ[n_] := {Mod[n, 32], Mod[n, 27], Mod[n, 25]}
```

```
distributedSummands = Map[θ, a]
```

$$\begin{pmatrix} 22 & 15 & 3 \\ 8 & 7 & 9 \\ 20 & 3 & 9 \\ 5 & 23 & 21 \\ 16 & 1 & 9 \\ 5 & 24 & 9 \\ 12 & 12 & 15 \\ 17 & 13 & 1 \\ 27 & 14 & 13 \\ 14 & 19 & 24 \\ 9 & 2 & 15 \\ 1 & 6 & 8 \\ 5 & 19 & 2 \\ 30 & 3 & 19 \\ 18 & 15 & 15 \\ 8 & 7 & 20 \\ 6 & 9 & 23 \\ 5 & 26 & 24 \\ 30 & 9 & 3 \\ 10 & 2 & 0 \end{pmatrix}$$

Addition in G can be done in parallel so that each new subtotal in the form of the triple (s_1, s_2, s_3) takes only as long to compute as it takes to add in the largest modulus, $\log_2 32 = 5$ time units, if calculations are done in parallel. By the time rule that we have established, the addition of 20 numbers can be done in $20 \times 5 = 100$ time units, as opposed to $15 \times 20 = 300$ time units if we do the calculations in $\mathbb{Z}_n$.

The result of adding the distributed summands in the three different moduli for our example would be the following.

```
distributedSum =
 Fold[{Mod[#1[[1]] + #2[[1]], 32], Mod[#1[[2]] + #2[[2]], 27], Mod[#1[[3]] + #2[[3]], 25]} &,
  {0, 0, 0}, distributedSummands]
```

```
{12, 13, 17}
```

Two more factors must still be considered, however. How easy is it to determine $\theta(a)$ and $\theta^{-1}(s_1, s_2, s_3)$? We must compute $\theta(a)$ twenty times, and, if it requires a sizable amount of time, there may not be any advantage to the fast adder. The computation of an inverse is not as time-critical since it must be done only once, after the final sums are determined in G.

The determination of $\theta(a)$ is not a major problem. If the values of $\theta(1)$, $\theta(10)$, $\theta(100)$, $\theta(1000)$, and $\theta(10\,000)$ are stored, $a = d_0 + 10\, d_1 + 100\, d_2 + 1000\, d_3 + 10\,000\, d_4$, then

$$\theta(a) = d_0\, \theta(1) + d_1\, \theta(10) + d_2\, \theta(100) + d_3\, \theta(1000) + d_4\, \theta(10\,000)$$

by the fact that θ is an isomorphism. The components of $\theta(a)$ can be computed economically using this formula so as not to slow down the actual adding process.

The computation of $\theta^{-1}(s_1, s_2, s_3)$ is simplified by the fact that θ^{-1} is also an isomorphism. The final sum is $s_1\, \theta^{-1}(1, 0, 0) + s_2\, \theta^{-1}(0, 1, 0) + s_3\, \theta^{-1}(0, 0, 1)$. The arithmetic in this expression is in $\mathbb{Z}_{21\,600}$ and is more time consuming. However, as was noted above, it need only be done once. This is why the fast adder is only practical in situations where many additions must be performed to get a single sum.

For our example, we can use Mathematica's built-in function for inverting θ:

```
ChineseRemainder[distributedSum, {32, 27, 25}]
```

```
2092
```

The result we get is exactly what we get by directly adding in the larger modulus.

```
Fold[Mod[#1 + #2, 32 × 27 × 25] &, 0, a]
```

```
2092
```

Notice that if we wanted the conventional sum of integers our list, the result we just arrived at would not be correct. The relationship between the integer sum and the modular sum is that they differ by a multiple of the modulus:

```
Total[a]

23 692

Mod[Total[a] - Fold[Mod[#1 + #2, 32 × 27 × 25] &, 0, a], 32 × 27 × 25]

0
```

To further illustrate the potential of fast adders, consider the problem of addition modulo

$$n = 2^5\, 3^3\, 5^2\, 7^2\, 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \approx 3.1 \times 10^{21}$$

Each addition using the usual modulo n addition with full adders would take 72 time units. By decomposing each summand into 15-tuples according to the CRT, the time is reduced to $\lceil \log_2 49 \rceil = 6$ time units per addition.

EXERCISES FOR SECTION 15.1

A Exercises

1. What generators besides 1 does $[\mathbb{Z}, +]$ have?

2. Without doing any multiplications, determine the number of generators of $[\mathbb{Z}_{11}, +_{11}]$.

3. Prove that if $|G| > 2$ and G is cyclic, G has at least two generators.

4. If you wanted to list the generators of $\mathbb{Z}_n$ you would only have to test the first $n/2$ positive integers. Why?

5. Which of the following groups are cyclic? Explain.

   (a) $[\mathbb{Q}, +]$

   (b) $[\mathbb{R}^+, \cdot]$

   (c) $[6\mathbb{Z}, +]$ where $6\mathbb{Z} = \{6n \mid n \in \mathbb{Z}\}$

   (d) $\mathbb{Z} \times \mathbb{Z}$

   (e) $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$

6. For each group and element, determine the order of the cyclic subgroup generated by the element:

   (a) $\mathbb{Z}_{25}$, 15

   (b) $\mathbb{Z}_4 \times \mathbb{Z}_9$, $(2, 6)$ (apply Exercise 8)

   (c) $\mathbb{Z}_{64}$, 2

B Exercises

7. How can Theorem 15.1.4 be applied to list the generators of $\mathbb{Z}_n$? What are the generators of $\mathbb{Z}_{25}$? Of $\mathbb{Z}_{256}$?

8. Prove that if the greatest common divisor of n and m is 1, then $(1, 1)$ is a generator of $\mathbb{Z}_n \times \mathbb{Z}_m$, and, hence, $\mathbb{Z}_n \times \mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_{n\,m}$.

9. (a) Illustrate how the fast adder can be used to add the numbers 21, 5, 7, and 15 using the isomorphism between $\mathbb{Z}_{77}$ and $\mathbb{Z}_7 \times \mathbb{Z}_{11}$.

   (b) If the same isomorphism is used to add the numbers 25, 26, and 40, what would the result be, why would it be incorrect, and how would the answer differ from the answer in part a?

10. Prove that if G is a cyclic group of order n with generator a, and $p, q \in \{0, 1, \ldots, n-1\}$, then

$$(p + q)\,a = (p +_n q)\,a$$

15.2 Cosets and Factor Groups

Consider the group $[\mathbb{Z}_{12}, +_{12}]$. As we saw in the previous section, we can picture its cyclic properties with the string art of Figure 15.1.1. Here we will be interested in the non-generators, like 3. The solid lines in Figure 15.2.1 show that only one-third of the tacks have been reached by starting at zero and jumping to every third tack. The numbers of these tacks correspond to $(3) = \{0, 3, 6, 9\}$.

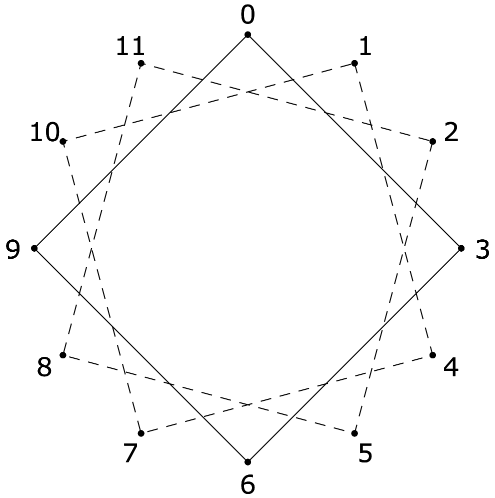


Figure 15.2.1

What happens if you start at one of the unused tacks and again jump to every third tack? The two broken paths on Figure 15.2.1 show that identical squares are produced. The tacks are thus partitioned into very similar subsets. The subsets of $\mathbb{Z}_{12}$ that they correspond to are {0, 3, 6, 9}, {1, 4, 7, 10}, and {2, 5, 8, 11}.These subsets are called *cosets*. In particular, they are called cosets of the subgroup {0, 3, 6, 9}. We will see that under certain conditions, cosets of a subgroup can form a group of their own. Before pursuing this example any further we will examine the general situation.

Definition: Coset. *If* $[G, *]$ *is a group,* $H \leq G$ *and* $a \in G$*, the left coset of H generated by a is*

$$a*H = \{a*h \mid h \in H\}.$$

The right coset of H generated by a is

$$H*a = \{h*a \mid h \in H\}.$$

Notes:

(a) H itself is both a left and right coset since $e*H = H*e = H$.

(b) If G is abelian, $a*H = H*a$ and the left-right distinction for cosets can be dropped. We will normally use left coset notation in that situation.

Definition: Coset Representative. *Any element of a coset is called a representative of that coset.*

One might wonder whether a is in any way a special representative of $a*H$ since it seems to define the coset. It is not, as we shall see.

Theorem 15.2.1. *If* $b \in a*H$*, then* $a*H = b*H$*, and if* $b \in H*a$*, then* $H*a = H*b$.

Remark: A Duality Principle. A duality principle can be formulated concerning cosets because left and right cosets are defined in such similar ways. Any theorem about left and right cosets will yield a second theorem when "left" and "right" are exchanged for "right" and "left."

Proof of Theorem 15.2.1: In light of the remark above, we need only prove the first part of this theorem. Suppose that $x \in a*H$. We need only find a way of expressing x as "b times an element of H." Then we will have proven that $a*H \subseteq b*H$. By the definition of $a*H$, since b and x are in $a*H$, there exist h_1 and h_2 in H such that $b = a*h_1$ and $x = a*h_2$. Given these two equations, $a = b h_1^{-1}$ and

$$x = a*h_2 = \left(b*h_1^{-1}\right)*h_2 = b*\left(h_1^{-1}*h_2\right).$$

Since $h_1, h_2 \in H,\ h_1^{-1}*h_2 \in H$, and we are done with this part of the proof. In order to show that $b*H\, C\, a*H$, one can follow essentially the same steps, which we will let the reader fill in. ■

Example 15.2.1. In Figure 15.2.1, you can start at either 1 or 7 and obtain the same path by taking jumps of three tacks in each step. Thus,

$$1 +_{12} \{0, 3, 6, 9\} = 7 +_{12} \{0, 3, 6, 9\} = \{1, 4, 7, 10\}.$$

The set of left (or right) cosets of a subgroup partition a group in a special way:

Theorem 15.2.2. *If* $[G, *]$ *is a group and* $H \leq G$*, the set of left cosets of H is a partition of G. In addition, all of the left cosets of H have the same cardinality. The same is true for right cosets.*

Proof: That every element of G belongs to a left coset is clear because $a \in a*H$ for all $a \in G$. If $a*H$ and $b*H$ are left cosets, they are either equal or disjoint. If two left cosets $a*H$ and $b*H$ are not disjoint, $a*H \cap b*H$ is nonempty and some element c belongs to the intersection. Then by Theorem 15.2.1,

$$c \in a*H \Rightarrow a*H = c*H \text{ and}$$

$$c \in b*H \Rightarrow b*H = c*H.$$

Hence $a*H = b*H$.

We complete the proof by showing that each left coset has the same cardinality as H. To do this, we simply observe that if $a \in G$, $\rho : H \to a*H$ defined by $\rho(h) = a*h$ is a bijection and hence $|H| = |a*H|$. We will leave the proof of this statement to the reader. ■

The function ρ has a nice interpretation in terms of our opening example. If $a \in \mathbb{Z}_n$, the graph of $\{0, 3, 6, 9\}$ is rotated $30\,a°$ to coincide with one of the three cosets of $\{0, 3, 6, 9\}$.

A Counting Formula. *If $|G| < \infty$ and $H \leq G$, the number of distinct left cosets of H equals $\frac{|G|}{|H|}$. For this reason we use G/H to denote the set of left cosets of H in G.*

Example 15.2.2. The set of integer multiples of four, $4\mathbb{Z}$, is a subgroup of $[\mathbb{Z}, +]$. Four distinct cosets of $4\mathbb{Z}$ partition the integers. They are $4\mathbb{Z}$, $1+4\mathbb{Z}$, $2+4\mathbb{Z}$, and $3+4\mathbb{Z}$, where, for example, $1+4\mathbb{Z} = \{1+4k \mid k \in \mathbb{Z}\}$. $4\mathbb{Z}$ can also be written $0+4\mathbb{Z}$.

Distinguished Representatives. Although we have seen that any representative can describe a coset, it is often convenient to select a distinguished representative from each coset. The advantage to doing this is that there is a unique name for each coset in terms of its distinguished representative. In numeric examples such as the one above, the distinguished representative is usually the smallest nonnegative representative. Remember, this is purely a convenience and there is absolutely nothing wrong in writing $-203+4\mathbb{Z}$, $5+4\mathbb{Z}$, or $621+4\mathbb{Z}$ in place of $1+4\mathbb{Z}$ because $-203, 5, 621 \in 1+4\mathbb{Z}$.

Before completing the main thrust of this section, we will make note of a significant implication of Theorem 15.2.2. Since a finite group is divided into cosets of a common size by any subgroup, we can conclude:

Lagrange's Theorem. *The order of a subgroup of a finite group must divide the order of the group.*

One immediate implication of Lagrange's Theorem is that if p is prime, $\mathbb{Z}_p$ has no proper subgroups.

We will now describe the operation on cosets which will, under certain circumstances, result in a group. For most of this section, we will assume that G is an abelian group. This is one condition that guarantees that the set of left cosets will form a group.

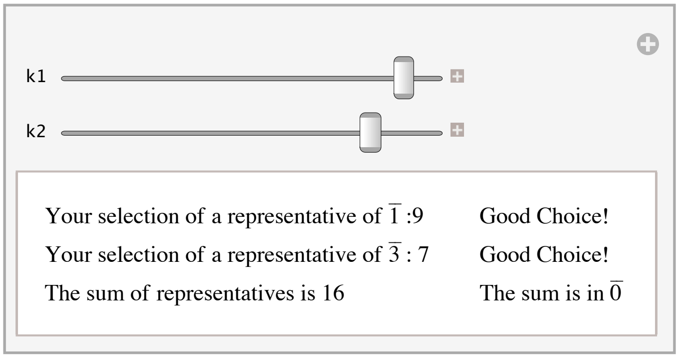
Definition: Operation on Cosets. *Let C and D be left cosets of H, a subgroup of G with representatives c and d, respectively. Then*

$$C \otimes D = c*H \otimes d*H = (c*d)*H$$

The operation $\otimes$ is called the operation induced on left cosets by $*$.

In Theorem 15.2.3, later in this section, we prove that if G is an abelian group, $\otimes$ is indeed an operation. In practice, if the group G is an additive group, the symbol $\otimes$ is replaced by $+$, as in the following example.

Example 15.2.3. Consider the cosets described in Example 15.2.2. For brevity, we rename $0+4\mathbb{Z}$, $1+4\mathbb{Z}$, $2+4\mathbb{Z}$, and $3+4\mathbb{Z}$ with the symbols $\overline{0}$, $\overline{1}$, $\overline{2}$, and $\overline{3}$. Let's do a typical calculation, $\overline{1}+\overline{3}$. We will see that the result is always going to be $\overline{0}$, no matter what representatives we select. For example, $9 \in \overline{1}$, $7 \in \overline{3}$, and $9+7=16 \in \overline{0}$. Our choice of the representatives $\overline{1}$ and $\overline{3}$ were completely arbitrary. If you are reading this as a *Mathematica* Notebook, you can try out this demonstration that lets you select representatives of the two cosets by moving the sliders and see how the result is consistent.



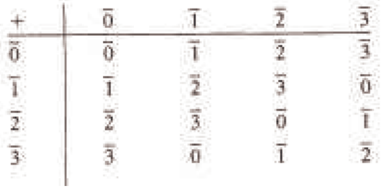
Your selection of a representative of $\overline{1}$:9 Good Choice!

Your selection of a representative of $\overline{3}$: 7 Good Choice!

The sum of representatives is 16 The sum is in $\overline{0}$

Since $C \otimes D$ (or $\overline{1}+\overline{3}$ in this case) can be computed in many ways, it is necessary to show that the choice of representatives does not affect the result. When the result we get for $C \otimes D$ is always independent of our choice of representatives, we say that "$\otimes$ is well defined." Addition of cosets is a well-defined operation on the left cosets of $4\mathbb{Z}$ and is summarized in Table 15.2.1. Do you notice anything familiar?

TABLE 15.2.1
Coset Operation—Table of Example 15.2.3



$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Example 15.2.4. Consider the real numbers. $[\mathbb{R}; +]$, and its subgroup of integers, $\mathbb{Z}$. Every element of $\mathbb{R}/\mathbb{Z}$ has the same cardinality as $\mathbb{Z}$. Let $s, t \in \mathbb{R}$. $s \in t + \mathbb{Z}$ if s can be written $t + n$ for some $n \in \mathbb{Z}$. Hence s and t belong to the same coset if they differ by an integer. (See Exercise 6 for a generalization of this fact.)

Now consider the coset $0.25 + \mathbb{Z}$. Real numbers that differ by an integer from 0.25 are 1.25, 2.25, 3.25, ... and -0.75, -1.75, -2.75… . If any real number is selected, there exists a representative of its coset that is greater than or equal to 0 and less than 1. We will call that representative the distinguished representative of the coset. For example, 43.125 belongs to the coset represented by 0.125; $-6.382 + \mathbb{Z}$ has 0.618 as its distinguished representative. The operation on $\mathrm{R}/\mathbb{Z}$ is commonly called addition modulo 1. A few typical calculations in $\mathbb{R}/\mathbb{Z}$ are

$$(0.1 + \mathbb{Z}) + (0.48 + \mathbb{Z}) = 0.58 + \mathbb{Z}\ ,$$

$$(0.7 + \mathbb{Z}) + (0.31 + \mathbb{Z}) = 0.01 + \mathbb{Z},$$

and $\quad -(0.41 + \mathbb{Z}) = -0.41 + \mathbb{Z} = 0.59 + \mathbb{Z}.$

In general, $-(a + \mathbb{Z}) = (1 - a) + \mathbb{Z}$.

Example 15.2.5. Consider $F = (\mathbb{Z}_4 \times \mathbb{Z}_2)/H$, where $H = \{(0, 0), (0, 1)\}$. Since $\mathbb{Z}_4 \times \mathbb{Z}_2$ is of order 8, each element of F is a coset containing two ordered pairs. We will leave it to the reader to verify that the four distinct cosets are

$$(0,\ 0) + H,\ (1, 0)\ + H, (2,\ 0) + H, \text{and } (3,\ 0) + H.$$

The reader can also verify that F is isomorphic to $\mathbb{Z}_4$, since F is cyclic. An educated guess should give you a generator.

Example 15.2.6. Consider the group $\mathbb{Z}_2{}^4 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Let H be $\langle(1, 0, 1,\ 0)\rangle$, the cyclic subgroup of $\mathbb{Z}_2{}^4$ generate by (1,0,1,0). Since

$$(1, 0, 1,\ 0) + (1, 0, 1,\ 0) = (1 +_2 1, 0 +_2 0, 1 +_2 1, 0 +_2 0) = (0, 0, 0, 0)$$

The order of H is 2 and , $\mathbb{Z}_2{}^4/H$ has $|\mathbb{Z}_2^4/H| = \frac{|\mathbb{Z}_2^4|}{|H|} = \frac{16}{2} = 8$ elements. A typical coset is

$$C = (0,\ 1,\ 1,\ 1) + H = \{(0,\ 1,\ 1,\ 1),\ (1,\ 1,\ 0,\ 1)\}.$$

Since $2(0,\ 1,\ 1,\ 1) = (0,\ 0,\ 0,\ 0), 2C = H$, the identity for the operation $\mathbb{Z}_2{}^4/H$. The orders of all non-identity elements of $\mathbb{Z}_2{}^4/H$ are all 2, and it can be shown that the factor group is isomorphic to $\mathbb{Z}_2{}^3$.

Theorem 15.2.3. *If G is an abelian group, and $H \leq G$, the operation induced on cosets of H by the operation of G is well defined.*

Proof: Suppose that a, b, and a', b' are two choices for representatives of cosets C and D. That is to say that $a,\ a' \in C, b,\ b' \in D$. We will show that $a*b$ and $a'*b'$ are representatives of the same coset. Theorem 15.2.1 implies that $C = a*H$ and $D = b*H$, thus we have

$$a' \in a*H \text{ and } b' \in b*H.$$

Then there exists $h_1,\ h_2 \in H$ such that $a' = a*h_1$ and $b' = b*h_2$ and so

$$\begin{aligned} a'*b' &= (a*h_1)*(b*h_2) \\ &= (a*b)*(h_1*h_2) \end{aligned}$$

by various group properties and the assumption that H is abelian, which lets us reverse the order in which b and $h_1$appear. This last expression for $a'*b$' implies that $a'*b' \in (a*b)*H$ since $h_1*h_2 \in H$ because H is as subgroup of G. ■

Theorem 15.2.4. *Let G be a group and $H \leq G$. If the operation induced on left cosets of H by the operation of G is well defined, then the set of left cosets forms a group under that operation.*

Proof: Let C_1, C_2, and C_3 be the left cosets with representatives r_1, r_2, and r_3, respectively. The values of $C_1 \otimes (C_2 \otimes C_3)$ and $(C_1 \otimes C_2\ ) \otimes C_3$ are determined by $r_1 * (r_2 * r_3)$ and $(r_1 * r_2\ ) * r_3$. By the associativity of $*$ in G, these two group elements are equal and so the two coset expressions must be equal. Therefore, the induced operation is associative. As for the identity and inverse properties, there is no surprise. The identity coset is H , or $e*H$, the coset that contains G's identity. If C is a coset with representative a, that is, if, $C = a*H$, then C^{-1} is $a^{-1}*H$.

$$(a*H) \otimes (a^{-1}*H) = (a*a^{-1})*H = e*H = \text{identity coset}.$$

Definition: Factor Group. *Let G be a group and $H \leq G$. If the set of left cosets of H forms a group, then that group is called the factor group of G modulo H. It is denoted G/H.*

Note: If G is abelian, then every subgroup of G yields a factor group. We will delay further consideration of the non-abelian case to Section 15.4.

Remark on Notation: It is customary to use the same symbol for the operation of G/H as for the operation on G. The reason we used distinct symbols in this section was to make the distinction clear between the two operations.

EXERCISES FOR SECTION 15.2

A Exercises

1. Consider $\mathbb{Z}_{10}$ and the subsets of $\mathbb{Z}_{10}$, $\{0, 1, 2, 3, 4\}$ and $\{5, 6, 7, 8, 9\}$. Why is the operation induced on these subsets by modulo 10 addition not well defined?

2. Can you think of a group G, with a subgroup H such that $|H| = 6$ and $|G/H| = 6$? Is your answer unique?

3. For each group and subgroup, what is G/H isomorphic to?

(a) $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ and $H = \langle(2, 0)\rangle$. Compare to Example 15.2.5.

(b) $G = [\mathbb{C}, +]$ and $H = \mathbb{R}$.

(c) $G = \mathbb{Z}_{20}$ and $H = \langle 8 \rangle$.

4. For each group and subgroup, what is G/H isomorphic to?

(a) $G = \mathbb{Z} \times \mathbb{Z}$ and $H = \{(a, a) \mid a \in \mathbb{Z}\}$.

(b) $G = [\mathbb{R}^*, \cdot]$ and $H = \{1, -1\}$.

(c) $G = {\mathbb{Z}_2}^5$ and $H = \langle(1, 1, 1, 1, 1)\rangle$.

B Exercises

5. Prove that if G is a group, $H \leq G$ and $a, b \in G$, $a * H = b * H$ if and only if $b^{-1} * a \in H$.

6. (a) Real addition modulo r, $r > 0$, can be described as the operation induced on cosets of $\langle r \rangle$ by ordinary addition. Describe a system of distinguished representatives for the elements of $\mathbb{R}/\langle r \rangle$.

(b) Consider the trigonometric function sine. Given that $\sin(x + 2\pi k) = \sin x$ for all $x \in \mathbb{R}$ and $k \in \mathbb{Z}$, show how the distinguished representatives of $\mathbb{R}/\langle 2\pi \rangle$ can be useful in developing an algorithm for calculating the sine of a number.

15.3 Permutation Groups

At the risk of boggling the reader's mind, we will now examine groups whose elements are functions. Recall that a permutation on a set A is a bijection from A into A. Suppose that $A = \{1, 2, 3\}$. There are $3! = 6$ different permutations on A. We will call the set of all 6 permutations S_3. They are listed in Table 15.3.1. The matrix form for describing a function on a finite set is to list the domain across the top row and the image of each element directly below it. For example $r_1(1) = 2$.

$$i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$
$$r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Table 15.3.1
Elements of S_3

The operation that will give $\{i, r_1, r_2, f_1, f_2, f_3\}$ a group structure is function composition. Consider the "product" $r_1 \circ f_3$:

$$\begin{aligned} r_1 \circ f_3(1) &= r_1(f_3(1)) = r_1(2) = 3 \\ r_1 \circ f_3(2) &= r_1(f_3(2)) = r_1(1) = 2 \\ r_1 \circ f_3(3) &= r_1(f_3(3)) = r_1(3) = 1 \end{aligned}$$

The images of 1, 2, and 3 under $r_1 \circ f_3$ and $f_2$are identical. Thus, by the definition of equality for functions, we can say $r_1 \circ f_3 = f_2$. The complete table for the operation of function composition is given in Table 15.3.2. We don't even need the table to verify that we have a group:

(a) Function composition is always associative (see Chapter 7).

(b) The identity for the group is i. If g is any one of the permutations on A and $x \in A$,

$$g \circ i(x) = g(i(x)) = g(x)$$

and

$$i \circ g(x) = i(g(x)) = g(x).$$

Therefore $g \circ i = i \circ g = g$.

(c) A permutation, by definition, is a bijection. In Chapter 7 we proved that this implies that it must have an inverse and the inverse itself is a bijection and hence a permutation. Hence all elements of S_3 have an inverse in S_3. If a permutation is displayed in matrix form, its inverse can be obtained by exchanging the two rows and rearranging the columns so that the top row is in order. The first step is actually sufficient to obtain the inverse, but the sorting of the top row makes it easier to recognize the inverse.

Example 15.3.1. Lets consider a typical permutation on $\{1, 2, 3, 4, 5\}$,

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}.$$

$$f^{-1} = \begin{pmatrix} 5 & 3 & 2 & 1 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$$

Note from Table 15.3.2 that this group is non-abelian. Remember, non-abelian is the negation of abelian. The existence of two elements that don't commute is sufficient to make a group non-abelian. In this group, r_1 and f_3 is one such pair: $r_1 \circ f_3 = f_2$ while $f_3 \circ r_1 = f_1$, so $r_1 \circ f_3 \neq f_3 \circ r_1$. Caution: Don’t take this to mean that every pair of elements has to have this property. There are several pairs of elements in S_3 that *do* commute. In fact, the identity, i, must commute with everything. Also every element must commute with its inverse.

$\circ$	i	r_1	r_2	f_1	f_2	f_3
i	i	r_1	r_2	f_1	f_2	f_3
r_1	r_1	r_2	i	f_3	f_1	f_2
r_2	r_2	i	r_1	f_2	f_3	f_1
f_1	f_1	f_2	f_3	i	r_1	r_2
f_2	f_2	f_3	f_1	r_2	i	r_1
f_3	f_3	f_1	f_2	r_1	r_2	i

Table 15.3.2
Operation Table for S_3

Definition: Symmetric Group. *Let A be a nonempty set. The set of all permutations on A with the operation of function composition is called the symmetric group on A, denoted* S_A.

Our main interest will be in the case where A is finite. The size of A is more significant than the elements, and we will denote by S_k the symmetric group on any set of cardinality k, $k \geq 1$.

Example 15.3.2. Our opening example, S_3, is the smallest non-abelian group. For that reason, all of its proper subgroups are abelian: in fact, they are all cyclic. Figure 15.3.1 shows the Hasse diagram for the subgroups of S_3.

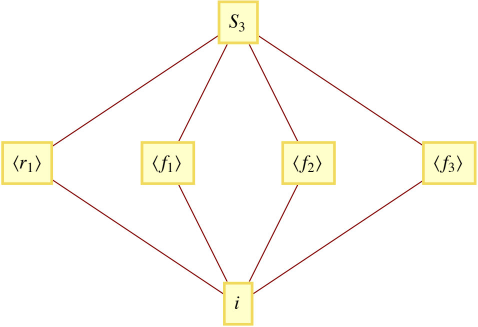


Figure 15.3.1
Lattice diagram of subgroups of S_3

Example 15.3.3. The only abelian symmetric groups are S_1 and S_2 , with 1 and 2 elements, respectively. The elements of S_2 are

$$i = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \text{ and } \alpha = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

S_2 is isomorphic to $\mathbb{Z}_2$.

Theorem 15.3.1. *For* $k \geq 1$, $|S_k| = k!$ *and for* $k \geq 3$, S_k *is non-abelian.*

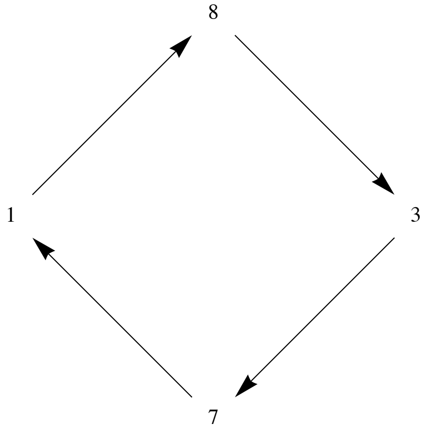
Proof: The first part of the theorem follows from the extended rule of products (see Chapter 2). We leave the details of proof of the second part to the reader after the following hint. Consider f in S_k where $f(1) = 2$, $f(2) = 3$, $f(3) = 1$, and $f(j) = j$ for $3 < j \leq n$. Now define g in a similar manner so that when you compare $f(g(1))$ and $g(f(1))$ you get different results. ■

Cycle Notation

A second way of describing a permutation is by means of cycles, which we will introduce first with an example. Consider $f \in S_8$:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 7 & 6 & 5 & 4 & 1 & 3 \end{pmatrix}$$

Consider the images of 1 when f is applied repeatedly. The images $f(1)$, $f(f(1))$, $f(f(f(1)))$, … are 8, 3, 7, 1, 8, 3, 7, ... If $j \geq 1$, In Figure 15.3.2(a), this situation is represented by the component of the graph that consists of 1, 8, 3, and 7 and shows that the values that you get by repeatedly applying f cycle through those values. This is why we refer to this part of f as a *cycle of length 4*. Of course starting at 8, 3, or 7 also produces the same cycle with only the starting valued changing.



(a)

(8,3,7,1)
(3,7,1,8)
(7,1,8,3)
or
(1,8,3,7)

(b)

Figure 15.3.2
Representations of cycles of length 4.

Figure 15.3.2(a) illustrates how the cycle can be represented in a visual manner, but it is a bit awkward to write.. Part (b) of the figure presents a more universally recognized way to write a cycle. In (b), a cycle is represented by a list where the image of any number in the list is its successor. In addition, the last number in the list has as its image the first number.

The other elements of the domain of f, are never reached if you start in the cycle (1, 8, 3, 7), and so looking at image of these other numbers will produce numbers that are disjoint from the set {1, 8, 3, 7}. The other *disjoint cycles* of f are (2), (4, 6), and (5). We can express f as a *product of disjoint cycles*:

$$f = (1,\ 8,\ 3,\ 7)(2)(4,\ 6)(5)$$

or

$$f = (1, 8, 3, 7)(4, 6)$$

where the absence of 2 and 5 implies that $f(2) = 2$ and $f(5) = 5$.

Disjoint Cycles. We say that two cycles are disjoint if no number appears in both cycles, as is the case in our expressions for / above. Disjoint cycles can be written in any order. Thus, we could also say that

$$f = (4, 6)(1, 8, 3, 7).$$

Composing Permutations. We will now consider the composition of permutations written in cyclic form, again by an example. Suppose that $f = (1,\ 8,\ 3,\ 7)(4,\ 6)$ and $g = (1,\ 5,\ 6)(8,\ 3,\ 7,\ 4)$ are elements of S_8. To calculate $f \circ g$, we start with simple concatenation:

$$f \circ g = (1, 8,\ 3,\ 7)(4,\ 6)(1, 5, 6)(8,\ 3,\ 7, 4). \qquad \text{(P)}$$

Although this is a valid expression for $f \circ g$, our goal is to express the composition as a product of disjoint cycles as f and g were individually written. We will start by determining the cycle that contains 1. *When combining any number of cycles, they are always read from right to left*. The first cycle in (P) does not contain 1; thus we move on to the second. The image of 1 under that cycle is 5. Now we move on to the next cycle, looking for 5, which doesn't appear. The fourth cycle does not contain a 5 either; so $f \circ g(1) = 5$. At this point, we would have written

$$f \circ g = (1, 5$$

on paper. We repeat the steps to determine $f \circ g(5)$. This time the second cycle of (P) moves 5 to 6 and then the third cycle moves 6 to 4. Therefore, $f \circ g(5) = 4$. We continue until the cycle (1, 5, 4, 3) is completed by determining that $f \circ g(3) = 1$. The process is then repeated starting with any number that does not appear in the cycle(s) that have already obtained. The final result for our example is

$$f \circ g = (1,\ 5,\ 4,\ 3)(6,\ 8,\ 7).$$

Since $f(2) = 2$ and $g(2) = 2$, $f \circ g(2) = 2$ and we need not include the one-cycle (2).

Video: For a video that illustrates this process, go to http://faculty.uml.edu/klevasseur/ads2/videos/cyclecomposition/.

Example 15.3.4.

(a) $(1,\ 2,\ 3,\ 4)(1,\ 2,\ 3,\ 4) = (1,\ 3)(2,\ 4)$.

(b) $(1,\ 4)(1,\ 3)(1,\ 2) = (1,\ 2,\ 3,\ 4)$.

Note that the cyclic notation does not indicate the set which is being permuted. The examples above could be in S_5, where the image of 5 is 5. This ambiguity is usually overcome by making the context clear at the start of a discussion.

Definition: Transposition. *A transposition is a cycle of length 2,*

Example 15.3.5. $f = (1,\ 4)$ and $g = (4, 5)$ are transpositions in S_5. $f \circ g = (1, 4,\ 5)$ and $g \circ f = (1,\ 5,\ 4)$ are not transpositions; thus, the set of transpositions is not closed under composition. Since $f^2 = f \circ f$ and $g^2 = g \circ g$ are both equal to the identity permutation, f and g are their own inverses. In fact, every transposition is its own inverse.

Theorem 15.3.2. *Every cycle of length greater than 2 can be expressed as a product of transpositions.*

Instead of a formal proof, we will indicate how the product of transpositions can be obtained. The key fact needed is that if $(a_1,\ a_2,\ a_3,\ \ldots,\ a_k)$ is a cycle of length k, it is equal to the following product of $k-1$ cycles.

$$(a_1,\ a_k)\cdots(a_1,\ a_3)\,(a_1,\ a_2)$$

Example 11.3.4 (b) illustrates this fact. Of course, a product of cycles can be written as a product of transpositions just as easily by applying the rule above to each cycle. For example,

$$(1,\ 3,\ 5,\ 7)(2,\ 4,\ 6) = (1,\ 7)(1,\ 5)(1,\ 3)(2,\ 6)(2,\ 4).$$

Unlike the situation with disjoint cycles, we are not free to change the order of these transpositions.

The proofs of the following two theorems appear in many abstract algebra texts.

Theorem 15.3.3. *Every permutation on a finite set can be expressed as the product of an even number of transpositions or an odd number of transpositions, but not both.*

Theorem 15.3.3 suggests that S_n can be partitioned into its "even" and "odd" elements.

Example 15.3.6. The even permutations of S_3 are i , $r_1 =$ and $r_2 =$. They form a subgroup, $\{i,\ r_1,\ r_2\}$ of S_3.

In general:

Theorem 15.3.4. *Let $n\ \geq 2$. The set of even permutations in S_n is a proper subgroup of S_n called the alternating group on $\{1,\ 2,\ \ldots n\}$, denoted A_n. The order of A_n is $\frac{n!}{2}$.*

Proof: In this proof, the letters s and t stand for transpositions and p, q are *even* nonnegative integers.

If $f,\ g\ \in A_n$, we can write the two permutations as products of even numbers of transpositions:

$$f \circ g = s_1\, s_2 \cdots s_p\, t_1\, t_2 \cdots t_q$$

Since $p+q$ is even, $f \circ g\ \in A_n$. Since A_n is closed With respect to function composition, we have proven that A_n is a subgroup of S_n. by Theorem 11.5.2. To prove the final assertion, let B_n be the set of odd permutations and let $\tau = (1, 2)$. Define $\theta : A_n \to B_n$ by $\theta(f) = f \circ \tau$. Suppose that $\theta(f) = \theta(g)$. Then f∘τ = g∘τ and by the cancellation law, f = g. Hence, θ is an injection. Next we show that θ is also a surjection. If $h\ \in B_n$, h is the image of an element of A_n. Specifically, h is the image of $h \circ \tau$.

$\theta(h \circ \tau) = (h \circ \tau) \circ \tau$ Why?

$= h \circ (\tau \circ \tau)$ Why?

$= h \circ i$ Why?

$= h$ Why?

Since θ is a bijection, $|A_n| = |B_n| = \frac{n!}{2}$. ■

Example 15.3.8. Consider the sliding-tile puzzles pictured in Figure 15.3.3. Each numbered square is a tile and the dark square is a gap. Any tile that is adjacent to the gap can slide into the gap. In most versions of this puzzle, the tiles are locked into a frame so that they can be moved only in the manner described above. The object of the puzzle is to arrange the tiles as they appear in Configuration a. Configurations b and c are typical starting points. We propose to show why the puzzle can be solved starting with b, but not with c.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	■

(a)

5	6	7	8
3	4	1	2
10	9	14	11
12	13	15	■

(b)

5	6	7	8
3	4	15	2
10	9	14	11
12	13	1	■

(c)

Figure 15.3.3
Configurations of the tile puzzle.

We will associate any configuration of the puzzle with an element of S_{16}. Imagine that a tile numbered 16 fills in the gap. If f is any configuration of the puzzle, i is Configuration a, and for $1 \leq k \leq 16$,

$f(k) =$ the number that appears in the position of k of i.

If we call Configurations b and c by the names f_1 and f_2 respectively,

$$f_1 = (1,\ 5,\ 3,\ 7)(2,\ 6,\ 4,\ 8)(9,\ 10)(11,\ 14,\ 13,\ 12)(15)(16)$$

and

$$f_2 = (1,\ 5,\ 3,\ 7,\ 15)(2,\ 6,\ 4,\ 8)(9,\ 10)(11,\ 14,\ 13,\ 12)(16).$$

How can we interpret the movement of one tile as a permutation? Consider what happens when the 12 tile of i slides into the gap. The result is a configuration that we would interpret as $(12,\ 16)$, a single transposition. Now if we slide the 8 tile into the 12 position, the result is or $(8,\ 16,\ 12)$. Hence, by "exchanging" the tiles 8 and 16, we have obtained $(8,\ 16)(12,\ 16) = (8,\ 16,\ 12)$.

1	2	3	4
5	6	7	■
9	10	11	8
13	14	15	12

Figure 15.3.4
The configuration $(8,\ 16,\ 12)$.

Every time you slide a tile into the gap, the new permutation is a transposition composed with the old permutation. Now observe that to start with i and terminate after a finite number of moves with the gap in its original position, you must make an even number of moves. Thus, any permutation that leaves 16 fixed, such as f_1 or f_2, cannot be solved if it is odd. Note that f_2 is an odd permutation; thus, Puzzle c can't be solved. The proof that all even permutations, such as f_1, can be solved is left to the interested reader to pursue.

Realizations of Groups. By now we've seen several instances a group can appear through an isomorphic copy of itself in various settings. The simplest such example is the cyclic group of order 2. When this group is mentioned, we might naturally think of the group $[\mathbb{Z}_2, +_2]$, but the groups $[\{-1, 1\}, \cdot]$ and $[S_2, \circ]$ are isomorphic to it. None of these groups are necessarily more natural or important than the others. Which one you use depends on the situation you are in and all are referred to as *realizations* of the cyclic group of order 2. The next family of groups we will study has two natural realizations, first as permutations and second as geometric symmetries.

Example 15.3.9. Dihedral Groups. The dihedral groups can realized in several ways and we will concentrate on two of them. They can be visualized as symmetries of a regular polygon — this is probably the easiest way to understand the groups. In order to represent the groups on a computer, it is convenient to represent the groups as subgroups of the symmetric groups. If $k \geq 3$, the dihedral group, D_k , is a subgroup of S_k. It is the subgroup of S_k generated by the k-

Realization as symmetries of regular polygons.

We can describe D_n in terms of symmetries of a regular n-gon ($n = 3$: equilateral triangle, $n = 4$: square, $n = 5$: a regular pentagon, ...). Here we will only concentrate on the case of D_4. If a square is fixed in space, there are several motions of the square that will, at the end of the motion, not change the apparent position of the square. The actual changes in position can be seen if the corners of the square are labeled. In Figure 15.3.5, the initial labeling scheme is shown, along with the four axes of symmetry of the square.

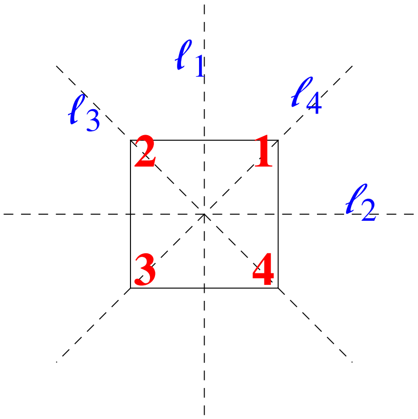
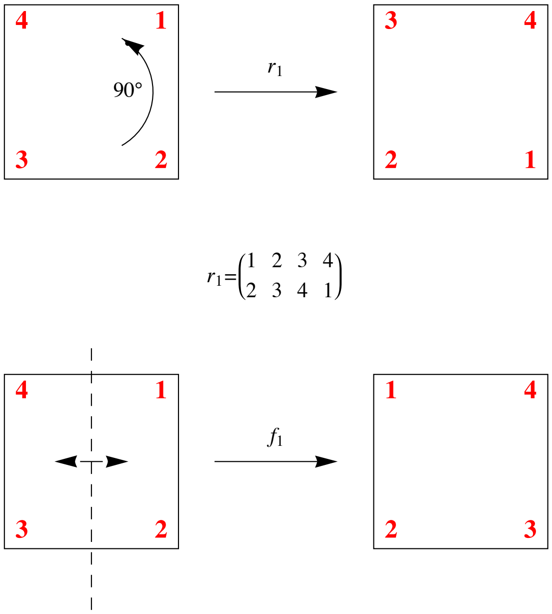


Figure 15.3.5
Axes of symmetry of the square.

It might be worthwhile making a square like this with a sheet of paper. Be careful to label the back so that the numbers match up. Two motions of the square will be considered equivalent if the square is in the same position after performing either motion. There are eight distinct motions. The first four are 0 °, 90 °, 180 °, and 270 ° clockwise rotations of the square, and the other four are the 180° flips along the axes l_1, l_2, l_3, and l_4. We will call the rotations i, r_1, r_2, and r_3, respectively, and the flips f_1, f_2, f_3, and f_4, respectively. Figure 15.3.6 illustrates r_1 and f_1. For future reference we also include the permutations to which they will correspond.



$$r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Figure 15.3.6
Two elements of D_4

What is the operation on this set of symmetries? We will call the operation "followed by" and use the symbol $*$ to represent it. The operation will be combine motions, apply motions from right to left, as with functions. We will illustrate how $*$ is computed by finding $r_1 * f_1$. Starting with the initial configuration, if you perform the f_1 motion, and then immediately perform r_1 on the result, we get the same configuration as if we just performed f_4, which is to flip the square along the line l_4. Therefore, $r_1 * f_1 = f_4$.

Realization as permutations.

We can also realize the dihedral groups as permutations. For any symmetric motion of the square we can associate with it a permutation. In the case of D_4, the images of each of the numbers 1 through 4 are the positions on the square that each of the corners 1 through 4 are moved to. For example, since corner 4 moves to position 1 when you perform r_1, the corresponding function will map 4 to 1. In addition, 1 gets mapped to 2, 2 to 3 and 3 to 4. Therefore, r_1 is the cycle (1, 2, 3, 4) . The flip $f_1$transposed two pairs of corners and corresponds to (1, 4) (2, 3). If we want to combine these two permutations, using the same names as with motions, we get

$$r_1 \circ f_1 = (1, 2, 3, 4) \circ (1, 4)(2, 3) = (1)(2, 4)(3) = (2, 4).$$

Notice that this permutation is corresponds withe flip f_4.

Although D_4 isn't cyclic (since it isn't abelian), it can be generated from the two elements r_1 and f_1:

$$D_4 = \langle r_1, f_1 \rangle = \{i, r_1, r_1^2, r_1^3, f_1, r_1 \circ f_1, r_1^2 \circ f_1, r_1^3 \circ f_1\}$$

It is quite easy to describe any of the dihedral groups in a similar fashion. Let

$r = (1, 2, \ldots, n)$, an n-cycle, and

$f = (1, n)(2, n-1) \ldots$

Then $D_n = \langle r, f \rangle = \{i, r, r^2, \ldots, r^{n-1}, f, r \circ f, r^2 \circ f, \ldots, r^{n-1} \circ f\}$

An application of D_4. One application of D_4 is in the design of a letter-facing machine. Imagine letters entering a conveyor belt to be postmarked. They are placed on the conveyor belt at random so that two sides are parallel to the belt. Suppose that a postmarker can recognize a stamp in the top right corner of the envelope, on the side facing up. In Figure 15.3.7, a sequence of machines is shown that will recognize a stamp on any letter, no matter what position in which the letter starts. The letter P stands for a postmarker. The letters R and F stand for rotating and flipping machines that perform the motions of r_1 and f_1 .

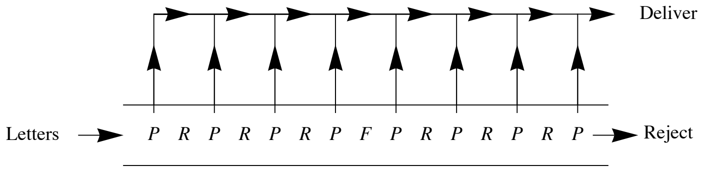


Figure 15.3.7
A letter facer

The arrows pointing up indicate that if a letter is postmarked, it is taken off the conveyor belt for delivery. If a letter reaches the end, it must not have a stamp. Letter-facing machines like this have been designed (see Gallian's paper). One economic consideration is that R-machines tend to cost more than F-machines. R-machines also tend to damage more letters. Taking these facts into consideration, the reader is invited to design a better letter-facing machine. Assume that R-machines cost \$800 and F-machines cost \$500. Be sure that all corners of incoming letters will be examined as they go down the conveyor belt.

EXERCISES FOR SECTION 15.3

A Exercises

1. Given

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \text{and } h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix},$$

compute

(a) $f \circ g$

(b) $g \circ h$

(c) $(f \circ g) \circ h$

(d) $f \circ (g \circ h)$

(e) h^{-1}

(f) $h^{-1} g \circ h$

(g) f^{-1}

2. Write f, g, and h from Exercise 1 as products of disjoint cycles and determine whether each is odd or even.

3. Do the left cosets of $A_3 = \{i, r_1, r_2\}$ over S_3 form a group under the induced operation on left cosets of A_3? What about the left cosets of $\langle f_1 \rangle$?

4. In its realization as permutations, the dihedral group D_3 is equal to S_3. Can you give a geometric explanation why? Why isn't D_4 equal to S_4?

B Exercises

5. (a) Complete the list of elements of D_4 and write out a table for the group in its realization as symmetries.

(b) List the subgroups of D_4 in a lattice diagram. Are they all cyclic? To what simpler groups are the subgroups of D_4 isomorphic?

6. Design a better letter-facing machine (see Example 15.3.9). How can you verify that a letter-facing machine does indeed check every corner of a letter? Can it be done on paper without actually sending letters through it?

7. Prove by induction that if $r \geq 1$ and each t_i, is a transposition, then

$$(t_1 \circ t_2 \circ \cdots \circ t_r)^{-1} = t_r \circ \cdots \circ t_2 \circ t_1$$

8. How many elements are there in D_5 ? Describe them geometrically.

9. Complete the proof of Theorem 15.3.1.

10. How many left cosets does A_n, $n \geq 2$ have?

11. Prove that in D_n, $f \circ r = r^{n-1} \circ f$

C Exercise

12. (a) Prove that the tile puzzles corresponding to $A_{16} \cap \{f \in S_{16} \mid f(16) = 16\}$ are solvable.

(b) If $f(16) \neq 16$, how can you determine whether f's puzzle is solvable?

13. (a) Prove that S_3 is isomorphic to R_3, the group of 3×3 rook matrices (see Section 11.2 exercises).

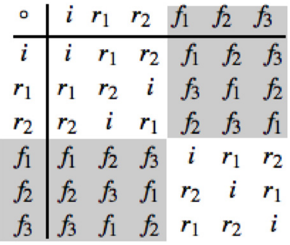
(b) Prove that for each $n \geq 2$, R_n is isomorphic to S_n.

15.4 Normal Subgroups and Group Homomorphisms

Our goal in this section is to answer an open question and introduce a related concept. The question is: When are left cosets of a subgroup a group under the induced operation? This question is open for non-abelian groups. Now that we have some examples to work with, we can try a few experiments.

NORMAL SUBGROUPS

Example 15.4.1 $A_3 = \{i, r_1, r_2\}$ is a subgroup of S_3, and its left cosets are A_3 itself and $B_3 = \{f_1, f_2, f_3\}$. Whether $\{A_3\ ,\ B_3\}$ is a group boils down to determining whether the induced operation is well defined. Consider the operation table for S_3in Figure 15.4.1.



$\circ$	i	r_1	r_2	f_1	f_2	f_3
i	i	r_1	r_2	f_1	f_2	f_3
r_1	r_1	r_2	i	f_3	f_1	f_2
r_2	r_2	i	r_1	f_2	f_3	f_1
f_1	f_1	f_2	f_3	i	r_1	r_2
f_2	f_2	f_3	f_1	r_2	i	r_1
f_3	f_3	f_1	f_2	r_1	r_2	i

Figure 15.4.1
Shaded operation table for S_3

We have shaded in all occurrences of the elements of B_3 in gray. We will call these elements the gray elements and the elements of A_3 the white ones.

Now consider the process of computing the coset product $A_3 \circ B_3$. The "product" is obtained by selecting one white element and one gray element. Note that white "times" gray is always gray. Thus, $A_3 \circ B_3$ is well defined. Similarly, the other three possible products are well defined. The table for the factor group S_3 / A_3 is

$\circ$	A_3	B_3
A_3	A_3	B_3
B_3	B_3	A_3

Clearly, S_3 / A_3 is isomorphic toe $\mathbb{Z}_2$. Note that A_3 and B_3 are also the right cosets of A_3. This is significant.

Example 15.4.2. Now let's try the left cosets of $\langle f_1 \rangle$ in S_3. There are three of them. Will we get a complicated version of $\mathbb{Z}_3$? The left cosets are

$$C_0 = \langle f_1 \rangle\ , C_1 = r_1 \langle f_1 \rangle = \{r_1, f_3\},\ \text{and}\ C_2 = r_2 \langle f_1 \rangle = \{r_2, f_2\}$$

The reader might be expecting something to go wrong eventually, and here it is. To determine $C_1 \circ C_2$ we can choose from four pairs of representatives:

$$r_1 \in C_1, r_2 \in C_2 \quad \longrightarrow \quad r_1 \circ r_2 = i \in C_0$$

$$r_1 \in C_1, f_2 \in C_2 \quad \longrightarrow \quad r_1 \circ f_2 = f \in C_0$$

$$f_3 \in C_1, r_2 \in C_2 \quad \longrightarrow \quad f_3 \circ r_2 = f_2 \in C_2$$

$$f_3 \in C_1, f_2 \in C_2 \quad \longrightarrow \quad f_3 \circ f_2 = r_2 \in C_2$$

This time, we don't get the same coset for each pair of representatives. Therefore, the induced operation is not well defined and no factor group is obtained.

Commentary: This last development changes our course of action. If we had gotten a factor group from $\{C_0, C_1, C_2\}$, we might have hoped to prove that every collection of left cosets forms a group. Now our question is: How can we determine whether we will get a factor group? Of course, this question is equivalent to: When is the induced operation well defined? There was only one step in the proof of Theorem 15.2.3, where we used the fact that G was abelian. We repeat the equations here:

$$a' * b' \ = \ (a * h_1) * (b * h_2\ ) \ = \ (a * b) * (h_1 * h_2),$$

since G was abelian.

The last step was made possible by the fact that $h_1 * b = b * h_1$. As the proof continued, we used the fact that $h_1 * h_2$ was in H and so $a' * b'$ is $(a * b) * h$ for some h in H. All that we really needed in the "abelian step" was that

$$h_1 * b \ = \ b * (\text{something in}\ H) \ = \ b * h_3\ .$$

Then, since H is closed under G's operation, $h_3 * h_2$ is an element of H. The consequence of this observation is included in the following theorem, the proof of which can be found in any abstract algebra text.

Theorem 15.4.1. *If $H \le G$, then the operation induced on left cosets of H by the operation of G is well defined if and only if any one of the following conditions is true:*

(a) If $h \in H, a \in G$, then there exists $h' \in H$ such that $h * a = a * h'$.

(b) If $h \in H, a \in G$, then $a^{-1} * h * a \in H$.

(c) Every left coset of H is equal to a right coset of H.

Corollary 15.4.2. *If $H \leq G$, then the operation induced on left cosets of H by the operation of G is well defined if either of the following two conditions is true.*

(a) G is abelian.

(b) $|H| = \frac{|G|}{2}$.

Example 15.4.3. The right cosets of $\langle f_1 \rangle \leq S_3$ are $\{i, f_1\}$, $\{r_1 f_2\}$, and $\{r_2, f_3\}$. These are not the same as the left cosets of $\langle f_1 \rangle$. In addition, $f_2^{-1} f_1 f_2 = f_2 f_1 f_2 = f_3 \notin \langle f_1 \rangle$.

Definition: Normal Subgroup. *If G is a group, $H \leq G$, then H is called a normal subgroup of G, denoted $H \lhd G$, if it satisfies any of the conditions of Theorem 15.4.1.*

Example 15.4.4. The improper subgroups $\{e\}$ and G of any group G are normal subgroups. $G/\{e\}$ is isomorphic to G. All other normal subgroups of a group, if they exist are called *proper normal subgroups*.

Example 15.4.5. By Condition b of Corollary 15.4.2, A_n is a normal subgroup of S_n and S_n/A_n is isomorphic to $\mathbb{Z}_2$.

Example 15.4.6. A_5, a group in its own right with 60 elements, has many proper subgroups, but none are normal. Although this could be done by brute force, the number of elements in the group would make the process tedious. A far more elegant way to approach the verification of this statement is to use the following fact about the cycle structure of permutations. If $f \in S_n$ is a permutation with a certain cycle structure, $\sigma_1 \sigma_2 \cdots \sigma_k$, where the length of σ_i is ℓ_i, then for any $g \in S_n$, $g^{-1} \circ f \circ g$, which is *the conjugate of f by g,* will have a cycle structure with exactly the same cycle lengths. For example if we take $f = (1, 2, 3, 4)(5, 6)(7, 8, 9) \in S_9$ and conjugate by $g = (1, 3, 5, 7, 9)$,

$$\begin{aligned} g^{-1} \circ f \circ g &= (1, 9, 7, 5, 3) \circ (1, 2, 3, 4)(5, 6)(7, 8, 9) \circ (1, 3, 5, 7, 9) \\ &= (1, 4, 9, 2)(3, 6)(5, 8, 7) \end{aligned}$$

Notice that the condition for normality of a subgroup H of G is that the conjugate of any element of H by an element of G must be remain in H.

To verify that A_5 has no proper normal subgroups, you can start by cataloging the different cycle structures that occur in A_5 and how many elements have those structures. Then consider what happens when you conjugate these different cycle structures with elements of A_5. An outline of the process is in the exercises.

Example 15.4.7. Let G be the set of two by two invertible matrices of real numbers. That is,

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \; a, b, c, d \in \mathbb{R},\ a d - b c \neq 0 \right\}$$

We saw in Chapter 11 that G is a group with matrix multiplication.

$$H_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| \; a \neq 0 \right\} \text{ and } H_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \middle| \; a d \neq 0 \right\}$$

are both subgroups of G. H_1 a normal subgroup of G, while H_2 is not normal.

Homomorphisms

Think of the word *isomorphism*. Chances are, one of the first images that comes to mind is an equation something like

$$\theta(x * y) = \theta(x) \diamond \theta(y) \qquad \text{(H)}$$

An isomorphism must be a bijection, but equation (H) is the algebraic feature of an isomorphism. Here we will examine functions that satisfy equations of this type.

Many homomorphisms are useful since they point out similarities between the two groups (or, on the universal level, two algebraic systems) involved.

Consider the groups $[\mathbb{R}^3, +]$ and $[\mathbb{R}^2, +]$. Every time you use a camera, you are trying to transfer the essence of something three-dimensional onto a photograph—that is, something two-dimensional. If you show a friend a photo you have taken, that person can appreciate much of what you saw, even though a dimension is lacking. The "picture-taking" map is a function $f : \mathbb{R}^3 \to \mathbb{R}^2$ defined by $f(x_1, x_2, x_3) = (x_1, x_2)$. This function is not a bijection, but it does satisfy the equation $f(x + y) = f(x) + f(y)$ for $x = (x_1, x_2, x_3)$ and $y = (y_1, y_2, y_3)$. Such a function is called a homomorphism, and when a homomorphism exists between two groups, the groups are called homomorphic that is, they are similar. A question that arises with groups, or other algebraic structures, that we claim are homomorphic, or similar, is: How similar are they? When we say that two groups are isomorphic—that is, identical—the map that we use to prove this is unimportant. However, when we say that two groups are homomorphic, the map used gives us a measure of the group's similarities (or dissimilarities). For example, the maps:

$f_1 : \mathbb{R}^3 \to \mathbb{R}^3$ defined by $f_1(x_1, x_2, x_3) = (x_1, x_2, x_3)$,

$f_2 : \mathbb{R}^3 \to \mathbb{R}^3$ defined by $f_2(x_1, x_2, x_3) = (x_1, x_2, 0)$, and

$f_3 : \mathbb{R}^3 \to \mathbb{R}^3$ defined by $f_3(x_1, x_2, x_3) = (0, 0, 0)$

are all homomorphisms. Think of them all as "picture-taking" maps, or cameras. The first camera gives us a three-dimensional picture, the ideal, actually an isomorphism. The second gives us the usual two-dimensional picture, certainly something quite worthwhile. The third collapses the whole scene onto a point, a "black dot," which gives no idea of the original structure. Hence, the knowledge that two groups are homomorphic doesn't give complete information about the similarities in the structures of the two groups. For this reason, the term homomorphic is rarely used (unlike isomorphic), and the functions, the homomorphisms, are studied.

Definition: Homomorphism. Let $[G, *]$ and $[G', \diamond]$ be groups. $\theta : G \to G'$ is a homomorphism if $\theta(x * y) = \theta(x) \diamond \theta(y)$ for all $x, y \in G$.

Example 15.4.8. Define $\alpha : \mathbb{Z}_6 \to \mathbb{Z}_3$ by $\alpha(n) = n(1)$, where $n \in \mathbb{Z}_6$ and $n(1)$ is the sum of n ones in $\mathbb{Z}_3$. Therefore, $\alpha(0) = 0$, $\alpha(1) = 1$, $\alpha(2) = 2, \alpha(3) = 1 + 1 + 1 = 0, \alpha(4) = 1$, and $\alpha(5) = 2$. If $n, m \in \mathbb{Z}_6$,

$$\begin{aligned} \alpha(n +_6 m) &= (n +_6 m)(1) \\ &= n(1) +_3 m(1) \\ &= \alpha(n) +_3 \alpha(m) \end{aligned}$$

Theorem 15.4.2. A few properties of homomorphisms are that if $\theta : G \to G'$ is a homomorphism, then:

(a) $\theta(e) = \theta(\text{identity of } G) = \text{identity of } G' = e'$.

(b) $\theta(a^{-1}) = \theta(a)^{-1}$ for all $a \in G$.

(c) If $H \leq G$, then $\theta(H) = \{\theta(h) \mid h \in H\} \leq G'$.

Proof:

(a) Let a be any element of G. Then $\theta(a) \in G'$.

$$\begin{aligned} \theta(a) \diamond e' &= \theta(a) && \text{by the definition of } e' \\ &= \theta(a * e) && \text{by the definition of } e \\ &= \theta(a) \diamond \theta(e) && \text{by the fact that } \theta \text{ is } a \text{ homomorphism} \end{aligned}$$

By cancellation, $e' = \theta(e)$.

(b) Again, let $a \in G$.

$$e' = \theta(e) = \theta(a * a^{-1}) = \theta(a) \diamond \theta(a^{-1}).$$

Hence, by the uniqueness of inverses, $\theta(a)^{-1} = \theta(a^{-1})$.

(c) Let $b_1, b_2 \in \theta(H)$. Then there exists $a_1, a_2 \in H$ such that $\theta(a_1) = b_1, \theta(a_2) = b_2$. Recall that a compact necessary and sufficient condition for $H \leq G$ is that $x * y^{-1} \in H$ for all $x, y \in H$. Now we apply the same fact in G' :

$$\begin{aligned} b_1 \diamond b_2{}^{-1} &= \theta(a_1) \diamond \theta(a_2)^{-1} \\ &= \theta(a_1) \diamond \theta(a_2{}^{-1}) \\ &= \theta(a_1 * a_2{}^{-1}) \in \theta(H) \end{aligned}$$

since $a_1 * a_2{}^{-1} \in H$, and so we can conclude that $\theta(H) \leq G'$. ■

***Corollary**. Since a homomorphism need not be a surjection and part (c) of Theorem 15.4.2 is true for the case of $H = G$, the range of θ, $\theta(G)$, is a subgroup of G'*

Example 15.4.9. If we define $\pi : \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ by $\pi(n) = n + 4\mathbb{Z}$. then π is a homomorphism. The image of the subgroup $4\mathbb{Z}$ is the single coset $0 + 4\mathbb{Z}$, the identity of the factor group. Homomorphisms of this type are called *natural homomorphisms*. The following theorems will verify that π is a homomorphism and also show the connection between homomorphisms and normal subgroups. The reader can find more detail and proofs in most abstract algebra texts.

***Theorem 15.4.3.** If $H \lhd G$, then the function $\pi : G \to G/H$ defined by $\pi(a) = aH$ is a homomorphism, called the natural homomorphism.*

Based on Theorem 15.4.3, every normal subgroup gives us a homomorphism.

***Definition: Kernel.** Let $\theta : G \to G'$ be a homomorphism, and let e' be the identity of G'. The kernel of θ is the set*

$$ker\, \theta = \{a \in G \mid \theta(a) = e'\}$$

***Theorem 15.4.4.** Let $\theta : G \to G'$ be a homomorphism from G into G'. The kernel of θ is a normal subgroup of G.*

Based on Theorem 15.4.4, every homomorphism gives us a normal subgroup.

***Theorem 15.4.5 : Fundamental Theorem of Group Homomorphisms.** Let $\theta : G \to G'$ be a homomorphism. Then $\theta(G)$ is isomorphic to $G/ker\, \theta$.*

Example 15.4.10. Define $\theta : \mathbb{Z} \to \mathbb{Z}_{10}$ by $\theta(n) =$ the remainder from dividing n by 10. The three previous theorems imply the following:

(15.4.3) $\pi : \mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$ defined by $\pi(n) = n + 10\mathbb{Z}$ is a homomorphism.

(15.4.4) $\{n \in \mathbb{Z} \mid \theta(n) = 0\} = \{10\,n \mid n \in \mathbb{Z}\} = 10\,\mathbb{Z} \lhd \mathbb{Z}$.

(15.4.5) $\mathbb{Z} / 10\,\mathbb{Z}$ is isomorphic to $\mathbb{Z}_{10}$.

Example 15.4.11. Let G be the same group of two by two invertible real matrices as in Example 15.4.6. Define $\Phi : G \to G$ by $\Phi(A) = \frac{A}{\sqrt{|\det A|}}$. We will let the reader verify that Φ is a homomorphism. The theorems above imply:

(15.4.4) $\ker \Phi = \{A \mid \Phi(A) = I\} = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \,\middle|\, a \in \mathbb{R},\ a \neq 0 \right\} \lhd G$. This verifies our statement in Example 15.4.6. As in that example, let $\ker \Phi = H_1$.

(15.4.5) G / H_1 is isomorphic to $\{A \in G \mid \det A = \pm 1\}$.

(15.4.3) $\pi : G -> G / H_1$ defined, naturally, by $\pi(A) = A\,H_1$ is a homomorphism.

For the remainder of this section, we will be examining certain kinds of homomorphisms that will play a part in our major application to homomorphisms, coding theory.

Example 15.4.12. Consider $\Phi : {\mathbb{Z}_2}^2 \to {\mathbb{Z}_2}^3$ defined by $\Phi(a,\ b) = (a,\ b,\ a +_2 b)$. If $(a_1, b_1),\ (a_2\,,\ b_2) \in {\mathbb{Z}_2}^2$,

$$\begin{aligned} \Phi((a_1, b_1) + (a_2\,,\ b_2)) &= \Phi(a_1 +_2 a_2, b_1 +_2 b_2) \\ &= (a_1 +_2 a_2, b_1 +_2 b_2\,, a_1 +_2 a_2 +_2 b_1 +_2 b_2) \\ &= (a_1, b_1\,,\ a_1 +_2 b_1) + (a_2, b_2\,,\ a_2 +_2 b_2) \\ &= \Phi(a_1, b_1) + \Phi(a_2\,,\ b_2) \end{aligned}$$

Since $\Phi(a,\ b) = (0,\ 0,\ 0)$ implies that $a = 0$ and $b = 0$, the kernel of Φ is $\{(0,\ 0)\}$. By previous theorems, $\Phi\left({\mathbb{Z}_2}^2\right) = \{(0,\ 0,\ 0),\ (1,\ 0,\ 1),\ (0,\ 1,\ 1),\ (1,\ 1,\ 0)\}$ is isomorphic to ${\mathbb{Z}_2}^2$.

We can generalize the previous example as follows: If $n,\ m \geq 1$ and A an $m \times n$ matrix of 0's and 1's (elements of $\mathbb{Z}_2$), then $\Phi : {\mathbb{Z}_2}^m \to {\mathbb{Z}_2}^n$ defined by

$$\Phi(a_1,\ a_2\,,\ \ldots,\ a_m) = (a_1,\ a_2\,,\ \ldots,\ a_m)\,A$$

is a homomorphism. This is true because matrix multiplication is distributive over addition. The only new idea here is that computation is done in $\mathbb{Z}_2$ where $1 +_2 1 = 0$. If $a = (a_1,\ a_2\,,\ \ldots,\ a_m)$ and $b = (b_1,\ b_2\,,\ \ldots,\ b_m)$, $(a + b)\,A = a\,A + b\,A$ is true by basic matrix laws. Therefore, $\Phi(a + b) = \Phi(a) + \Phi(b)$.

EXERCISES FOR SECTION 15.4

A Exercises

1. Which of the following functions are homomorphisms? What are the kernels of those functions that are homomorphisms?

(a) $\theta_1 : \mathbb{R}^* \to \mathbb{R}^+$ defined by $\theta_1(a) = |a|$.

(b) $\theta_2 : \mathbb{Z}_8 \to \mathbb{Z}_2$ where $\theta_2(n) = \begin{cases} 0 & \text{if } n \text{ is even} \\ 1 & \text{if } n \text{ is odd} \end{cases}$.

(c) $\theta_3 : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, where $\theta_3(a,\ b) = a + b$.

(d) $\theta_4 : S_4 \to S_4$ defined by $\theta_4(f) = f \circ f = f^2$.

2. Which of the following functions are homomorphisms? What are the kernels of those functions that are homomorphisms?

(a) $\alpha_1 : M_{2\times2}(\mathbb{R}) \to \mathbb{R}$, defined by $\alpha_1(A) = A_{11}\,A_{22} + A_{12}\,A_{21\,ß}$.

(b) $\alpha_2 : (\mathbb{R}^*)^2 -> \mathbb{R}^*$ defined by $\alpha_2\,(a,\ b) = a\,b$.

(c) $\alpha_3 : \{A \in M_{2\times2}(\mathbb{R}) \mid \det A \neq 0\} \to \mathbb{R}^*$, where $\alpha_3(A) = \det A$.

(d) $\alpha_4 : S_4 \to S_4$ defined by $\alpha_4(f) = f^{-1}$.

3. Show that D_4 has one proper normal subgroup, but that $\langle(1,\,4)\,(2,\,3)\rangle$ is not normal.

4. Prove that the function Φ in Example 15.4.11 is a homomorphism.

5. Define the two functions $\alpha : {\mathbb{Z}_2}^3 \to {\mathbb{Z}_2}^4$ and $\beta : {\mathbb{Z}_2}^4 \to \mathbb{Z}_2$ by

$\alpha(a_1, a_2, a_3) = (a_1, a_2, a_3\,, a_1 +_2 a_2 +_2 a_3)$, and

$\beta(b_1, b_2, b_3, b_4) = b_1 + b_2 + b_3 + b_4$

Describe the function $\beta \circ \alpha$. Is it a homomorphism?

6. Express Φ in Example 15.4.12 in matrix form.

B Exercises

7. Prove that if G is an abelian group, then $q(x) = x^2$ defines a homomorphism from G into G. Is q ever an isomorphism?

8. Prove that if $\theta : G \to G'$ is a homomorphism, and $H \lhd G$, then $\theta(H) \lhd \theta(G)$. Is it also true that $\theta(H) \lhd G'$?

9. Prove that if $\theta : G \to G'$ is a homomorphism, and $H' \leq \theta(G)$, then $\theta^{-1}(H') = \{a \in G \mid \theta(a) \in H'\} \leq G$.

C Exercises

10. Following up on Example 11.4.6, prove that A_5 is a simple group; i. e., it has no proper normal subgroups.

(a) Make a list of the different cycle structures that occur in A_5 and how many elements have those structures.

(b) Within each set of permutations with different cycle structures, identify which subsets are closed with respect to the conjugation operation. With this you will have a partition of A_5 into *conjugate classes* where for each class C,

$$f,\ g \in C \quad \text{if and only if} \quad \exists\ \phi \in A_5 \quad \text{such that} \quad \phi^{-1} \circ f \circ \phi = g$$

(c) Use the fact that a normal subgroup of A_5 needs to be a union of conjugate classes and verify that no such union exists.

15.5 Coding Theory—Group Codes

In this section, we will introduce the basic ideas involved in coding theory and consider solutions of a coding problem by means of group codes.

A Transmission Problem. Imagine a situation in which information is being transmitted between two points. The information takes the form of high and low pulses (for example, radio waves or electric currents), which we will label 1 and 0, respectively. As these pulses are sent and received, they are grouped together in *blocks* of fixed length. The length determines how much information can be contained in one block. If the length is r, there are 2^r different values that a block can have. If the information being sent takes the form of text, each block might be a character. In that case, the length of a block may be seven, so that $2^7 = 128$ block values can represent letters (both upper and lower case), digits, punctuation, and so on. Figure 15.5.1 illustrates the problem that can be encountered if information is transmitted between two points. During the transmission of data, noise can alter the signal so that what is received differs from what is sent.

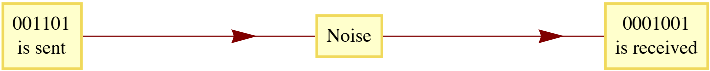


Figure 15.5.1
A noisy transmission

Noise. Noise is a fact of life for anyone who tries to transmit information. Fortunately, in most situations, we could expect a high percentage of the pulses that are sent to be received properly. However, when large numbers of pulses are transmitted, there are usually some errors due to noise. For the remainder of the discussion, we will make assumptions about the nature of the noise and the message that we want to send. Henceforth, we will refer to the pulses as bits.

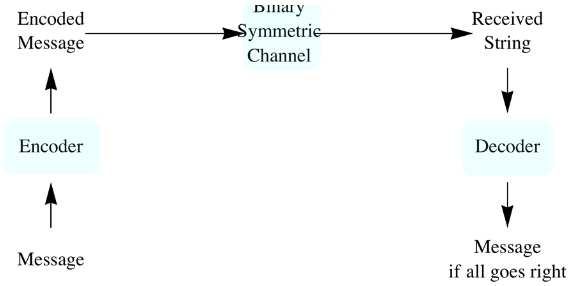


Figure 15.5.2
The Coding Process

Binary Symmetric Channels

We will assume that our information is being sent along a *binary symmetric channel*. By this we mean that any single bit that is transmitted will be received improperly with a certain fixed probability, p. The value of p is usually quite small. To illustrate the process, we will assume that $p = 0.001$, which, in the real world, would be considered somewhat large. Since $1 - p = 0.999$, we can expect 99.9% of all bits to be properly received.

Suppose that our message consists of 3,000 bits of information, to be sent in blocks of three bits each. Two factors will be considered in evaluating a method of transmission. The first is the probability that the message is received with no errors. The second is the number of bits that will be transmitted in order to send the message. This quantity is called the rate of transmission:

$$\text{Rate} = \frac{\text{Message length}}{\text{Number of bits transmitted}}$$

As you might expect, as we devise methods to improve the probability of success, the rate will decrease.

Case 1: Raw information. Suppose that we ignore the noise and transmit the message “as is.” The probability of success is

$$0.999^{3000} = 0.0497124$$

Therefore we only successfully receive the message totally correct less than 5% of the time. The rate of $3000/3000 = 1$ certainly doesn't offset this poor probability.

The Coding Process

Our strategy for improving our chances of success will be to send an encoded message across the binary symmetric channel. The encoding will be done in such a way that small errors can be identified and corrected. This idea is illustrated in Figure 15.5.2.

In our examples, the functions that will correspond to our encoding and decoding devices will all be homomorphisms between Cartesian products of $\mathbb{Z}_2$.

Case 2: An Error-Detecting Code. Suppose that each block of three bits $a = (a_1, a_2, a_3)$ is encoded according to the function

$$e : \mathbb{Z}_2{}^3 \to \mathbb{Z}_2{}^4 4 ,$$

where

$$e(a) = (a_1, a_2, a_3, a_1 +_2 a_2 +_2 a_3).$$

When the encoded block is received, the first three bits are probably part of the message (it is correct approximately 99.7% of the time), but the added bit that is sent will make it possible to detect single errors in the block. Note that when $e(a)$ is transmitted, the sum of its components is

$$a_1 +_2 a_2 +_2 a_3 +_2 (a_1 +_2 a_2 +_2 a_3) = 0$$

since $a_i + a_i = 0$ in $\mathbb{Z}_2$.

If any single bit is garbled by noise, the sum of the received bits will be 1. The last bit of $e(a)$ is called the parity bit. A parity error occurs if the sum of the received bits is 1. Since more than one error is unlikely when p is small, a high percentage of all errors can be detected.

At the receiving end, the decoding function acts on the four-bit block $b = (b_1, b_2, b_3, b_4)$ according to

$$d(b) = (b_1, b_2, b_3, b_1 +_2 b_2 +_2 b_3 +_2 b_4).$$

The fourth bit is called the parity-check bit. If no parity error occurs, the first three bits are recorded as part of the message. If a parity error occurs, we will assume that a retransmission of that block can be requested. This request can take the form of automatically having the parity-check bit of $d(b)$ sent back to the source. If 1 is received, the previous block is retransmitted; if 0 is received, the next block is sent. This assumption of two-way communication is significant, but it is necessary to make this coding system useful. It is reasonable to expect that the probability of a transmission error in the opposite direction is also 0.001. Without going into the details, we will report that the probability of success is approximately 0.990 and the rate is approximately 3/5. The rate includes the transmission of the parity-check bit to the source.

Case 3: An Error-Correcting Code. For our final case, we will consider a coding process that can correct errors at the receiving end so that only one-way communication is needed. Before we begin, recall that every element of $\mathbb{Z}_2{}^n$, $n \geq 1$, is its own inverse; that is, $-b = b$. Therefore, $a - b = a + b$.

The three-bit message blocks are difficult to transmit because they are so similar to one another. If a and b are in $\mathbb{Z}_2{}^3$, their difference, $a +_2 b$, can be thought of as a measure of how close they are. If a and b differ in only one bit position, one error can change one into the other. The encoding that we will introduce takes a block $a = (a_1, a_2, a_3)$ and produces a block of length 6 called the code word of a. The code words are selected so that they are farther from one another than the messages are. In fact, each code word will differ from each other code word by at least three bits. As a result, any single error will not push a code word close enough to another code word to cause confusion. Now for the details. Let

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

be the *generator matrix* for the code, and

$$a = (a_1, a_2, a_3)$$

Define $e : \mathbb{Z}_2{}^3 \to \mathbb{Z}_2{}^6$ by

$$e(a) = a G = (a_1, a_2, a_3, a_4, a_5, a_6)$$

where

$$\begin{aligned} a_4 &= a_1 +_2 a_2 \\ a_5 &= a_1 \qquad +_2 a_3 \\ a_6 &= \qquad a_2 +_2 a_3 \end{aligned}$$

Notice that e is a homomorphism. If a and b are distinct elements of $\mathbb{Z}_2{}^3$, then $c = a + b$ has at least one coordinate equal to 1. Now consider the difference between $e\,(a)$ and $e\,(b)$:

$$\begin{aligned} e\,(a) + e\,\{b) &= e\,(a + b) \\ &= e(c) \\ &= (c_1,\ c_2,\ c_3, c_4,\ c_5,\ c_6) \end{aligned}$$

Whether c has 1, 2, or 3 ones, $e\,(c)$ must have at least three ones; therefore $e\,(a)$ and $e\,(b)$ differ in at least three bits.

Now consider the problem of decoding the code words. Imagine that a code word, $e\,(a)$, is transmitted, and $b = (b_1,\ b_2,\ b_3, b_4,\ b_5,\ b_6)$ is received. At the receiving end, we know the formula for $e\,(a)$, and if no error has occurred in transmission,

$$\begin{array}{r} b_1 = a_1 \\ b_2 = a_2 \\ b_3 = a_3 \\ b_4 = a_1 +_2 a_2 \\ b_2 = a_1 +_2 a_3 \\ b_2 = a_2 +_2 a_3 \end{array} \Rightarrow \begin{array}{l} b_1 +_2 b_2 +_2 b_4 = 0 \\ b_1 +_2 b_3 +_2 b_5 = 0 \\ b_2 +_2 b_3 +_2 b_6 = 0 \end{array}$$

The three equations on the right are called parity-check equations. If any of them is not true, an error has occurred. This error checking can be described in matrix form. Let

$$P = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

P is called the parity-check matrix for this code. Now define $p : \mathbb{Z}_2{}^6 \to \mathbb{Z}_2{}^3$ by $p\,(b) = b\,P.$ We call $p\,(b)$ the syndrome of the received block. For example,

$$p(0, 1, 0, 1, 0, 1) = (0, 0, 0) \text{ and } p(1, 1, 1, 1, 0, 0) = (1, 0, 0)$$

Note that p is also a homomorphism. If the syndrome of a block is $(0,\ 0,\ 0)$, we can be almost certain that the message block is $(b_1,\ b_2,\ b_3)$.

Next we turn to the method of correcting errors. Despite the fact that there are only eight code words, one for each three-bit block value, the set of possible received blocks is $\mathbb{Z}_2{}^6$, with 64 elements. Suppose that b is not a code word, but that it differs from a code word by exactly one bit. In other words, it is the result of a single error in transmission. Suppose that w is the code word that b is close to and that they differ in the first bit. Then

$$b + w = (1,\ 0,\ 0,\ 0,\ 0,\ 0)$$

and

$$\begin{aligned} p(b) &= p\,(b) + p(w) && \text{since } p\,(w) = (0,\ 0,\ 0) \\ &= p(b + w) && \text{since } p \text{ is a homomorphism} \\ &= p(1, 0, 0, 0, 0, 0) \\ &= (1, 1, 0) \end{aligned}$$

Note that we haven't specified b or w, only that they differ in the first bit. Therefore, if b is received and $p\,(b) = (1,\ 1,\ 0)$, the transmitted code word was probably $b + (1,\ 0,\ 0,\ 0,\ 0,\ 0)$ and the message block was $(b_1 +_2 1,\ b_2,\ b_3)$. The same analysis can be done if b and w differ in any of the other five bits.

This process can be described in terms of cosets. Let W be the set of code words; that is, $W = e\left(\mathbb{Z}_2{}^3\right)$. W is a subgroup of $\mathbb{Z}_2{}^6$. Consider the factor group $\mathbb{Z}_2{}^6 \big/ W$:

$$\left|\mathbb{Z}_2{}^6 \big/ W\right| = \frac{|\mathbb{Z}_2{}^6|}{|W|} = \frac{64}{8} = 8.$$

Suppose that b_1 and b_2 are representatives of the same coset. Then $b_1 = b_2 + w$ for some w in W. Therefore,

$$\begin{aligned} p(b_{\,1}) &= p(b_1) + p\,(w) \text{ since } p\,(w) = (0,\ 0,\ 0) \\ &= p(b_1 + w) \\ &= p(b_2\,) \end{aligned}$$

and so b_1 and b_2 have the same syndrome.

Finally, suppose that d_1 and d_2 are distinct and both have only a single coordinate equal to 1. Then $d_1 + d_2$ has exactly two ones. Note that the identity of $\mathbb{Z}_2{}^6$, $(0, 0, 0, 0, 0, 0)$, must be in W. Since $d_1 + d_2$ differs from the identity by two bits, $d_1 + d_2 \notin W$. Hence d_1 and d_2 belong to distinct cosets. The reasoning above serves as a proof of the following theorem.

Theorem 15.5.1. *There is a system of distinguished representatives of* $\mathbb{Z}_2^{\,6}\big/W$ *such that each of the six-bit blocks having a single 1 is a distinguished representative of its own coset.*

Now we can describe the error-correcting process. First match each of the blocks with a single 1 with its syndrome. In addition, match the identity of W with the syndrome (0, 0, 0) (see Table 15.5.1). Since there are eight cosets of W, select any representative of the eighth coset to be distinguished. This is the coset with syndrome (1, 1, 1).

Syndrome	Error Correction
0 0 0	0 0 0 0 0 0
1 1 0	1 0 0 0 0 0
1 0 1	0 1 0 0 0 0
0 1 1	0 0 1 0 0 0
1 0 0	0 0 0 1 0 0
0 1 0	0 0 0 0 1 0
0 0 1	0 0 0 0 0 1
1 1 1	1 0 0 0 0 1

Table 15.5.1
Error Correction Table

When block b is received, you need only:

(1) Compute the syndrome, $p\,(b)$, and

(2) Add to b the error correction that matches $p\,(b)$.

We will conclude this example by computing the probability of success for our hypothetical situation. It is

$$\left(0.999^6 \;+\; 6\times 0.999^5 \times 0.001\right)^{1000} = 0.985151\,.$$

The rate for this method is $\frac{1}{2}$.

EXERCISES FOR SECTION 15.5

A Exercises

1. If the error-detecting code is being used, how would you act on the following received blocks?

(a) (1, 0, 1, 1)

(b) (1, 1, 1, 1)

(c) (0, 0, 0, 0)

2. Express the encoding and decoding functions for the error-detecting code using matrices.

3. If the error-correcting code is being used, how would you decode the following blocks? Expect a problem with one of these. Why?

(a) (1, 0, 0, 0, 1, 1)

(b) (1, 0, 1, 0, 1, 1)

(c) (0, 1, 1, 1, 1, 0)

(d) (0, 0, 0, 1, 1, 0)

4. Describe how the triple-repetition code with encoding function, $e : \mathbb{Z}_2 \to \mathbb{Z}_2{}^3$, where $e(a_1) = (a_1, a_1, a_1)$ can allow us to correct a single error. What is the probability of success for the $p = 0.001$, 3000-bit situation? What are the generator and parity-check matrices for this code?

B Exercise

5. Consider the linear code defined the generator matrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

(a) What size blocks does this code encode and what is the length of the code words?

(b) What are the code words for this code?

(c) With this code, can you detect single bit errors? Can you correct all, some, or no single bit errors?

6. **Rectangular codes.** To build a rectangular code, you partition your message into blocks of length m and then factor m into $k_1 \cdot k_2$ and arrange the bits in a k_1 by k_2 rectangular array as in the figure below (read "digit" as "bit"). Then you add parity bits along the right side and bottom of the rows and columns. The code word is read row by row.

$$\begin{array}{cccccc} \blacksquare & \blacksquare & \blacksquare & \cdots & \blacksquare & \square \\ \blacksquare & \blacksquare & \blacksquare & \cdots & \blacksquare & \square \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \blacksquare & \blacksquare & \blacksquare & \cdots & \blacksquare & \square \\ \square & \square & \square & \cdots & \square & \end{array}$$

■ = message bit
□ = parity bit

For example, if m is 4, then our only choice is a 2 by 2 array. The message 1101 would be encoded as so

$$\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & 1 & 1 \\ \hline 1 & 0 & \end{array}$$

And the code word is the string 11001110.

(a) Suppose that you were sent four bit messages using this code and your received the following strings. What were the messages.

(i) 11011000
(ii) 01110010
(iii) 10001111

(b) If you encoded n^2 bits in this manner, what would be the rate of the code?

(c) Rectangular codes are linear codes for the 3 by 2 rectangular code, what are the generator and parity check matrices?

SUPPLEMENTARY EXERCISES FOR CHAPTER 15

Section 15.1

1. How does one find all subgroups of any cyclic group? Can this same process be used to determine all subgroups of noncyclic groups?

2. Exercise 8 of Section 15.1 tells us that $\mathbb{Z}_2 \times \mathbb{Z}_5$ is isomorphic to $\mathbb{Z}_{10}$. Use the Chinese Remainder Theorem to find an isomorphism between these two groups,

3. Use the Chinese Remainder Theorem to add 74 and 85 in $\mathbb{Z}_{120}$.

Section 15.2

4. Let G be a group and assume $|G| = 10$. Can G have subgroups of order 2? ...of order 3? ... of order 4? Explain.

5. List all left cosets of $H = \{0, 4, 8\}$ in the group $\mathbb{Z}_{12}$ and write out the table for $\mathbb{Z}_{12}/H$.

6. Let G be a finite group of order n. Then for any $a \in G, a^n = e$, where e is the identity of G. Interpret this statement for the groups $[\mathbb{Z}_6, +_6]$ and $[U(\mathbb{Z}_6), \times_6]$

7. (a) Consider $\mathbb{Z}_8/\langle 2 \rangle$. How many distinct left cosets of $\langle 2 \rangle$ in $\mathbb{Z}_8$ are there? List them.

(b) Repeat part a for $\mathbb{Z}_{12}/\langle 2 \rangle$.

(c) Is $\mathbb{Z}_8/\langle 2 \rangle$ isomorphic to $\mathbb{Z}_{12}/\langle 2 \rangle$? Explain.

Section 15.3

8. Determine all proper subgroups of the symmetric group S_3 and draw a Hasse diagram for the relation "is a subset of."

9. Let $f \in S_n$. Prove that f is even if and only if f^{-1} is even.

10. (a) By analogy with the motions of a square, how many motions of a cube are there?

(b) Design a "package-facing" machine using the group of motions of the cube.

Section 15.4

11. (a) Let $[B_1, -_1, \vee_1, \wedge_1]$ and $[B_2, -_2, \vee_2, \wedge_2]$ be Boolean algebras. Define a Boolean algebra homomorphism based on the definition of a group homomorphism.

(b) Your definition in part a should result in properties similar to the ones of a group homomorphism. Let $f : B_1 \to B_2$ be a Boolean algebra homomorphism. Prove:

(i) $f(0_1) = 0_2$ and $f(1_1) = 1_2$

(ii) $a \leq b \Rightarrow f(a) \leq f(b) \;\forall\; a, b \in B_1$ and

(iii) $f(B_1)$ is a Boolean subalgebra of B_2.

12. (a) Prove the contentions of example 15.4.6 that H_1 is a normal subgroup of $\text{GL}(2, \mathbb{R})$ but that H_2 is not.

(b) In order to get a clearer picture of what $\text{GL}(2, \mathbb{R})/\text{SL}(2, \mathbb{R})$ is, prove that the determinant function $\det : \text{GL}(2, \mathbb{R}) \to \mathbb{R}^*$ is an onto homomorphism, and apply Theorem 15.4.5.

Section 15.5

13. This exercise concerns a code called the Hamming (7, 4) code, an error-correcting code with rate 4/7. A four by seven generator matrix G encodes message blocks of length 4 according to the rule $e(a) = a\,G$, so that the parity check matrix for the code is

$$P = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

That is, b is a code word iff $b\,P = (\,0 \quad 0 \quad 0\,)$.

(a) Find G.

(b) Encode 1111 and 1001.

(c) Compute the syndrome of the following received message blocks and correct them, if necessary:

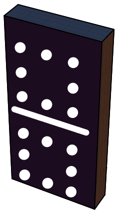
(i) 0100000 (ii) 1010101 (iii) 1011011.

(d) Prove that this code does indeed correct all single bit errors.

14. Given a code with parity check matrix P whose transpose is given below, identify the generator matrix, and the rate of the code. Prove that the code corrects all single errors.

$$P = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Chapter 16



An Introduction to Rings and Fields

GOALS

In our early elementary school days we began the study of mathematics by learning addition and multiplication on the set of positive integers. We then extended this to operations on the set of all integers. Subtraction and division are defined in terms of addition and multiplication. Later we investigated the set of real numbers under the operations of addition and multiplication. Hence, it is quite natural to investigate those structures on which we can define these two fundamental operations, or operations similar to them. The structures similar to the set of integers are called rings, and those similar to the set of real numbers are called fields.

In coding theory, highly structured codes are needed for speed and accuracy. The theory of finite fields is essential in the development of many structured codes. We will discuss basic facts about finite fields and introduce the reader to polynomial algebra.

16.1 Rings—Basic Definitions and Concepts

As mentioned in our goals, we would like to investigate algebraic systems whose structure imitates that of the integers.

Definition: Ring. *A ring is a set R together with two binary operations, addition and multiplication, denoted by the symbols + and $\cdot$ such that the following axioms are satisfied:*

(1) $[R, +]$ *is an abelian group.*

(2) Multiplication is associative on R.

(3) Multiplication is distributive over addition; that is, for all a, b, c $\in$ R, the left distributive law, a(b + c) = ab + ac, and the right distributive law, (b + c)a - ba + ca, hold.

Comments:

(1) A ring is designated as $[R, +, \cdot]$ or as just plain R if the operations are understood.

(2) The symbols + and $\cdot$ stand for arbitrary operations, not just "regular" addition and multiplication. These symbols are referred to by the usual names. For simplicity, we will write $a\,b$ instead of $a \cdot b$ if it is not ambiguous.

(3) For the abelian group $[R, +]$, we use additive notation. In particular, the group identity is designated by 0 rather than by e and is customarily called the "zero" of the ring. The group inverse is also written in additive notation: $-a$ rather than a^{-1} .

We now look at some examples of rings. Certainly all the additive abelian groups of Chapter 11 are likely candidates for rings.

Example 16.1.1. $[\mathbb{Z}, +, \cdot]$ is a ring, where + and $\cdot$ stand for regular addition and multiplication on $\mathbb{Z}$. From Chapter 11, we already know that $[\mathbb{Z}, +]$ is an abelian group, so we need only check parts 2 and 3 of the definition of a ring. From elementary algebra, we know that the associative law under multiplication and the distributive laws are true for $\mathbb{Z}$. This is our main example of an infinite ring.

Example 16.1.2. $[\mathbb{Z}_n, +_n, \times_n]$ is a ring. The properties of modular arithmetic on $\mathbb{Z}_n$ were described in Section 11.4, and they give us the information we need to convince ourselves that $[\mathbb{Z}_n, +_n, \times_n]$ is a ring. This example is our main example of finite rings of different orders.

Definition: Commutative Ring. *A ring in which the commutative law holds under the operation of multiplication is called a commutative ring.*

It is common practice to use the word abelian when referring to the commutative law under addition and the word commutative when referring to the commutative law under the operation of multiplication.

Definition: Unity. *A ring $[R, +, \cdot]$ that has a multiplicative identity is called a ring with unity. The multiplicative identity itself is called the unity of the ring. More formally, if there exists an element in R, designated by* 1, *such that for all $x \in R$, $x \cdot 1 = 1 \cdot x = x$, then R is called a ring with unity.*

Example 16.1.3. The rings in Examples 16.1.1 and 16.1.2 are commutative rings with unity, the unity in both cases being the number 1. The ring $[M_{2\times 2}(\mathbb{R}), +, \cdot]$ is a noncommutative ring with unity, the unity being the identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

DIRECT PRODUCTS OF RINGS

Let $R_1, R_2, \ldots, R_n$ be rings under the operations $+_1, +_2, \ldots, +_n$ and $\cdot_1, \cdot_2, \ldots, \cdot_n$ respectively. Let

$$P = \mathop{\times}_{i=1}^{n} R_i$$

and $a = \{a_1, a_2, \ldots, a_n), b = (b_1, b_2, \ldots, b_n) \in P$.

From Chapter 11 we know that P is an abelian group under the operation of componentwise addition:

$$a + b = (a_1 +_1 b_1, a_2 +_2 b_2, \ldots, a_n +_n b_n).$$

We also define multiplication on P componentwise:

$$a \cdot b = (a_1 \cdot_1 b_1, a_2 \cdot_2 b_2, \ldots, a_n \cdot_n b_n).$$

To show that P is a ring under the above operations, we need only show that the (multiplicative) associative law and the distributive laws hold. This is indeed the case, and we leave it as an exercise. If each of the R_i is commutative, then P is commutative, and if each contains a unity, then P is a ring with unity, which is the $n -$ tuple consisting of the unities of each of the R_i' s.

Example 16.1.4. Since $[\mathbb{Z}_4, +_4, \times_4]$ and $[\mathbb{Z}_3, +_3, \times_3]$ are rings, then $\mathbb{Z}_4 \times \mathbb{Z}_3$ is a ring, where, for example,

$$(2, 1) + (2, 2) = (2 +_4 2, 1 +_3 2) = (0, 0)$$

and

$$(3, 2) \cdot (2, 2) = (3 \times_4 2, 2 \times_3 2) = (2, 1).$$

To determine the unity, if it exists, in the ring $\mathbb{Z}_4 \times \mathbb{Z}_3$, we look for the element (m, n) such that for all elements $(x, y) \in \mathbb{Z}_4 \times \mathbb{Z}_3$,

$$(x, y) = (x, y) \cdot (m, n) = (m, n) \cdot (x, y),$$

or, equivalently,

$$(x \times_4 m, y \times_3 n) = (m \times_4 x, n \times_3 y) = (x, y).$$

So we want m such that $x \times_4 m = m \times_4 x = x$ in the ring $\mathbb{Z}_4$. The only element m in $\mathbb{Z}_4$ that satisfies this equation is $m = 1$. Similarly, we obtain a value of 1 for n. So the unity of $\mathbb{Z}_4 \times \mathbb{Z}_3$, which is unique by Exercise 15 of this section, is $(1, 1)$. We leave to the reader to verify that this ring is commutative.

Hence, products of rings are analogous to products of groups or products of Boolean algebras. We now consider the extremely important concept of multiplicative inverses. Certainly many basic equations in elementary algebra (e.g., $2x = 3$) are solved with this concept. We introduce the main idea here and develop it more completely in the next section.

Example 16.1.5. The equation $2x = 3$ has a solution in the ring $[\mathbb{R}, +, \cdot]$ but does not have a solution in $[\mathbb{Z}, +, \cdot]$, since, to solve this equation, we multiply both sides of the equation $2x = 3$ by the multiplicative inverse of 2. This number, 2^{-1} exists in $\mathbb{R}$ but does not exist in $\mathbb{Z}$. We formalize this important idea in a definition which by now should be quite familiar to you.

Definition: Multiplicative Inverses. *Let $[R, +, \cdot]$ be a ring with unity,* 1. *If $u \in R$ and there exists an element $v \in R$ such that $u \cdot v = v \cdot u = 1$, then u is said to have a multiplicative inverse, v. We call a ring element that possesses a multiplicative inverse a unit of the ring. The set of all units of a ring R is denoted by U(R).*

By Theorem 11.3.2, the multiplicative inverse of a ring element is unique, if it exists. For this reason, we can use the notation u^{-1} for the multiplicative inverse of u, if it exists.

Example 16.1.6. In the rings $[\mathbb{R}, +, \cdot]$ and $[\mathbb{Q}, +, \cdot]$ every nonzero element has a multiplicative inverse. The only elements in $\mathbb{Z}$ that have multiplicative inverses are -1 and 1. That is, $U(\mathbb{R}) = \mathbb{R}^*$, $U(\mathbb{Q}) = \mathbb{Q}^*$, and $U(\mathbb{Z}) = \{-1, 1\}$.

Example 16.1.7. Let us find the multiplicative inverses, when they exist, of each element of the ring $[\mathbb{Z}_6 +_6, \times_6]$. If $u = 3$, we want an element v such that $u \times_6 v = 1$. We do not have to check whether $v \times_6 u = 1$ since $\mathbb{Z}_6$ is commutative. If we try each of the six elements, 0, 1, 2, 3, 4, and 5, of $\mathbb{Z}_6$, we find that none of them satisfies the above equation, so 3 does not have a multiplicative inverse in $\mathbb{Z}_6$. However, since $5 \times_6 5 = 1$, 5 does have a multiplicative inverse in $\mathbb{Z}_6$, namely itself: $5^{-1} = 5$. The following table summarizes all results for $\mathbb{Z}_6$.

u	u^{-1}
0	does not exist
1	1
2	does not exist
3	does not exist
4	does not exist
5	5

It shouldn't be a surprise that the zero of a ring is never going to have a multiplicative inverse except in the trivial case of $R = \{0\}$.

Isomorphism is a universal concept that is important in every algebraic structure. Two rings are isomorphic as rings if and only if they have the same cardinality and if they behave exactly the same under corresponding operations. They are essentially the same ring. For this to be true, they must behave the same as groups (under +) and they must behave the same under the operation of multiplication.

Definition: Ring Isomorphism. *Let $[R, +, \cdot]$ and $[R', +', \cdot']$ be rings. Then R is isomorphic to R' if and only if there exists a map, $f : R \to R'$, called a ring isomorphism, such that*

(1) f is one-to-one and onto,

(2) $f(a + b) = f(a) +' f(b)$ for all $a, b \in R$, and

(3) $f(a \cdot b) = f(a) \cdot' f(b)$ for all $a, b \in R$.

Conditions 1 and 2 tell us that f is a group isomorphism. Therefore, to show that two rings are isomorphic, we must produce a map, called an isomorphism, that satisfies the definition. Sometimes it is quite difficult to find a map that works. This does not necessarily mean that no such isomorphism exists, but simply that we cannot find it.

This leads us to the problem of how to show that two rings are not isomorphic. This is a universal concept. It is true for any algebraic structure and was discussed in Chapter 11. To show that two rings are not isomorphic, we must demonstrate that they behave differently under one of the operations. We illustrate through several examples.

Example 16.1.8. Consider the rings $[\mathbb{Z}, +, \cdot]$ and $[2\mathbb{Z}, +, \cdot]$. In Chapter 11 we showed that as groups, the two sets $\mathbb{Z}$ and $2\mathbb{Z}$ with addition were isomorphic. The group isomorphism that proved this was the map $f : \mathbb{Z} \to 2\mathbb{Z}$, defined by $f(n) = 2n$. Is f a ring isomorphism? We need only check whether $f(m \cdot n) = f(m) \cdot f(n)$ for all $m, n \in \mathbb{Z}$:

$f(m \cdot n) = 2 \cdot m \cdot n$ and

$f(m) \cdot f(n) = 2m \cdot 2n = 4 \cdot m \cdot n$

Therefore, f is not a ring isomorphism. This does not necessarily mean that the two rings $\mathbb{Z}$ and $2\mathbb{Z}$ are not isomorphic, but simply that the f doesn't satisfy the conditions. We could imagine that some other function does. We could proceed and try to determine another function f to see whether it is a ring isomorphism, or we could try to show that $\mathbb{Z}$ and $2\mathbb{Z}$ are not isomorphic as rings. To do the latter, we must find something different about the ring structure of $\mathbb{Z}$ and $2\mathbb{Z}$.

We already know that they behave identically under addition, so if they are different as rings, it must have something to do with how they behave under the operation of multiplication. Let's begin to develop a checklist of how the two rings could differ:

(1) Do they have the same cardinality? Yes, they are both countable.

(2) Are they both commutative? Yes.

(3) Are they both rings with unity? No.

$\mathbb{Z}$ is a ring with unity, namely the number 1. $2\mathbb{Z}$ is not a ring with unity, $1 \notin 2\mathbb{Z}$. Hence, they are not isomorphic as rings.

Example 16.1.9. Next consider whether $[2\mathbb{Z}, +, \cdot]$ and $[3\mathbb{Z}, +, \cdot]$ are isomorphic. Because of the previous example, we might guess that they are not. However, checklist items 1 through 3 above do not help us. Why? We add another checklist item:

(4) Find an equation that makes sense in both rings, which is solvable in one and not the other.

The equation $x + x = x \cdot x$, or $2x = x^2$, makes sense in both rings. However, this equation has a nonzero solution, $x = 2$, in $2\mathbb{Z}$, but does not have a nonzero solution in $3\mathbb{Z}$. Thus we have an equation solvable in one ring that cannot be solved in the other, so they cannot be isomorphic.

Another universal concept that applies to the theory of rings is that of a subsystem. A subring of a ring $[R, +, \cdot]$ is any nonempty subset S of R that is a ring under the operations of R. First, for S to be a subring of the ring R, S must be a subgroup of the group $[R, +]$. Also, S must be closed under $\cdot$, satisfy the associative law (under $\cdot$), and satisfy the distributive laws. But since R is a ring, the associative and distributive laws are true for every element in R, and, in particular, for all elements in S, since $S \subseteq R$. We have just proven the following theorem:

Theorem 16.1.1. *A subset S of a ring $[R, +, \cdot]$ is a subring of R if and only if:*

(1) $[5, +]$ is a subgroup of the group $[R, +]$, which by Theorem 11.5.1, means we must show:

(a) If $a, b \in S$, then $a + b \in S$,

(b) $0 \in S$, and

(c)) If $a \in S$, then $-a \in S$.

(2) S is closed under multiplication: if $a,\ b \in S$, then $a \cdot b \in S$.

Example 16.1.10. The set of even integers, $2\mathbb{Z}$, is a subring of the ring $[\mathbb{Z},\ +,\ \cdot]$ since $[2\mathbb{Z},\ +]$ is a subgroup of the group $[\mathbb{Z},\ +]$ and since it is also closed with respect to multiplication:

$$2m,\ 2n \in 2\mathbb{Z} \Rightarrow (2m)\cdot(2n) = 2(2\cdot m\cdot n) \in 2\mathbb{Z}.$$

Several of the basic facts that we are familiar with are true for any ring. The following theorem lists a few of the elementary properties of rings.

Theorem 16.1.2. *Let [R, +, -] be a ring, with $a, b \in R$. Then*

(1) $a \cdot 0 = 0 \cdot a = 0$

(2) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$

(3) $(-a) \cdot (-b) = a \cdot b$

Proof of Part 1:

$$\begin{aligned} a \cdot 0 &= a \cdot (0 + 0) \\ &= a \cdot 0 + a \cdot 0 \text{ by the left distributive law.} \end{aligned}$$

Hence if we add $-(a \cdot 0)$ to both sides of the above, we obtain $a \cdot 0 = 0$. Similarly, we can prove that $0 \cdot a = 0$.

Proof of Part 2: Before we begin the proof of part 2, recall that the inverse of each element of the group $[R,\ +]$ is unique. Hence the inverse of the element $a \cdot b$ is unique and it is denoted $-(a \cdot b)$.

Therefore, to prove that $a \cdot (—b) = -(a \cdot b)$, we need only show that $a \cdot (—b)$ inverts $a \cdot b$.

$$\begin{aligned} a\cdot(-b) + a\cdot b &= a\cdot(-b+b) && \text{by the distributive axiom} \\ &= a\cdot 0 && \text{since } -b \text{ inverts } b \\ &= 0 && \text{by part 1 of this theorem} \end{aligned}$$

Similarly, it can be shown that $(-a) \cdot b = -(a \cdot b)$. This completes the proof of part 2.

We leave the proof of part 3 to the reader (see Exercise 16 of this section). ■

Example 16.1.11. We will compute $2 \cdot (-2)$ in the ring $[\mathbb{Z}_6,\ +_6,\ \times_6]$.

$$2 \times_6 (-2) = -(2 \times_6 2) = -4 = 2,$$

since the additive inverse of 4 (mod 6) is 2. Of course, we could have done the calculation directly as

$$2 \times_6 (-2) = 2 \times_6 4 = 2.$$

As the example above illustrates, Theorem 16.1.2 is a modest beginning in the study of which algebraic manipulations are possible in the solution of problems in rings. A fact in elementary algebra that is used frequently in problem solving is the cancellation law. We know that the cancellation laws are true under addition for any ring (Theorem 11.3.5).

Are the cancellation laws true under multiplication? More specifically, let $[R,\ +,\ \cdot]$ be a ring and let $a,\ b,\ c \in R$ with a $\neq 0$. When can we cancel the a's in the equation $a \cdot b = a \cdot c$? We can certainly do so if a^{-1} exists, but we cannot assume that a has a multiplicative inverse. The answer to this question is found with the following definition and Theorem 16.1.3.

Definition: Divisors of Zero. *Let $[R,\ +,\ \cdot]$ be a ring. If a and b are two nonzero elements of R such that $a \cdot b = 0$, then a and b are called divisors of zero.*

Example 16.1.12 (a) In the ring $[\mathbb{Z}_8,\ +_8,\ \times_8]$, the numbers 4 and 2 are divisors of zero since $4 \times_8 2 = 0$. In addition, 6 is a divisor of zero because $6 \times_8 4 = 0$.

(b) In the ring $[M_{2\times 2}(\mathbb{R}),\ +,\ \cdot]$ the matrices $A = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ are divisors of zero since $A B = 0$.

Example 16.1.13. $[\mathbb{Z}, +, \cdot]$ has no divisors of zero.

Now here is why divisors of zero are related to cancellation.

Theorem 16.1.3. *The (multiplicative) cancellation law holds in a ring $[R,\ +,\ \cdot]$ if and only if R has no divisors of zero.*

We prove the theorem using the left cancellation law, namely that if $a \neq 0$ and $a \cdot b = a \cdot c$, then $b = c$ for all $a,\ b,\ c \in R$. The proof is similar using the right cancellation law.

Proof: (⇒) Assume the left cancellation law holds in R and assume that a and b are two elements in R such that $a \cdot b = 0$. We must show that either $a = 0$ or $b = 0$. To do this, assume that $a \neq 0$ and show that b must be 0.

$$\begin{aligned} a\cdot b = 0 &\Rightarrow a\cdot b = a\cdot 0 && \text{by Theorem 16.2.1, part 1} \\ &\Rightarrow b = 0 && \text{by the cancellation law} \end{aligned}$$

($\Leftarrow$) Conversely, assume that R has no divisors of 0 and we will prove that the cancellation law must hold. To do this, assume that $a, b, c \in R$, $a \neq 0$, such that $a \cdot b = a \cdot c$ and show that $b = c$.

$$\begin{aligned} a \cdot b = a \cdot c &\Rightarrow a \cdot b - a \cdot c = 0 \quad \text{Why?} \\ &\Rightarrow a \cdot (b - c) = 0 \quad \text{Why?} \\ &\Rightarrow b - c = 0 \quad \text{Why} \\ &\Rightarrow b = c \quad \blacksquare \end{aligned}$$

Hence, the only time that the cancellation laws hold in a ring is when there are no divisors of zero. The commutative rings with unity in which the above is true are given a special name.

Definition: Integral Domain. *A commutative ring with unity containing no divisors of zero is called an integral domain.*

In this chapter, Integral domains will be denoted generically by the letter D.

We state the following two useful facts without proof.

Theorem 16.1.4. *The element m in the ring $\mathbb{Z}_n$ is a divisor of zero if and only if m is not relatively prime to n (i.e., gcd$(m, n) \neq 1$).*

Corollary. *If p is a prime, then $\mathbb{Z}_p$ has no divisors of zero.*

Example 16.1.14. $[\mathbb{Z}, +, \cdot]$, $\left[\mathbb{Z}_p, +_p, \times_p\right]$ with p a prime, $[\mathbb{Q}, +, \cdot]$, $[\mathbb{R}, +, \cdot]$, and $[\mathbb{C}, +, \cdot]$ are all integral domains. The key example of an infinite integral domain is $[\mathbb{Z}, +, \cdot]$. In fact, it is from $\mathbb{Z}$ that the term integral domain is derived. The main example of a finite integral domain is $\left[\mathbb{Z}_p, +_p, \times_p\right]$, when p is prime.

We close this section with the verification of an observation that was made in Chapter 11, namely that the product of two algebraic systems may not be an algebraic system of the same type.

Example 16.1.15. Both $[\mathbb{Z}_2, +_2, \times_2]$ and $[\mathbb{Z}_3, +_3, \times_3]$ are integral domains. Consider the product $\mathbb{Z}_2 \times \mathbb{Z}_3$. It's true that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is a commutative ring with unity (see Exercise 13). However, $(1, 0) \cdot (0, 2) = (0, 0)$, so $\mathbb{Z}_2 \times \mathbb{Z}_3$ has divisors of zero and is therefore not an integral domain.

EXERCISES FOR SECTION 16.1

A Exercises

1. Review the definition of rings to show that the following are rings. The operations involved are the usual operations defined on the sets. Which

of these rings are commutative? Which are rings with unity? For the rings with unity, determine the unity and all units.

(a) $[\mathbb{Z}, +, \cdot]$

(b) $[\mathbb{C}, +, \cdot]$

(c) $[M_{n \times n}(\mathbb{R}), +, \cdot]$

(d) $[\mathbb{Q}, +, \cdot]$

(e) $[M_{2 \times 2}(\mathbb{R}), +, \cdot]$

(f) $[\mathbb{Z}_2, +_2, \times_2]$

2. Follow the instructions for Exercise 1 and the following rings:

(a) $[\mathbb{Z}_6, +_6, \times_6]$

(b) $[\mathbb{Z}_5, +_5, \times_5]$

(c) $\left[\mathbb{Z}_2{}^3, +, \cdot\right]$

(d) $[\mathbb{Z}_8, +_8, \times_8]$

(e) $[\mathbb{Z} \times \mathbb{Z}, +, \cdot]$

(f) $[\mathbb{R}^2, +, \cdot]$

3. Show that the following pairs of rings are not isomorphic:

(a) $[\mathbb{Z}, +, \cdot]$ and $[M_{2 \times 2}(\mathbb{Z}), +, \cdot]$

(b) $[3\,\mathbb{Z}, +, \cdot]$ and $[4\,\mathbb{Z}, +, \cdot]$.

4. Show that the following pairs of rings are not isomorphic:

(a) $[\mathbb{R}, +, \cdot]$ and $[\mathbb{Q}, +, \cdot]$.

(b) $[\mathbb{Z}_2 \times \mathbb{Z}_2, +, \cdot]$and $[\mathbb{Z}_4, +, \cdot]$.

5. (a) Show that $3\mathbb{Z}$ is a subring of the ring $[\mathbb{Z}, +, \cdot]$

(b) Find all subrings of $\mathbb{Z}_8$.

(c) Find all subrings of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

6. Verify the validity of Theorem 16.1.3 by finding examples of elements a, b, and c (a ≠ 0) in the following rings, where $a \cdot b = a \cdot c$ and yet $b \neq c$:

(a) $\mathbb{Z}_8$

(b) $M_{2\times2}(\mathbb{R})$

(c) $\mathbb{Z}_2{}^2$

7. (a) Determine all solutions of the equation $x^2 - 5x + 6 = 0$ in $\mathbb{Z}$. Can there be any more than two solutions to this equation (or any quadratic equation) in $\mathbb{Z}$?

(b) Find all solutions of the equation in part a in $\mathbb{Z}_{12}$. Why are there more than two solutions?

8. Solve the equation $x^2 + 4x + 4 = 0$ in the following rings. Interpret 4 as $1 + 1 + 1 + 1$, where 1 is the unity of the ring.

(a) in $\mathbb{Z}_8$

(b) in $M_{2\times2}(\mathbb{R})$

(c) in $\mathbb{Z}$

(d) in $\mathbb{Z}_3$

B Exercises

9. The relation "is isomorphic to" on rings is an equivalence relation. Explain the meaning of this statement.

10. Let $R_1, R_2, \ldots, R_n$ be rings. Prove the multiplicative, associative, and distributive laws for the ring

$$R = \underset{i=1}{\overset{n}{\times}} R_i$$

(a) If each of the R_i is commutative, is R commutative?

(b) Under what conditions will R be a ring with unity?

(c) What will the units of R be when it has a unity?

11. (a) Prove that the ring $\mathbb{Z}_2$ x $\mathbb{Z}_3$ is commutative and has unity.

(b) Determine all divisors of zero for the ring $\mathbb{Z}_2$ x $\mathbb{Z}_3$.

(c) Give another example illustrating the fact that the product of two integral domains may not be an integral domain. Is there an example where the product is an integral domain?

12. **Boolean Rings.** Let U be a nonempty set.

(a) Verify that $[\mathcal{P}(U), \oplus, \cap]$ is a commutative ring with unity.

(b) What are the units of this ring?

13. (a) For any ring $[R, +, \cdot]$, expand $(a + b)(c + d)$ for $a, b, c, d \in R$.

(b) If R is commutative, prove that $(a + b)^2 = a^2 + 2ab + b^2$ for all $a, b \in R$.

14. (a) Let R be a commutative ring with unity. Prove by induction that for $n \geq 1$,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

(b) Simplify $(a + b)^5$ in $\mathbb{Z}_5$.

(c) Simplify $(a + b)^{10}$ in $\mathbb{Z}_{10}$.

15. Prove: If R is a ring with unity then this unity is unique.

16. Prove part 3 of Theorem 16.1.2.

17. Prove the Corollary to Theorem 16.1.4.

18. Let U be a finite set. Prove that the Boolean ring $[\mathcal{P}(U), \oplus, \cap]$ is isomorphic to the ring $[\mathbb{Z}_2{}^n, +, \cdot]$. where $n = |U|$

16.2 Fields

Although the algebraic structures of rings and integral domains are widely used and play an important part in the applications of mathematics, we still cannot solve the simple equation ax = b, a ≠ 0 in all rings or in all integral domains. Yet this is one of the first equations we learn to solve in elementary algebra and its solubility is basic to innumerable questions. Certainly, if we wish to solve a wide range of problems in a system we need at least all of the laws true for rings and the cancellation laws together with the ability to solve the equation ax = b, a =£ 0. We summarize the above in a definition and list several theorems without proof that will place this concept in the context of the previous section.

Definition: Field. A field is a commutative ring with unity such that each nonzero element has a multiplicative inverse.

In this chapter, we denote a field generically by the letter F. The letters k, K and L are also conventionally used for fields.

Example16.2.1. $[\mathbb{Q}, +, \cdot]$, $[\mathbb{R}, +, \cdot]$, and $[\mathbb{C}, +, \cdot]$ are all fields.

Reminder: Since every field is a ring, all facts and concepts that are true for rings are true for any field.

***Theorem 16.2.1**. Every field is an integral domain.*

Of course the converse of Theorem 16.2.1 is not true. Consider $[\mathbb{Z}, +, \cdot]$.

***Theorem 16.2.2.** Every finite integral domain is a field.*

***Theorem 16.2.3.** If p is a prime, then $\mathbb{Z}_p$ is a field.*

Theorem 16.2.3 is immediate from Theorem 16.2.2.

Theorem 16.2.1 reminds us that the cancellation laws must be true for any field. Theorem 16.2.3 gives us a large number of finite fields, but we must be cautious. This theorem does not tell us that all finite fields are of the form $\mathbb{Z}_p$, p a prime. To see this, let's try to construct a field of order 4.

Example 16.2.2: a field of order 4. First the field must contain the additive and multiplicative identities, 0 and 1, so, without loss of generality, we can assume that the field we are looking for is of the form $F = \{0, 1, a, b\}$. Since there are only two nonisomorphic groups of order 4, we have only two choices for the group table for $[F, +]$. If the additive group is isomorphic to $\mathbb{Z}_4$ then two of the nonzero elements of F would not be their own additive inverse (as are 1 and 3 in $\mathbb{Z}_4$). Lets assume $\beta \in F$ is one of those elements and $\beta + \beta = \gamma \neq 0$. An isomorphism between the additive groups F and $\mathbb{Z}_4$ would require that γ in F correspond with 2 in $\mathbb{Z}_4$. We could continue our argument and infer that $\gamma \cdot \gamma = 0$, producing a zero divisor, which we need to avoid if F is to be a field. We leave the remainder of the argument to the reader. We can thus complete the addition table so that $[F, +]$ is isomorphic to $\mathbb{Z}_2{}^2$:

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

Next, by Theorem 16.1.2, Part 1, and since 1 is the unity of F, the table for multiplication must look like:

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	–	–
b	0	b	–	–

Hence, to complete the table, we have only four entries to find, and, since F must be commutative, this reduces our task to filling in three entries. Next, each nonzero element of F must have a unique multiplicative inverse. The inverse of a must be either a itself or b. If $a^{-1} = a$, then $b^{-1} = b$. (Why?) But

$a^{-1} = a \Rightarrow a \cdot a = 1$. And if $a \cdot a = 1$, then $a \cdot b$ is equal to a or b. In either case, by the cancellation law, we obtain $a = 1$ or $b = 1$, which is impossible. Therefore we are forced to conclude that $a^{-1} = b$ and $b^{-1} = a$. To determine the final two products of the table, simply note that, $a \cdot a \neq a$ because the equation $x^2 = x$ has only two solutions, 0 and 1 in any field. We also know that $a \cdot a$ cannot be 1 because a doesn't invert itself and cannot be 0 because a can't be a zero divisor. This leaves us with one possible conclusion, that $a \cdot a = b$ and similarly $b \cdot b = a$. Hence, our multiplication table for F is:

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

The table listing the multiplicative inverse of each nonzero element is:

u	u^{-1}
1	1
a	b
b	a

We leave it to the reader to convince him- or herself, if it is not already clear, that $[F, +, \cdot]$, as described above, is a field. Hence, we have produced a field of order 4 and 4 is not a prime.

This construction would be difficult to repeat for larger fields. In section 16.4 we will introduce a different approach to constructing fields that will be far more efficient.

Even though not all finite fields are isomorphic to $\mathbb{Z}_p$, for some prime p it can be shown that every field F must have either:

(1) a subfield isomorphic to $\mathbb{Z}_p$ for some prime p, or

(2) a subfield isomorphic to $\mathbb{Q}$.

In particular, if F is a finite field, a subfield of F must exist that is isomorphic to $\mathbb{Z}_p$. One can think of all fields as being constructed from either $\mathbb{Z}_p$ or $\mathbb{Q}$.

Example 16.2.3. $[\mathbb{R}, +, \cdot\ ]$ is a field, and it contains a subfield isomorphic to $[\mathbb{Q}, +, \cdot]$, namely $\mathbb{Q}$ itself.

Example 16.2.4. The field F that we constructed in Example 16.2.2 should have a subfield isomorphic to $\mathbb{Z}_p$ for some prime p. From the tables, we note that the subset $\{0, 1\}$ of $\{0, 1, a, b\}$ under the given operations of F behaves exactly like $[\mathbb{Z}_2, +_2, \times_2]$. Hence, the field in Example 16.2.2 has a subfield isomorphic to $\mathbb{Z}_2$. Does it have a subfield isomorphic to a larger field, say $\mathbb{Z}_3$? We claim not and leave this investigation to the reader (see Exercise 3 of this section).

We close this section with a brief discussion of isomorphic fields. Again, since a field is a ring, the definition of isomorphism of fields is the same as that of rings. It can be shown that if f is a field isomorphism, then $f(a^{-1}) = f(a)^{-1}$; that is, inverses are mapped onto inverses under any field isomorphism. A major question to try to solve is: How many different non-isomorphic finite fields are there of any given order? If p is a prime, it seems clear from our discussions that all fields of order p are isomorphic to $\mathbb{Z}_p$. But how many nonisomorphic fields are there, if any, of order 4, 6, 8, 9, etc? The answer is given in the following theorem, whose proof is beyond the scope of this text.

Theorem 16.2.4.

(1) Any finite field F has order p^n for a prime p and a positive integer n.

(2) For any prime p and any positive integer n there is a field of order p^n .

(3) Any two fields of order p^n are isomorphic. This field of order p^n is frequently referred to as the Galois field of order p^n and it is designated by $GF(p^n)$.

Evariste Galois (1811-32) was a pioneer in the field of abstract algebra.

A French stamp honoring Evariste Galois (1811-32)

Theorem 16.2.4 tells us that there is a field of order $2^2= 4$, and there is only one such field up to isomorphism. That is, all such fields of order 4 are isomorphic to F, which we constructed in Example 16.2.2.

EXERCISES FOR SECTION 16.2

A Exercises

1. Write out the addition, multiplication, and "inverse" tables for each of the following fields'.

(a) $[\mathbb{Z}_2, +_2, \times_2]$

(b) $[\mathbb{Z}_3, +_3, \times_3]$

(c) $[\mathbb{Z}_5, +_5, \times_5]$

2. Show that the set of units of the fields in Exercise 1 form a group under the operation of the multiplication of the given field. Recall that a unit is an element which has a multiplicative inverse.

3. Complete the argument in Example 16.2.2 to show that if $[F, +]$ is isomorphic to $\mathbb{Z}_4$, then F would have a zero divisor.

4. Write out the operation tables for $\mathbb{Z}_2{}^2$. Is $\mathbb{Z}_2{}^2$ a ring? An integral domain? A field? Explain.

5. Determine all values x from the given field that satisfy the given equation:

(a) $x + 1 = -1$ over $\mathbb{Z}_2$, $\mathbb{Z}_3$ and $\mathbb{Z}_5$

(b) $2x + 1 = 2$ over $\mathbb{Z}_3$ and $\mathbb{Z}_5$

(c) $3x + 1 = 2$ over $\mathbb{Z}_5$

6. (a) Prove that if p and q are prime, then $\mathbb{Z}_p \times \mathbb{Z}_q$, is never a field.

(b) Can $\mathbb{Z}_p{}^n$ be a field for any prime p and any positive integer $n \geq 2$?

7. The following are equations over $\mathbb{Z}_2$. Their coefficients come solely from $\mathbb{Z}_2$. Determine all solutions over $\mathbb{Z}_2$; that is, find all numbers in $\mathbb{Z}_2$ that satisfy the equations:

(a) $x^2 + x = 0$

(b) $x^2 + 1 = 0$

(c) $x^3 + x^2 + x + 1 = 0$

(d) $x^3 + x + 1 = 0$

8. Determine the number of different fields, if any, of all orders 2 through 15. Wherever possible, describe these fields via a known field.

B Exercise

9. Let $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

(a) Prove that $[\mathbb{Q}(\sqrt{2}), +, \cdot]$ is a field.

(b) Show that $\mathbb{Q}$ is a subfield of $\mathbb{Q}(\sqrt{2})$. For this reason, $\mathbb{Q}(\sqrt{2})$ is called an extension field of $\mathbb{Q}$.

(c) Show that all the roots of the equation $x^2 - 2 = 0$ lie in the extension field $\mathbb{Q}(\sqrt{2})$.

(d) Do the roots of the equation $x^2 - 3 = 0$ lie in this field? Explain.

16.3 Polynomial Rings

In the previous sections we examined the solutions of a few equations over different rings and fields. To solve the equation $x^2 - 2 = 0$ over the field of the real numbers means to find all solutions of this equation that are in this particular field $\mathbb{R}$. This statement can be replaced as follows: Determine all $a \in \mathbb{R}$ such that the polynomial $f(x) = x^2 - 2$ is equal to zero when evaluated at $x = a$. In this section, we will concentrate on the theory of polynomials. We will develop concepts using the general setting of polynomials over rings since results proven over rings are true for fields (and integral domains). The reader should keep in mind that in most cases we are just formalizing concepts that he or she learned in high school algebra over the field of reals.

Definition: Polynomial over R. *Let $[R, +, \cdot]$ be a ring. A polynomial, $f(x)$, over R is an expression of the form*

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \ , \ n \geq 0,$$

where $a_0, a_1, a_2, \ldots, a_n \in R$. If $a_n \neq 0$, then the degree of $f(x)$ is n, If f(x) = 0, then the degree of f(x) is undefined and we assign the value $-\infty$ to the degree. If the degree of f(x) is n, we write deg $f(x) = n$.

Comments:

(1) The symbol x is an object called an *indeterminate*, which is not an element of the ring R.

(2) The set of all polynomials in the indeterminate x with coefficients in R is denoted by $R[x]$.

(3) Note that $R \subseteq R[x]$, The elements of R are called *constant polynomials*, with the nonzero elements of R being the polynomials of degree 0.

(4) R is called the *ground ring* for $R[x]$.

(5) In the definition above, we have written the terms in increasing degree starting with the constant. The ordering of terms can be reversed without changing the polynomial. For example, $1 + 2x - 3x^4$ and $-3x^4 + 2x + 1$ are the same polynomial.

(6) A term of the form x^k in a polynomial is understood to be $1 x^k$,

Example 16.3.1. $f(x) = 3$, $g(x) = 2 - 4x + 7x^2$, and $h(x) = 2 + x^4$ are all polynomials in $\mathbb{Z}[x]$. Their degrees are 0, 2, and 4, respectively.

Addition and multiplication of polynomials are performed as in high school algebra. However, we must do our computations in the ground ring over which we are considering the polynomials.

Example 16.3.2. In $\mathbb{Z}_3[x]$, if $f(x) = 1 + x$ and $g(x) = 2 + x$, then

$$\begin{aligned} f(x) + g(x) &= (1 + x) + (2 + x) \\ &= (1 +_3 2) + (1 +_3 1)x \\ &= 0 + 2x \\ &= 2x \end{aligned}$$

and

$$\begin{aligned} f(x)g(x) &= (1 + x) \cdot (2 + x) \quad . \\ &= (1 + x) \cdot 2 + (1 + x) \cdot x \\ &= 1 \times_3 2 + 2x + 1x + x \cdot x \\ &= 2 + (2 +_3 1)x + x^2 \\ &= 2 + x^2 \end{aligned}$$

However, for the same polynomials as above, $f(x)$ and $g(x)$ in $\mathbb{Z}$[x], we have

$$\begin{aligned} f(x) + g(x) &= (1 + x) + (2 + x) \\ &= (1 + 2) + (1 + 1)x \\ &= 3 + 2x \end{aligned}$$

and

$$\begin{aligned} f(x)g(x) &= (1 + x) \cdot (2 + x) \quad . \\ &= (1 + x) \cdot 2 + (1 + x) \cdot x \\ &= 1 \cdot 2 + 2x + 1x + x \cdot x \\ &= 2 + (2 + 1)x + x^2 \\ &= 2 + 3x + x^2 \end{aligned}$$

The important fact to keep in mind is that addition and multiplication in $R[x]$ depends on addition and multiplication in R. The x's merely serve the purpose of "place holders." All computations are done over the given ring. We summarize in the following theorem:

Theorem 16.3.1. *Let [R, +, ·] be a ring. Then:*

(1) R[x] is a ring under the operations of polynomial addition and multiplication, which depend on (are induced by) the operations in R.

(2) If R is a commutative ring, then R[x] is a commutative ring.

(3) If R is a ring with unity, 1, *then R[x] is a ring with unity (the unity in R[x] is* $1 + 0\,x + 0\,x^2 + \cdots$*).*

(4) If R is an integral domain, then R[x] is an integral domain.

(5) If F is a field, then F[x] is not a field. However, F[x] is an integral domain.

The proofs for Parts 1 through 4 are not difficult but rather long, so we omit them. For those inclined to prove them, we include the formal definitions of addition and multiplication in $R[x]$ below.

Proof Of Part 5: $F[x]$ is not a field since for $x \in F[x]$, $x^{-1} = 1/x \notin F[x]$. Hence not all nonzero elements in $F[x]$ have multiplicative inverses in $F[x]$. Every field F is an integral domain. By Part 4, $F[x]$ is an integral domain. ■

Definition: Addition in R[x]. *Let* $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m$ *and* $g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n$ *be elements in R[x] so that* $a_i \in R$ *and* $b_i \in R$ *for all i. Let k be the maximum of m and n. Then*

$$f(x) + g(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_k x^k$$

where $c_i = a_i + b_i$ *for* $i = 0, 1, 2, \ldots, k$.

Definition: Multiplication in R[x]. *Let f (x) and g (x) be as above. Then*

$$f(x) \cdot g\{x) = d_0 + d_1 x + d_2 x^2 + \cdots + d_p x^p \text{ where}$$

$p = m + n$, *and*

$$\begin{aligned} d_s &= \sum_{i=0}^{s} a_i b_{s-i} \\ &= a_0 b_s + a_1 b_{s-1} + a_2 b_{s-2} + \cdots + a_{s-1} b_1 + a_s b_0 \end{aligned}$$

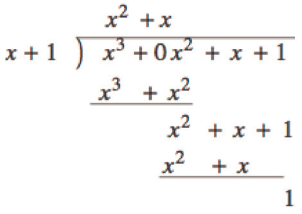
for $0 \le s \le p$.

Example 16.3.3. Let $f(x) = 2 + x^2$ and $g(x) = -1 + 4x + 3x^2$. We will compute $f(x) \cdot g(x)$ in $\mathbb{Z}[x]$. Of course this product can be obtained by the usual methods of high school algebra. We will, for illustrative purposes, use the above definition. Using the notation of the above definition, $a_0 = 2$, $a_1 = 0$, $a_2 = 1$, $b_0 = -1$, $b_1 = 4$, and $b_2 = 3$. We want to compute the coefficients d_0, d_1, d_2, d_3, and d_4 . We will compute d_3 , the coefficient of the x^3 term of the product, and leave the remainder to the reader (see Exercise 2 of this section). Since the degrees of both factors is 2, $a_i = b_i = 0$ for $i \ge 3$.

$$\begin{aligned} d_3 &= a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 \\ &= 2\cdot 0 + 0\cdot 3 + 1\cdot 4 + 0\cdot(-1) = 4 \end{aligned}$$

From high school algebra we all learned the standard procedure for dividing a polynomial $f(x)$ by a second polynomial $g(x)$. This process of polynomial long division is referred to as the division property for polynomials. Under this scheme we continue to divide until the result is a quotient $q(x)$ and a remainder $r(x)$ whose degree is strictly less than that of the divisor $g(x)$. This property is valid over any field.

Example 16.3.4. Let $f(x) = 1 + x + x^3$ and $g(x) = 1 + x$ be two polynomials in $\mathbb{Z}_2[x]$. Let us divide $f(x)$ by $g(x)$. Keep in mind that we are in $\mathbb{Z}_2[x]$ and that, in particular, $-1 = 1$ in $\mathbb{Z}_2$. This is a case where reordering the terms in decreasing degree is preferred.



$$\begin{array}{r l} & x^2 + x \\ x+1 \;\big) & x^3 + 0x^2 + x + 1 \\ & \underline{x^3 + x^2} \\ & \quad x^2 + x + 1 \\ & \quad \underline{x^2 + x} \\ & \qquad\qquad 1 \end{array}$$

Therefore,

$$\frac{x^3 + x + 1}{x + 1} = x^2 + x + \frac{1}{x + 1}$$

or equivalently,

$$x^3 + x + 2 = (x^2 + x)\cdot(x + 1) + 1$$

That is $f(x) = g(x)\cdot q(x) + r(x)$ where $q(x) = x^2 + x$ and $r(x) = 1$. Notice that $\deg(r(x)) = 0$, which is strictly less than the $\deg(g(x)) = 1$.

Example 16.3.5. Let $f(x) = 1 + x^4$ and $g(x) = 1 + x$ be polynomials in $\mathbb{Z}_2[x]$. Let us divide f(x) by g(x):

$$\begin{array}{rllllll}
 & & x^3 & +\;x^2 & +x & +1 \\
x+1\,\big) & x^4 & +\,0x^3 & +\,0x^2 & +\,0x & +\,1 \\
 & \underline{x^4} & \underline{+\,x^3} & & & \\
 & & x^3 & & & +\,1\\
 & & \underline{x^3} & \underline{+\,x^2} & & \\
 & & & x^2 & & +\,1 \\
 & & & \underline{x^2} & \underline{+\,x} & \\
 & & & & x & +\,1\\
 & & & & \underline{x} & \underline{+\,1}\\
 & & & & & 0
\end{array}$$

Thus $x^4 + 1 = (x^3 + x^2 + x + 1)(x + 1)$.

Since we have 0 as a remainder, $x + 1$ must be a factor of $x^4 + 1$, as in high school algebra. Also, since $x + 1$ is a factor of $x^4 + 1$, 1 is a zero (or root) of $x^4 + 1$. Of course we could have determined that 1 is a root of $f(x)$ simply by computing $f(1) = 1^4 +_2 1 = 1 +_2 1 = 0$.

Before we summarize the main results suggested by the previous examples, we should probably consider what could have happened if we had performed divisions of polynomials in the ring $\mathbb{Z}$[x] rather than over the field $\mathbb{Z}_2$. For example, $f(x) = x^2 - 1$ and $g(x) = 2x - 2$ are both elements of the ring $\mathbb{Z}$[x], yet

$$\frac{x^2+1}{2x-1} = \frac{1}{2}x + \frac{1}{2}$$

The quotient is not a polynomial over $\mathbb{Z}$ but a polynomial over the field $\mathbb{Q}$. For this reason it would be wise to describe all results over a field F rather than over an arbitrary ring R.

Theorem 16.3.2. Division Property for F[x]. *Let* $[F, +, \cdot]$ *be a field and let* $f(x)$ *and* $g(x)$ *be two elements of* $F[x]$ *with* $g(x) \neq 0$. *Then there exist unique polynomials* $q(x)$ *and* $r(x)$ *in* $F[x]$ *such that* $f(x) = g(x)\,q(x) + r(x)$, *where* $\deg r(x) < \deg g(x)$.

Theorem 16.3.2 can be proven by induction on $\deg f(x)$.

Theorem 16.3.3. *Let* $[F, +, \cdot]$ *be a field. An element* $a \in F$ *is a zero of* $f(x) \in F[x]$ *if and only if* $x - a$ *is a factor of* $f(x)$ *in* $F[x]$.

Proof: ($\Rightarrow$) Assume that $a \in F$ is a zero of $f(x) \in F[x]$. We wish to show that $x - a$ is a factor of $f(x)$. To do so, apply the division property to $f(x)$ and $g(x) = x - a$. Hence, there exist unique polynomials $q(x)$ and $r(x)$ from $F[x]$ such that $f(x) = (x - a)\cdot q(x) + r(x)$ and the $\deg r(x) < \deg(x - a) = 1$, so $r(x) = c \in F$, that is, $r(x)$ is a constant. Also a is a zero of $f(x)$ mean $f(a) = 0$. So $f(x) = (x - a)\cdot q(x) + c$ becomes $0 = f(a) = (a - a)q(a) + c$. Hence $c = 0$, so $f(x) = (x - a)\cdot q(x)$, and $x - a$ is a factor of $f(x)$. The reader should note that a critical point of the proof of this half of the theorem was the part of the division property that stated that $\deg r(x) < \deg g(x)$.

($\Leftarrow$) We leave this half to the reader, exercise 6. ■

Theorem 16.3.4. *A nonzero polynomial* $f(x) \in F[x]$ *of degree n can have at most n zeros.*

Proof: Let $a \in F$ be a zero of $f(x)$. Then $f(x) = (x - a)\cdot q_1(x)$, $q_1(x) \in F[x]$, by Theorem 16.3.3. If $b \in F$ is a zero of $q_1(x)$, then again by Theorem 16.3.3, $f(x) = (x - a)(x - b)\,q_2(x)$, $q_2(x) \in F[x]$. Continue this process, which must terminate in at most n steps since the degree of $q_k(x)$ would be $n - k$. ■

From Theorem 16.3.3 we can obtain yet another insight into the problems associated with solving polynomial equations; that is, finding the zeros of a polynomial. The theorem states that an element $a \in F$ is a zero of $f(x) \in F[x]$ if and only if $x - a$ is a factor of $f(x)$. The initial important idea here is that the zero a is from the ground field F. Second, a is a zero only if $(x - a)$ is a factor of $f(x)$ in $F[x]$ —that is, only when $f(x)$ can be factored (or reduced) to the product of $(x - a)$ times some other polynomial in $F[x]$.

Example 16.3.6. Consider the polynomial $f(x) = x^2 - 2$ taken as being in $\mathbb{Q}$[x]. From high school algebra we know that $f(x)$ has two zeros (or roots), namely $\pm\sqrt{2}$, and $x^2 - 2$ can be factored (reduced) as $\left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)$. However, we are working in $\mathbb{Q}[x]$, these two factors are not in the set of polynomials over the rational numbers, $\mathbb{Q}$ since $\sqrt{2} \notin \mathbb{Q}$. Therefore, $x^2 - 2$ does not have a zero in $\mathbb{Q}$ since it cannot be factored over $\mathbb{Q}$. When this happens, we say that the polynomial is irreducible over $\mathbb{Q}$.

The problem of factoring polynomials is tied hand-in-hand with that of the reducibility of polynomials. We give a precise definition of this concept.

Definition: Irreducible over F. *Let[F, +, ·] be a field and let f(x) ∈ F[x] be a nonconstant polynomial, f(x)) is irreducible over F if and only if f(x) cannot be expressed as a product of two (or more) polynomials, both from F[x] and both of degree lower than that of f(x).*

A polynomial is *reducible over F* if it is not irreducible over *F*.

Example 16.3.7. The polynomial $f(x) = x^4 + 1$ of Example 16.3.5 is reducible over $\mathbb{Z}_2$ since $x^4 + 1 = (x + 1)(x^3 + x^2 + x - 1)$.

Example 16.3.8. Is the polynomial $f(x) = x^3 + x + 1$ of Example 16.3.4 reducible over $\mathbb{Z}_2$? From Example 16.3.4 we know that $x + 1$ is not a factor of $x^3 + x + 1$, and from high school algebra we realize that a cubic (also second-degree) polynomial is reducible if and only if it has a linear (first-degree) factor. (Why?) Does $f(x) = x^3 + x + 1$ have any other linear factors? Theorem 16.3.1 gives us a quick way of determine this since $x - a$ is a factor of $x^3 + x + 1$ over $\mathbb{Z}_2$ if and only if a $\in \mathbb{Z}_2$ is a zero of $x^3 + x + 1$. So $x^3 + x + 1$ is reducible over $\mathbb{Z}_2$ if and only if it has a zero in $\mathbb{Z}_2$. Since $\mathbb{Z}_2$ has only two elements, 0 and 1, this is easy enough to check.

$f(0) = 0^3 +_2 0 +_2 1 = 1$ and

$f(1) = 1^3 +_2 1 +_2 1 = 1$

so neither 0 nor 1 is a zero of $f(x)$ over $\mathbb{Z}_2$. Hence, $x^3 + x + 1$ is irreducible over $\mathbb{Z}_2$.

From high school algebra we know that $x^3 + x + 1$ has three zeros from some field. Can we find this field? To be more precise, can we construct (find) the field which contains $\mathbb{Z}_2$ and all zeros of $x^3 + x + 1$? We will consider this task in the next section.

We close this section with a final analogy. Prime numbers play an important role in mathematics. The concept of irreducible polynomials (over a field) is analogous to that of a prime number. Just think of the definition of a prime number. A useful fact concerning primes is: If p is a prime and if $p \mid a\,b$, then $p \mid a$ or $p \mid b$. We leave it to the reader to think about the veracity of the following: If $p(x)$ is an irreducible polynomial over F, $a(x)$, $b(x) \in F[x]$ and $p(x) \mid a(x)\,b(x)$, then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.

EXERCISES FOR SECTION 16.3

A Exercises

1. Let $f(x) = 1 + x$ and $g(x) = 1 + x + x^2$. Compute the following sums and products in the indicated rings.

   (a) $f(x) + g(x)$ and $f(x) \cdot g(x)$ in $\mathbb{Z}[x]$

   (b) $f(x) + g(x)$ and $f(x) \cdot g(x)$ in $\mathbb{Z}_2$[x]

   (c) $(f(x) \cdot g(x)) \cdot f(x)$ in $\mathbb{Z}$[x]

   (d) $(f(x) \cdot g(x)) \cdot f(x)$ in $\mathbb{Z}_2[x]$

   (e) $f(x) \cdot f(x) + f(x) \cdot g(x)$ in $\mathbb{Z}_2[x]$

2. Complete Example 16.3.3.

3. Prove that:

   (a) The ring $\mathbb{R}$ is a subring of the ring $\mathbb{R}[x]$.

   (b) The ring $\mathbb{Z}[x]$ is a subring of the $\mathbb{Q}[x]$.

   (c) The ring $\mathbb{Q}[x]$ is a subring of the ring $\mathbb{R}[x]$.

4. (a) Find all zeros of $x^4 + 1$ in $\mathbb{Z}_3$. (b) Find all zeros of $x^5 + 1$ in $\mathbb{Z}_5$.

5. Determine which of the following are reducible over $\mathbb{Z}_2$. Explain.

   (a) $f(x) = x^3 + 1$

   (b) $g(x) = x^3 + x^2 + x$.

   (c) $h(x) = x^3 + x^2 + 1$.

   (d) $k(x) = x^4 + x^2 + 1$. (Be careful.)

6. Prove the second half of Theorem 16.3.3.

7. Give an example of the contention made in the last paragraph of this section.

8. Determine all zeros of $x^4 + 3x^3 + 2x + 4$ in $\mathbb{Z}_5[x]$

9. Show that $x^2 - 3$ is irreducible over $\mathbb{Q}$ but reducible over the field of real numbers.

B Exercises

10. The definition of a vector space given in Chapter 13 holds over any field F, not just over the field of real numbers, where the elements of F are called scalars.

    (a) Show that $F[x]$ is a vector space over F.

    (b) Find a basis for $F[x]$ over F.

    (c) What is the dimension of F[x] over F?

11. Prove Theorem 16.3.2.

    (a) Show that the field $\mathbb{R}$ of real numbers is a vector space over $\mathbb{R}$. Find a basis for this vector space. What is dim $\mathbb{R}$ over $\mathbb{R}$?

(b) Repeat part a for an arbitrary field F.

(c) Show that $\mathbb{R}$ is a vector space over $\mathbb{Q}$.

16.4 Field Extensions

From high school algebra we realize that to solve a polynomial equation means to find its roots (or, equivalently, to find the zeros of the polynomials). From Example 16.3.5 of the previous section we know that the zeros may not lie in the given ground field. Hence, to solve a polynomial really involves two steps: first, find the zeros, and second, find the field in which the zeros lie. For economy's sake we would like this field to be the smallest field that contains all the zeros of the given polynomial. To illustrate this concept, let us reconsider Example 16.3.5.

Example 16.4.1. Let $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. It is important to remember that we are considering $x^2 - 2$ over $\mathbb{Q}$, no other field. We would like to find all zeros of $f(x)$ and the smallest field, call it S for now, that contains them. The zeros are $x = \pm\sqrt{2}$, neither of which is an element of $\mathbb{Q}$. The set S we are looking for must satisfy the conditions:

(1) S be a field.

(2) S must contain $\mathbb{Q}$ as a subfield,

(3) S must contain all zeros of $f(x) = x^2 - 2$, and

By condition (3), $\sqrt{2}$ must be an element of S, and, if S is to be a field, the sum, product, difference, and quotient of elements in S must be in S. So $\sqrt{2}$, $\left(\sqrt{2}\right)^2$, $\left(\sqrt{2}\right)^3, \ldots$, $\sqrt{2} + \sqrt{2}$, $\sqrt{2} - \sqrt{2}$, and $\sqrt{2} \big/ \sqrt{2}$ must all be elements of S. Further, since S contains $\mathbb{Q}$ as a subset, any element of $\mathbb{Q}$ combined with $\sqrt{2}$ under any field operation must be an element of S. Hence, every element of the form $a + b\sqrt{2}$, where a and b can be any elements in $\mathbb{Q}$, is an element of S. We leave to the reader to show that S is a field (see Exercise 1 of this section). We note that the second zero of $x^2 - 2$, namely $-\sqrt{2}$, is an element of S. To see this, simply take $a = 0$ and $b = -1$. The field S is frequently denoted as $\mathbb{Q}\left(\sqrt{2}\right)$, and it is referred to as an extension field of $\mathbb{Q}$. Note that the polynomial $x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)$ factors into linear factors, or *splits*, in $\mathbb{Q}\left(\sqrt{2}\right)[x]$; that is, all coefficients of both factors are elements of the field $\mathbb{Q}\left(\sqrt{2}\right)$.

Example 16.4.2. Consider the polynomial $g(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Let's repeat the previous example for $g(x)$ over $\mathbb{Z}_2$. First, $g(0) = 1$ and $g(l) = 1$, so none of the elements of $\mathbb{Z}_2$ are zeros of $g(x)$. Hence, the zeros of $g(x)$ must lie in an extension field of $\mathbb{Z}_2$. By Theorem 16.3.3, $g(x) = x^2 + x + 1$ can have at most two zeros. Let a be a zero of $g(x)$. Then the extension field S of $\mathbb{Z}_2$ must contain $a \cdot a = a^2, a^3, a + a, a + 1$, and so on. But, since $g(a) = 0$, we have $a^2 + a + 1 = 0$, or, equivalently, $a^2 = -(a + 1) = a + 1$ (remember, we are working in an extension of $\mathbb{Z}_2$). Note the recurrence relation we can use to reduce powers of a.

So far our extension field S of $\mathbb{Z}_2$ is the set $\{0, 1, a, a + 1\}$. For S to be a field, all possible sums, products, differences, and quotients of elements in S must be in S. Let's try a few:

$$a + a = a(1 +_2 1) = a \cdot 0 = 0 \in S$$

Since $a + a = 0$, $-a = a$, which is in S. Adding three a's together doesn't give us anything new: $a + a + a = a \in S$ In fact, $n a$ is in S for all possible positive integers n. Next,

$$\begin{aligned} a^3 &= a^2 \cdot a \\ &= (a + 1) \cdot a \\ &= a^2 + a \\ &= (a + 1) + a \\ &= 1 \in S \end{aligned}$$

Therefore, $a^{-1} = a + 1$ and $(a + 1)^{-1} = a$.

It is not difficult to see that a^n is in S for all positive n. Does S contain all zeros of $x^2 + x + 1$? Remember, $g(x)$ can have at most two distinct zeros and we called one of them a, so if there is a second, it must be $a + 1$. To see if $a + 1$ is indeed a zero of $g(x)$, simply compute $f(a + 1)$:

$$\begin{aligned} f(a + 1) &= (a + 1)^2 + (a + 1) + 1 \\ &= a^2 + 1 + a + 1 + 1 \\ &= a^2 + a + 1 \\ &= 0 \end{aligned}$$

Therefore, $a + 1$ is also a zero of $x^2 + x + 1$. Hence, $S = \{0, 1, a, a + 1\}$ is the smallest field that contains $\mathbb{Z}_2 = \{0, 1\}$ as a subfield and all zeros of $x^2 + x + 1$. This extension field is denoted by $\mathbb{Z}_2(a)$. Note that $x^2 + x + 1$ splits in $\mathbb{Z}_2(a)$; that is, it factors into linear factors in $\mathbb{Z}_2(a)$. We also observe that $\mathbb{Z}_2(a)$ is a field containing exactly four elements. By Theorem 16.2.4, we expected that $\mathbb{Z}_2(a)$ would be of order p^2 for some prime p and positive integer n. Also recall that all fields of order p^n are isomorphic. Hence, we have described all fields of order $2^2 = 4$ by finding the extension field of a polynomial that is irreducible over $\mathbb{Z}_2$.

The reader might feel somewhat uncomfortable with the results obtained in Example 16.4.2. In particular, what is a? Can we describe it through a known quantity? All we know about a is that it is a zero of $g(x)$ and that $a^2 = a + 1$. We could also say that $a(a + 1) = 1$, but we really expected more. However, should we expect more? In Example 16.4.1, $\sqrt{2}$ is a number we are more comfortable with, but all we really know about it is that $\alpha = \sqrt{2}$ is the number such that $\alpha^2 = 2$. Similarly, the zero that the reader will obtain in Exercise 2 of this section is the imaginary number i. Here again, this is simply a symbol, and all we know about it is that $i^2 = -1$. Hence, the result obtained in Example 16.4.2 is not really that strange.

The reader should be aware that we have just scratched the surface in the development of topics in polynomial rings. One area of significant applications is in coding theory.

EXERCISES FOR SECTION 16.4

A Exercises

1. (a) Use the definition of a field to show that $\mathbb{Q}(\sqrt{2})$ is a field.

(b) Use the definition of vector space to show that $\mathbb{Q}\left(\sqrt{2}\right)$ is a vector space over $\mathbb{Q}$.

(c) Prove that $\left\{1, \sqrt{2}\right\}$ is a basis for the vector space $\mathbb{Q}\left(\sqrt{2}\right)$ over $\mathbb{Q}$, and, therefore, the dimension of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is 2.

2. (a) Determine the splitting field of $f(x) = x^2 + 1$ over $\mathbb{R}$. This means consider the polynomial $f(x) = x^2 + 1 \in \mathbb{R}[x]$ and find the smallest field that contains $\mathbb{R}$ and all the zeros of $f(x)$. Denote this field by $\mathbb{R}(i)$.

(b) $\mathbb{R}(i)$ is more commonly referred to by a different name. What is it?

(c) Show that $\{1, i\}$ is a basis for the vector space $\mathbb{R}(i)$ over $\mathbb{R}$. What is the dimension of this vector space (over $\mathbb{R}$)?

3. Determine the splitting field of $x^4 - 5x^2 + 6$ over $\mathbb{Q}$.

4. (a) Factor $x^2 + x + 1$ into linear factors in $\mathbb{Z}_2(a)$.

(b) Write out the field tables for the field $\mathbb{Z}_2(a)$ and compare the results to the tables of Example 16.2.2.

(c) Cite a theorem and use it to show why the results of part b were to be expected.

5. (a) Show that $x^3 + x + 1$ is irreducible over $\mathbb{Z}_2$.

(b) Determine the splitting field of $x^3 + x + 1$ over $\mathbb{Z}_2$.

(c) Use Theorem 16.2.4 to illustrate that you have described all fields of order 2^3 .

6. (a) List all polynomials of degree 1, 2, 3, and 4 over $\mathbb{Z}_2 = \mathrm{GF}(2)$.

(b) Use your results in part a and list all irreducible polynomials of degree 1, 2, 3, and 4.

(c) Determine the splitting fields of each of the polynomials in part b.

(d) What is the order of each of the splitting fields obtained in part c? Explain your results using Theorem 16.2.4.

16.5 Power Series

In Section 16.3 we found that a polynomial of degree n over a ring R is an expression of the form

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \ , \ n \geq 0,$$

where each of the a_i are elements of R and $a_n \neq 0$. In Section 8.5 we defined a generating function of a sequence s with terms $s_0, s_1, s_2, \ldots$ as the infinite sum

$$G(s, z) = \sum_{i=0}^{\infty} s_i z^i = s_0 + s_1 z + s_2 z^2 + \cdots$$

The main difference between these two expressions, disregarding notation, is that the latter is an infinite expression and the former is a finite expression. In this section we will extend the algebra of polynomials to the algebra of infinite expressions like $G(s, z)$, which are called *power series*.

Definition: Power Series. *Let $[R; +, \cdot]$ be a ring. A power series over R is an expression of the form*

$$f(x) = \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots$$

where $a_1, a_2, a_3, \ldots \in R$. The set of all such expressions is denoted by $R[[x]]$.

Our first observation in our comparison of $R[x]$ and $R[[x]]$ is that every polynomial is a power series and so $R[x] \subseteq R[[x]]$. This is true because a polynomial $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ of degree n in $R[x]$, can be thought of as an infinite expression where $a_i = 0$ for $i > n$. In addition, we will see that $R[[x]]$ is a ring with subring $R[x]$.

$R[[x]]$ is given a ring structure by defining addition and multiplication on power series as we did in $R[x]$, with the modification that, since we are dealing with infinite expressions, the sums and products will remain infinite expressions that we can determine term by term, as was done in Section 16.3.

Definition: Power Series Addition and Multiplication. Given power series

$$f(x) = \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots$$

and

$$g(x) = \sum_{i=0}^{\infty} b_i x^i = b_0 + b_1 x + b_2 x^2 + \cdots$$

their sum is

$$f(x) + g(x) = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

and their product is

$$f(x) \cdot g(x) = \sum_{i=0}^{\infty} d_i x^i$$

where

$$d_i = \sum_{j=0}^{i} a_j b_{i-j}$$

Let's look at an example.

Example 16.5.1. (Example 8.5.3, Revisited.) Let

$$f(x) = \sum_{i=0}^{\infty} i x^i = 0 + 1 x + 2 x^2 + 3 x^3 + \cdots$$

and

$$g(x) = \sum_{i=0}^{\infty} 2^i x^i = 1 + 2 x + 4 x^2 + 8 x^3 + \cdots$$

be elements in $\mathbb{Z}[[x]]$. Let us compute $f(x) + g(x)$ and $f(x) \cdot g(x)$. First the sum:

$$\begin{aligned} f(x) + g(x) &= \sum_{i=0}^{\infty} i x^i + \sum_{i=0}^{\infty} 2^i x^i = \sum_{i=0}^{\infty} (i + 2^i) x^i \\ &= 1 + 3 x + 6 x^2 + 11 x^3 + \cdots \end{aligned}$$

The product is a bit more involved:

$$\begin{aligned} f(x) \cdot g(x) &= \left(\sum_{i=0}^{\infty} i x^i\right)\left(\sum_{i=0}^{\infty} 2^i x^i\right) \\ &= (0 + 1 x + 2 x^2 + 3 x^3 + \cdots)(1 + 2 x + 4 x^2 + 8 x^3 + \cdots) \\ &= 0 \cdot 1 + (0 \cdot 2 + 1 \cdot 1) x + (0 \cdot 4 + 1 \cdot 2 + 2 \cdot 1) x^2 + \cdots \\ &= \sum_{i=0}^{\infty} d_i x^i \end{aligned}$$

where

$$d_i = \sum_{j=0}^{i} a_j b_{i-j} = \sum_{j=0}^{i} j 2^{i-j}$$

For example,

$$\begin{aligned} d_3 &= 0 \cdot 2^3 + 1 \cdot 2^2 + 2 \cdot 2^1 + 3 \cdot 2^0 \\ &= 0 + 4 + 4 + 3 \\ &= 11 \end{aligned}$$

Hence,

$$f(x)\cdot g(x) = x + 4x^2 + 11x^3 + \cdots$$

The First few terms of the product do not suggest a pattern but with *Mathematica*, we can get a closed form expression for the coefficients.

$$\textbf{Simplify}\Big[\sum_{j=0}^{i} j\, 2^{i-j}\Big]$$

$$-i + 2^{i+1} - 2$$

Therefore, $d_i = 2^{i+1} - i - 2$ and

$$\begin{aligned} f(x)\cdot g(x) &= \left(\sum_{i=0}^{\infty} i\, x^i\right)\left(\sum_{i=0}^{\infty} 2^i\, x^i\right) \\ &= \sum_{i=0}^{\infty} (2^{i+1} - i - 2)\, x^i \end{aligned}$$

We have shown that addition and multiplication in $R[[x]]$ is virtually identical to that in $R[x]$. The following theorem parallels Theorem 16.3.1, establishing the ring properties of $R[[x]]$.

Theorem 16.5.1. *Let [R, +, ·] be a ring. Then:*

(1) $R[[x]]$ is a ring under the operations of power series addition and multiplication, which depend on (are induced by) the operations in R.

(2) If R is a commutative ring, then $R[[x]]$ is a commutative ring.

(3) If R is a ring with unity, 1, then $R[[x]]$ is a ring with unity (the unity in R[x] is $1 + 0x + 0x^2 + \cdots$).

(4) If R is an integral domain, then $R[[x]]$ is an integral domain.

(5) If F is a field, then $F[[x]]$ is not a field. However, $F[[x]]$ is an integral domain.

We are most interested in the situation when the set of coefficients is a field. Theorem 16.5.1 indicates that when F is a field, $F[[x]]$ is an integral domain. A reason that $F[[x]]$ is not a field is the same as one that we can cite for F[x], namely that x does not have multiplicative inverse in $F[[x]]$. With all of these similarities, one might wonder it the rings of polynomials and power series over a field are isomorphic. It turns out that they are not.

The difference between $F[x]$ and $F[[x]]$ become apparent when one studies which elements are units (i.e., elements that have multiplicative inverses) in each. First we prove that the only units in $F[x]$ are the nonzero constants— that is, the nonzero elements of F.

Theorem 16.5.2. *Let $[F;\ +,\ \cdot]$ be afield, f(x) is a unit in F[x] if and only f(x) is a nonzero element of F.*

Proof: (⇒) Let $f(x)$ be a unit in $F[x]$. Then $f(x)$ has a multiplicative inverse, call it $g(x)$, such that $f(x)\cdot g(x) = 1$. Hence, the $\deg(f(x)\cdot g(x)) = \deg(1) = 0$. But $\deg(f(x)\cdot g(x)) = \deg f(x) + \deg g(x)$. So $\deg f(x) + \deg g(x) = 0$, and since the degree of a polynomial is always nonnegative, this can only happen when the $\deg f(x) = \deg g(x) = 0$. Hence, $f(x)$ is a constant, an element of F, which is a unit if and only if it is nonzero.

(⇐) If $f(x)$ is a nonzero element of F, then it is a unit since F is a field. Thus it has an inverse, which is also in $F[x]$ and so $f(x)$ is a unit of $F[x]$. ■

Before we proceed to categorize the units in $F[[x]]$, we remind the reader that two power series $a_0 + a_1x + a_2x^2 + \cdots$ and $b_0 + b_1x + b_2x^2 + \cdots$ are equal if and only if corresponding coefficients are equal, $a_i = b_i$ for all $i \geq 0$.

Theorem 16.5.3. *Let $[F;\ +,\ \cdot]$ be a field. Then $f(x) = \sum_{i=0}^{\infty} a_i x^i$ is a unit of $F[[x]]$ if and only if $a_0 \neq 0$.*

Proof: (⇒) If $f(x)$ is a unit of $F[[x]]$, then there exists $g(x) = \sum_{i=0}^{\infty} b_i x^i$ in $F[[x]]$ such that

$$\begin{aligned} f(x)\cdot g(x) &= (a_0 + a_1x + a_2x^2 + \cdots)\cdot(b_0 + b_1x + b_2x^2 + \cdots) \\ &= 1 \\ &= 1 + 0x + 0x^2 + \cdots \end{aligned}$$

Since corresponding coefficients in the equation above must be equal, $a_0\cdot b_0 = 1$, which implies that $a_0 \neq 0$.

(⇐) Assume that $a_0 \neq 0$. To prove that $f(x)$ is a unit of $F[[x]]$ we need to find $g(x) = \sum_{i=0}^{\infty} b_i x^i$ in $F[[x]]$ such that

$$f(x)\cdot g(x) = \sum_{i=0}^{\infty} d_i x^i = 1.$$

If we use the formula for the coefficients $d_0, d_1, d_2, \ldots$ of $f(x)\cdot g(x)$ and equate coefficients, we will obtain

$$\begin{aligned}
d_0 &= a_0 \cdot b_0 = 1\\
d_1 &= a_0\, b_1 + a_1\, b_0 = 0\\
d_2 &= a_0\, b_2 + a_1\, b_1 + a_2\, b_0\\
&\vdots\\
d_s &= a_0\, b_s + a_1\, b_{s-1} + \cdots + a_s\, b_0\\
&\vdots
\end{aligned}$$

Therefore, the existence of $g(x)$ is equivalent to the existence of a solution $b_0, b_1, b_2, \ldots$, to the above system of equations. Since $a_0 \neq 0$, we can solve the first equation for b_0. Then we can continue to the second equation and solve for b_1, then b_2 can be found by solving the third equation, etc. Hence,

$$\begin{aligned}
b_0 &= a_0^{-1}\\
b_1 &= -a_0^{-1}(a_1\, b_0)\\
b_1 &= -a_0^{-1}(a_1\, b_1 + a_2\, b_0)\\
&\vdots\\
b_s &= -a_0^{-1}(a_1\, b_{s-1} + a_2\, b_{s-2} + \cdots + a_s\, b_0)\\
&\vdots
\end{aligned}$$

Therefore the powers series $\sum_{i=0}^{\infty} b_i\, x^i$ is an expression whose coefficients lie in F and that satisfies the statement $f(x) \cdot g(x) = 1$. Hence, $g(x)$ is the multiplicative inverse of $f(x)$ and $f(x)$ is a unit..

Example 16.5.2. Let

$$\begin{aligned}
f(x) &= 1 + 2x + 3x^2 + 4x^3 + \cdots\\
&= \sum_{i=0}^{\infty} (i+1)\, x^i
\end{aligned}$$

be an element of $\mathbb{Q}[[x]]$. Then, by Theorem 16.5.3, since $a_0 = 1 \neq 0$, $f(x)$ is a unit and has an inverse, call it $g(x)$. To compute $g(x)$, we follow the procedure outlined in Theorem 16.5.3 . Using the formulas for the b_i's, we obtain

$$\begin{aligned}
b_0 &= 1\\
b_1 &= -1\,(2\cdot 1) = -2\\
b_2 &= -1\,(2\cdot(-2) + 3\cdot 1) = 1\\
b_3 &= -1\,(2\cdot 1 + 3\cdot(-2) + 4\cdot 1) = 0\\
b_4 &= -1\,(2\cdot 0 + 3\cdot 1 + 4\cdot(-2) + 5\cdot 1) = 0\\
b_5 &= -1\,(2\cdot 0 + 3\cdot 0 + 4\cdot(1) + 5\cdot(-2) + 6\cdot 1) = 0\\
&\vdots\\
b_s &= -1\,(2\cdot 0 + 3\cdot 0 + \cdots(s-2)\cdot 0 + (s-1)\cdot 1 + s\cdot(-2) + (s+1)\cdot 1) = 0 \quad s \geq 3
\end{aligned}$$

Hence, $g(x) = 1 - 2x + x^2$ is the multiplicative inverse of $f(x)$.

If we compare Theorems 16.5.2 and 16.5.3, we note that while the only elements in $F[x]$ that are units are the nonzero constants of F, the units in $F[[x]]$ are every single expression in x where $a_0 \neq 0$. So certainly $F[[x]]$ contains a wider variety of units than $F[x]$. Yet $F[[x]]$ is not a field, since $x \in F[[x]]$ is not a unit by Theorem 16.5.3. So concerning the algebraic structure of $F[[x]]$, we know that it is an integral domain that contains $F[x]$. If we allow our power series to take on negative exponents—that is, consider expressions of the form

$$f(x) = \sum_{i=-\infty}^{\infty} a_i\, x^i$$

where all but a finite number of terms with a negative index equal zero. These expressions are called *extended power series*. The set of all such expressions is a field, call it E. This set does contain, for example, the inverse of x namely x^{-1}. It can be shown that each nonzero element of E is a unit.

EXERCISES FOR SECTION 16.5

A Exercises

1. Let $f(x) = \sum_{i=0}^{\infty} a_i\, x^i$ and $g(x) = \sum_{i=0}^{\infty} b_i\, x^i$ be elements of $R[[x]]$. Let

$$f(x) \cdot g(x) = \sum_{i=0}^{\infty} d_i\, x^i = 1.$$

(a) Apply the distributive law repeatedly to

$$(a_0 + a_1\, x + a_2\, x^2 + \cdots)\cdot(b_0 + b_1\, x + b_2\, x^2 + \cdots)$$

to obtain the formula

$$d_s = \sum_{i=0}^{s} a_i\, b_{s-i}$$

for the coefficients of $f(x) \cdot g(x)$. Hence, you have shown that

$$f(x) \cdot g(x) = \sum_{s=0}^{\infty} \left(\sum_{i=0}^{s} a_i\, b_{s-i} \right) x^s$$

(b) Apply the above formula to the product in Example 16.5.1 and show that the result is the same as that obtained in this example.

2. (a) Prove that for any integral domain D, the following can be proven:

$f(x) = \sum_{i=0}^{\infty} a_i\, x^i$ is a unit of $D[[x]]$ if and only if a_0 is a unit in D.

(b) Compare the statement in part a to that in Theorem 16.5.3.

(c) Give an example of the statement in part a in $\mathbb{Z}[[x]]$.

3. Use the formula for the product to verify that the expression g(x) of Example 16.5.2 is indeed the inverse of f(x).

4. (a) Determine the inverse of $f(x) = 1 + x + x^2 + \cdots = \sum_{i=0}^{\infty} x^i$ in $\mathbb{Q}[[x]]$.

(b) Repeat part a with $f(x)$ taken in $\mathbb{Z}_2[[x]]$.

(c) Use the method outlined in Chapter 8 to show that the power series $f(x) = \sum_{i=0}^{\infty} x^i$ is the rational generating function $\frac{1}{1-x}$. What is the inverse of this function? Compare your results with those in part a.

5. (a) Determine the inverse of $h(x) = \sum_{i=0}^{\infty} 2^i\, x^i$ in $\mathbb{Q}[[x]]$.

(b) Use the procedures in Chapter 8 to find a rational generating function for $h(x)$ in part a. Find the multiplicative inverse of this function.

6. Let $a(x) = 1 + 3x + 9x^2 + 27x^3 + \cdots = \sum_{i=0}^{\infty} 3^i\, x^i$ and

$b(x) = 1 + x + x^2 + x^3 + \cdots = \sum_{i=0}^{\infty} x^i$ both in $\mathbb{R}[[x]]$.

(a) What are the first four terms (counting the constant term as the 0th term) of $a(x) + b(x)$?

(b) Find a closed form expression for $a(x)$.

(c) What are the first four terms of $a(x)\, b(x)$?

B Exercise

7. Write as an extended power series:

(a) $\left(x^4 - x^5\right)^{-1}$

(b) $(x^2 - 2x^3 + x^4)^{-1}$

SUPPLEMENTARY EXERCISES FOR CHAPTER 16

Section 16.1

1. (a) Expand $(A + B)^2$ in the ring $[M_{n\times n}(\mathbb{R}); +, \cdot]$.
   (b) Will your result be similar for any noncommutative ring?

2. (a) Expand $(A + B)^3$ in the ring $[M_{n\times n}(\mathbb{R}); +, \cdot]$.
   (b) Will your result be similar for any noncommutative ring?

3. Let D be the set of all 2×2 diagonal matrices over the real numbers.
   (a) Prove that D is a subring of $[M_{2\times 2}(\mathbb{R}); +, \cdot]$, hence a ring under the usual operations.
   (b) Prove that D is a commutative ring with unity.
   (c) Is the cancellation law true in D?

4. (a) Use the definition of a ring to convince yourself that $R = \left\{a + b\sqrt{2} \mid a,\ b \epsilon \mathbb{Z}\right\}$ is a ring. A common name given this ring is $\mathbb{Z}\left[\sqrt{2}\right]$.
   (b) What is the unity of $\mathbb{Z}\left[\sqrt{2}\right]$?
   (c) Prove that $\mathbb{Z}\left[\sqrt{2}\right]$ is an integral domain.

5. It can be shown, in general, that if R is any ring, $[M_{n\times n}(R); +, \cdot]$ is a ring.
   (a) How many elements are there in the ring $R = [M_{2\times 2}(\mathbb{Z}_2); +, \cdot]$? What are the zero and unity of R?
   (b) Determine all solutions of the equation $X^2 - I = 0$ in R.

6. Find all six units of $[M_{2\times 2}(\mathbb{Z}_2); +, \cdot]$. Hint: The set of units is closed with respect to multiplication and one of them is $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$

7. Let $A = \left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| a \in \mathbb{R}\right\}$ then A is a ring under matrix addition and multiplication. Prove that A is isomorphic to the ring of real numbers..

Section 16.2

8. Show that $\mathbb{Z}_2$ is a subfield of the field given in Example 16.2.2, or equivalently, that the field in this example is an extension field of $\mathbb{Z}_2$.

9. Show that a and b are the two roots of the equation $x^2 + x + 1 = 0$ in the field of Example 16.2.2.

10. Let $A = \left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{R}\right\}$. Prove that A with matrix addition and multiplication is isomorphic to the ring of complex numbers, $\mathbb{C}$.

Section 16.3

11. Find all rational zeros (roots) of $f(x) = x^4 - 6x^3 + 10x^2 - 6x + 9$ and factor $f(x)$ into irreducible factors in $\mathbb{Q}[x]$.

12. Determine all zeros of $f(x) = x^3 + 1$ in the field of Example 16.2.2, and express $f(x)$ as a product of irreducible factors over that field.

13. Repeat Exercise 12 for $g(x) = x^2 + x^2 + x$,

14. Find all five roots of $f(x) = x^3 + 7x$ in $\mathbb{Z}_8$. Explain why this does not contradict Theorem 16.3.4.

Exercises 15 to 20 develop an introduction to polynomial codes. In Chapter 15 we introduced group codes. Here, we will discuss another code that uses polynomials. A k – tuple in $\mathbb{Z}_2{}^k$ can be identified with a polynomial of degree $k - 1$ in the integral domain $\mathbb{Z}_2[x]$ and conversely. We do this by associating a k-tuple with the coefficients of a polynomial starting with the constant term. For example, the 5-tuple $(1, 0, 1, 1, 0)$ is viewed as the polynomial $1 + 0x + 1x^2 + 1x^3 + 0x^4 = 1 + x^2 + x^3$. If we define addition and multiplication on $\mathbb{Z}_2{}^k$ based on polynomial operations, we will have highly structured codes. For the actual code, we present an example where $k = 7$.

15. To add k-tuples, we can take two equivalent approaches. We can either simply add the k-tuples coordinatewise as in any direct product, or we can covert the k-tuples to polynomials of degree $k - 1$ or less, add them, and then write down the coefficients of the sum.

(a) For each of the following pairs of add and multiply the pairs k-tuples, where k varies, compute their sum. Use both ways to add for at least one part.

(i) $(0, 1, 0)$ and $(1, 1, 1)$

(ii) $(0, 1, 0, 1)$ and $(1, 1, 0, 1)$

(iii) $(1, 1, 1, 0, 1, 0, 1)$ and $(0, 0, 0, 0, 1, 0, 0)$

(iv) $(1, 0, 0, 1, 1, 1, 1)$ and $(0, 0, 0, 1, 0, 0, 0)$

(b) What what relationship between polynomials and k-tuples makes it possible to do this addition two different ways to get the same sum.

16. The encoding of a string of bits is based on polynomial division. Given a four bit message, we make the bits coefficients of a sixth degree polynomial, $b_3 x^3 + b_4 x^4 + b_5 x^5 + b_6 x^6$ which we can also express in $\mathbb{Z}_2{}^6$ as $(0, 0, 0, b_3, b_4, b_5, b_6)$, we divide this polynomial by $p(x) = 1 + x + x^3$ and add the remainder to the "message polynomial. The quotient is in the division is discarded. Thus, if the remainder, which must be a polynomial of degree less than 2, is $b_0 + b_1 x + b_2 x^2$, the encoded message is the string of bits $(b_0, b_1, b_2, b_3, b_4, b_5, b_6)$.

(a) Encode the following elements of $\mathbb{Z}_2{}^6$as described above.

(a) $(0, 0, 0, 1, 1, 0, 1)$

(b) $(0, 0, 0, 1, 1, 1, 1)$

(c) $(0, 0, 0, 0, 0, 1, 0)$

(b) Prove that the encoded message will always represent a polynomial with is evenly divisible by the polynomial $p(x)$ that is used to encode the message.

17. A single bit error in the transmission of our seven bit encoded message $(b_0, b_1, b_2, b_3, b_4, b_5, b_6)$ can be though of as a monomial expression x^j, where $0 \leq j \leq 6$. The effect of an error occurring is to add that monomial to the encoded message. So if the last bit is transmitted incorrectly, the monomial x^6 is added and the received bit sequence is $(b_0, b_1, b_2, b_3, b_4, b_5, b_6 +_2 1)$. If no error takes place, we can think of the zero polynomial being added. Prove that if an error takes place, the received bit string represents a polynomial that is *not* a multiple of $p(x)$.

18. There are seven different single bit errors. Let's focus on what happens if an error occurs in the last bit. If the error occurs in the last bit and the received bit string represents the polynomial $m(x)$, show that the remainder upon dividing $m(x)$ by $p(x)$ will be the same for all possible values of $m(x)$. What is that remainder? This is called the *syndrome* for an error in the last bit.

19. What are the syndromes for each of the other error positions? Let's agree to number them 0th through 6th , so the 6th position syndrome was determined above. What the syndrome if no error occurs?

20. Assuming no more than a single bit error in the transmission of seven bits, what is the transmitted bit string, given these received strings?

(a) $(0, 1, 0, 1, 0, 1, 1)$

(b) $(1, 1, 1, 0, 0, 0, 0)$

(c) $(0, 0, 1, 1, 0, 1, 0)$

Section 16.4

21. In Exercise 5 of Section 16.4 you constructed GF(8) using $x^3 + x + 1$. Show that GF(8) can also be obtained by using the polynomial $g(x) = x^3 + x^2 + 1$.

22. (a) Show that $f(x) = x^4 + x + 1$ is irreducible over $\mathbb{Z}_2$.

(b) Describe the splitting field of $f(x)$ over $\mathbb{Z}_2$.

(c) Let a be a zero of $f(x)$. Show that each nonzero element of the splitting field in part (b) can be described as a power of a.

Section 16.5

23. Review Example 16.5.2. Derive the multiplicative inverse of $1 - 2x + x^2$ by doing repeated polynomial division, as suggested by the following first step:

$$\begin{array}{rl} & 1 \\ \cline{2-2} 1-2x+x^2 & \big)\,1 \\ & \underline{1-2x+x^2} \\ & 2x-x^2 \end{array}$$

24. Use polynomial long division to obtain the power series representation of $\frac{1}{1+x^3}$ over $\mathbb{Q}$. What is the inverse of the power series you obtained?

25. Find the generating function for the sequence defined by the difference equation $a_k = a_{k-1} + a_{k-2}$, $k \geq 2$, with $a_0 = a_1 = 1$ the indicated fields.

(a) $\mathbb{Q}$

(b) $\mathbb{Z}_2$

(c) $\mathbb{Z}_3$

26. Determine the inverse of each of the power series in Exercise 25.

27. Recall from high school algebra that any quadratic with real coefficients, of the form $a x^2 + b x + c = 0$, $a \neq 0$, can be solved using the quadratic formula:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

(a) Does this formula always produce zeros in $\mathbb{R}$?

(b) Use the quadratic formula to solve $x^2 + x + 1 = 0$ in $\mathbb{Z}_3$,

(c) Use the quadratic formula to solve $x^2 + 2 = 0$ in $\mathbb{Z}_3$.

(d) Use the quadratic formula to solve $x^2 + x + 2 = 0$ in $\mathbb{Z}_3$.

(e) What observations do you have based on parts (b) - (d)?

Solutions and Hints to Odd-Numbered Exercises

CHAPTER 1

Section 1.1

1. (a) $8, \ 15, \ 22, \ 29$

(b) apple, pear, peach, plum   These solutions are not unique.

(c) $1/2, \ 1/3, \ 1/4, \ 1/5$

(d) $-8, \ -6, \ -4, \ -2$

(e) $6, \ 10, \ 15, \ 21$

3.(a) $\{2k + 1 : k \in \mathbb{Z}, \ 2 \leqslant k \leqslant 39\}$ (b) $\{x \in \mathbb{Q} : -1 < x < 1\}$

(c) $\{2n : n \in \mathbb{Z}\}$ (d) $\{9n : n \in \mathbb{Z}, -2 \leqslant n\}$

5.(a) True   (b) False   (e) True   (d) True   (e) False

(f) True   (g) False   (h) True

Section 1.2

1. (a) $\{2, 3\}$ (b) $\{0, 2, 3\}$ (c) $\{0, 2, 3\}$ (d) $\{0, 1, 2, 3, 5, 9\}$

(e) $\{0\}$ (f) $\emptyset$ (g)$\{1, 4, 5, 6, 7, 8, 9\}$ (h) $\{0, 2, 3, 4, 6, 7, 8\}$

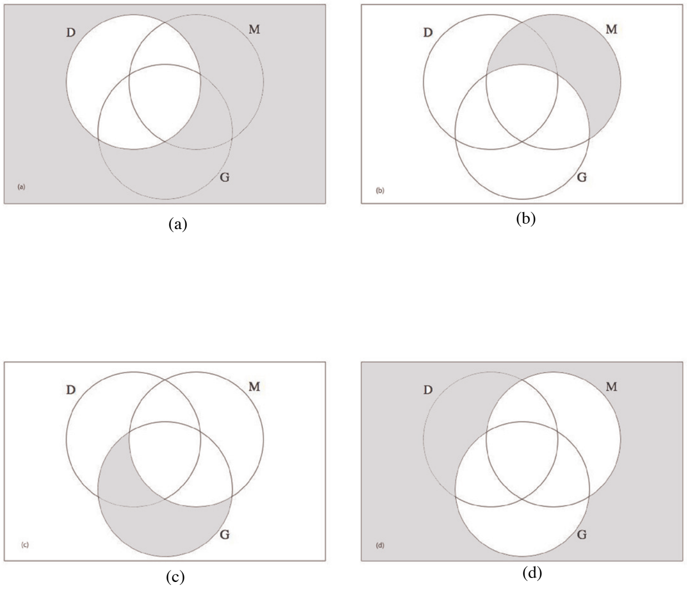
(i) $\emptyset$ (j) $\{0\}$

3. These are all true for any sets A, B, and C.

5. (a) $\{1, \ 4\} \subseteq A \subseteq \{1, \ 2, \ 3, \ 4\}$

(b) $\{2\} \subseteq A \subseteq \{1, \ 2, \ 4, \ 5\}$ (c) $A = \{2, \ 4, \ 5\}$

7.



(a)

(b)

(c)

(d)

9. (a)

```
? Select
```

Select[*list*, *crit*] picks out all elements e_i of *list* for which *crit*[e_i] is True.
Select[*list*, *crit*, *n*] picks out the first *n* elements for which *crit*[e_i] is True. ≫

```
? PrimeQ
```

PrimeQ[*expr*] yields True if *expr* is a prime number, and yields False otherwise. ≫

(b)

```
Select[Range[2000, 2099], PrimeQ[#] &]
```

{2003, 2011, 2017, 2027, 2029, 2039, 2053, 2063, 2069, 2081, 2083, 2087, 2089, 2099}

Section 1.3

1. (a) $\{(0, 2), (0, 3), (2, 2), (2, 3), (3, 2), (3, 3)\}$

(b) $\{(2, 0), (2, 2), (2, 3), (3, 0), (3, 2), (3, 3)\}$

(c) $\{(0, 2, 1), (0, 2, 4), (0, 3, 1), (0, 3, 4), (2, 2, 1), (2, 2, 4), (2, 3, 1), (2, 3, 4), (3, 2, 1), (3, 2, 4), (3, 3, 1), (3, 3, 4)\}$

(d) $\emptyset$

(e) $\{(0, 1), (0, 4), (2, 1), (2, 4), (3, 1), (3, 4)\}$

(f) $\{(2, 2), (2, 3), (3, 2), (3, 3)\}$

(g) $\{(2, 2, 2), (2, 2, 3), (2, 3, 2), (2, 3, 3), (3, 2, 2), (3, 2, 3), (3, 3, 2), (3, 3, 3)\}$

(h) $\{(2, \emptyset), (2, \{2\}), (2, \{3\}), (2, \{2, 3\}), (3, \emptyset), (3, \{2\}), (3, \{3\}), (3, \{2, 3\})\}$

3.$\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}$

5. There are n singleton subsets, one for each element.

7. (a) $\{+00, +01, +10, +11, -00, -01, -10, -11\}$ (b) 16 and 512

9. When $A = B$

Section 1.4

1.(a) 11 111 (b) 100 000 (c) 1010 (d) 1 100 100

3. (a) 18 (b) 19 (c) 42 (d) 1264

5.There is a bit for each power of 2, starting with the zeroth power. The number 1990 is between $2^{10} = 1024$ and $2^{11} = 2048$, so there are $10 + 1$ (the 0 power of 2) bits.

(a) 11 (b) 12 (c) 13 (d) 8

7.It must be a multiple of four.

Section 1.5

1.(a) 24 (b) 6 (c) 3, 7, 15, 31 (d) 1, 4, 9, 16

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

(b) $\frac{1}{1(2)} + \frac{1}{2(3)} + \frac{1}{3(4)} = \frac{1}{2} + \frac{1}{6} + \frac{1}{12} = \frac{3}{4} = \frac{3}{3+1}$

(c) $1 + 2^3 + 3^3 + \cdots + n^3 = \left(\frac{1}{4}\right) n^2 (n+1)^2$

$1 + 4 + 27 = 36$ $\left(\frac{1}{4}\right) (3)^2 (3+1)^2 = 36$

5.$(x+y)^n = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \cdots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n$

7.(a) $\{x \in \mathbb{Q} \mid 0 < x \leqslant 5\}$ (b) $\emptyset$

(c) $\{x \in \mathbb{Q} \mid -5 < x < 5\} = B_5$ (d) $\{x \in \mathbb{Q} \mid -1 < x < 1\} = B_1$

9.(a) 36 (b) 105

Supplementary Exercises—Chapter 1

1. (a) $\{2, 1\}$ (b) $\emptyset$ (c) $\{\mathbb{i}, -\mathbb{i}\}$

3. (a) $\{0, 3, 4, 5, 6, 7, 8, 9\}$ (b) $\{3, 6, 9\}$ (c) $\{0, 1, 2\}$

5. (a) $A \bigcup B = \{1, 2, 3, 4, 5, 6, 7, 9, 12\} \Rightarrow |(A \bigcup B)| = 9$

$|A| = 6,\ |B| = 5\ \ A \bigcap B = \{2, 5\} \Rightarrow |(A \bigcap B)| = 2$

$|A| + |B| - |(A \bigcap B)| = 6 + 5 - 2 = 9$

(b) $10, 8, 2$

(c) $(A \bigcup B \bigcup C) = |((A \bigcup B) \bigcup C)|$

by part (a) $= |(A \bigcup B)| + |C| - |((A \bigcup B) \bigcap C)|$

Distributive $= |(A \bigcup B)| + |C| - |((A \bigcap C) \bigcup (B \bigcap C))|$

by part (a) $= |A| + |B| - |(A \bigcap B)| + |C| - [|(A \bigcap C)|$
$+ |(B \bigcap C)| - |((A \bigcap C) \bigcap (B \bigcap C))|]$

Simplify $= |A| + |B| + |C| - |(A \bigcap B)| - |(A \bigcap C)|$
$-|(B \bigcap C)| + |(A \bigcap B \bigcap C)|$

7. (a) $\{(4, 4)\}$

(b) $\{(2, 4), (4, 4), (6, 4)\}$

(c) $\{(4, 4, 4)\}$

(d) $\{(4, 2), (4, 4), (4, 6)\}$

(e) $\{(2, 4, 1), (2, 4, 5), (4, 4, 1), (4, 4, 5), (6, 4, 1), (6, 4, 5)\}$

15. (a) $A_0 = \{0\},\ A_1 = \{0, 1, 2, 3\},\ A_2 = \{0, 1, 2, \ldots, 6\},\ A 3 = \{0, 1, 2, \ldots, 9\}$

(b) $(0, 1, 2, 3\}$

(c) $\{0\}$

(d) $\{0, 1, 2, \ldots, 9\}$

(e) $\{0, 1, 2, \ldots, 9\}$

17. Parts a, b, and d are true with multiplication replacing addition.

CHAPTER 2

Section 2.1

1. If there are m horses in race 1 and n horses in race 2 then there are $m \cdot n$ possible daily doubles.

3. $72 = 4 \cdot 6 \cdot 3$

5. $720 = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$

7. If we always include the blazer in the outfit we would have 6 outfits. If we consider the blazer optional then there would be 12 outfits. When we add a sweater we have the same type of choice. Considering the sweater optional produces 24 outfits.

9. (a) $2^8 = 256$ (b) $2^4 = 16$. Here we are concerned only with the first four bits, since the last four must be the same.

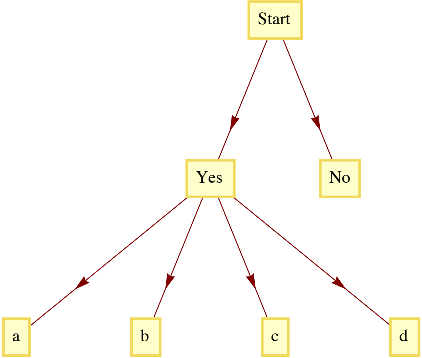
(c) $2^7 = 128$, you have no choice in the last bit.

11. (a) 16 (b) 30

13. (a) 3 (b) 6

15. 18

17. (a)



(b) 5^6

19. $2^{n-1} - 1$ and $2^n - 2$

Section 2.2

1. $P(1000; 3)$

3. With repetition: $26^8 \approx 2.0883 \times 10^{11}$

Without repetition: $P(26; 8) \approx 6.2991 \times 10^{10}$

5. 15!

7. (a) $P(15; 5) = 360\,360$ (b) $2 \cdot 14 \cdot 13 \cdot 12 \cdot 11 = 48\,048$

9. $2 \cdot P(3; 3) = 12$

11. (a) $P(4; 2) = 12$ (b) $P(n; 2) = n(n-1)$

(c) Case 1: $m > n$. Since the coordinates must be different, this case is impossible.

Case 2: $m \leqslant n$. $P(n; m)$.

Section 2.3

1. $\{\{a\}, \{b\}, \{c\}\}$, $\{\{a, b\}, \{c\}\}$, $\{\{a, c\}, \{b\}\}$, $\{\{a\}, \{b, c\}\}$, $\{\{a, b, c\}\}$

3. No. By this definition it is possible that an element of A; might not belong to A.

5. The first subset is all the even integers and the second is all the odd integers.

These two sets do not intersect and they cover the integers completely.

7. Since 17 participated in both activities, 30 of the tennis players only played tennis and 35 of the swimmers only swam. Therefore, $17 + 30 + 35 = 82$ of those who were surveyed participated in an activity and so 8 did not.

9. Assume $|(A_1 \cup A_2)| = |A_1| + |A_2| - |(A_1 \cap A_2)|$.

$|(A_1 \cup A_2 \cup A_3)| = |((A_1 \cup A_2) \cup A_3)|$

by 1st law $= |(A_1 \cup A_2)| + |A_3| - |((A_1 \cup A_2) \cap A_3)|$

Distributive $= |(A_1 \cup A_2)| + |A_3| - |((A_1 \cap A_3) \cup (A_2 \cap A_3))|$

1st law (twice) $= |A_1| + |A_2| - |(A_1 \cap A_2)| + |A_3|$
$-[|(A_1 \cap A_3)| + |(A_2 \cap A_3)| - |((A_1 \cap A_3) \cap (A_2 \cap A_3))|]$

Simplify $= |A_1| + |A_2| + |A_3| - |(A_1 \cap A_2)| - |(A_1 \cap A_3)|$
$-|(A_2 \cap A_3)| + |(A_1 \cap A_2 \cap A_3)|$.

(b) $|(A_1 \bigcup A_2 \bigcup A_3 \bigcup A_4)| = |A_1| + |A_2| + |A_3| + |A_4| - |(A_1 \bigcap A_2)|$
$-|(A_1 \bigcap A_3)| - |(A_1 \bigcap A_4)| - |(A_2 \bigcap A_3)| - |(A_2 \bigcap A_4)|$
$-|(A_3 \bigcap A_4)| + |(A_1 \bigcap A_2 \bigcap A_3)| + |(A_1 \bigcap A_2 \bigcap A_4)|$
$+|(A_1 \bigcap A_3 \bigcap A_4)| + |(A_2 \bigcap A_3 \bigcap A_4)| - |(A_1 \bigcap A_2 \bigcap A_3 \bigcap A_4)|$

Derivation:

$|(A_1 \bigcup A_2 \bigcup A_3 \bigcup A_4)| = |((A_1 \bigcup A_2 \bigcup A_3) \bigcup A_4)|$

1st law $= |(A_1 \bigcup A_2 \bigcup A_3)| + |A_4| - |((A_1 \bigcup A_2 \bigcup A_3) \bigcap A_4)|$

Distributive $= |(A_1 \bigcup A_2 \bigcup A_3)| + |A_4| - |((A_1 \bigcap A_4) \bigcup (A_2 \bigcap A_4)$
$\bigcup (A_3 \bigcap A_4))|$

2nd law (twice) $= |A_1| + |A_2| + |A_3| - |(A_1 \bigcap A_2)| - |(A_1 \bigcap A_3)|$
$-|(A_2 \bigcap A_3)| + |(A_1 \bigcap A_2 \bigcap A_3)| + |A_4| - [|(A_1 \bigcap A_4)|$
$+ |(A_2 \bigcap A_4)| + |(A_3 \bigcap A_4)| - |((A_1 \bigcap A_4) \bigcap (A_2 \bigcap A_4))|$
$- |((A_1 \bigcap A_4) \bigcap (A_3 \bigcap A_4))| - |((A_2 \bigcap A_4) \bigcap (A_3 \bigcap A_4))|$
$+ |((A_1 \bigcap A_4) \bigcap (A_2 \bigcap A_4) \bigcap (A_3 \bigcap A_4))|]$

Simplify $= |A_1| + |A_2| + |A_3| + |A_4| - |(A_1 \bigcap A_2)| - |(A_1 \bigcap A_3)|$
$-|(A_2 \bigcap A_3)| - |(A_1 \bigcap A_4)| - |(A_2 \bigcap A_4)| - |(A_3 \bigcap A_4)|$
$+|(A_1 \bigcap A_2 \bigcap A_3)| + |(A_1 \bigcap A_2 \bigcap A_4)| + |(A_1 \bigcap A_3 \bigcap A_4)|$
$+|(A_2 \bigcap A_3 \bigcap A_4)| - |(A_1 \bigcap A_2 A_3 \bigcap A_4)|$

11. *Hint*: Partition the set of fractions into blocks, where each block contains fractions that are numerically equivalent. Describe how you would determine whether two fractions belong to the same block. Redefine the rational numbers to be this partition. Each rational number is a set of fractions.

Section 2.4

1. $C(10; 3) \cdot C(25; 4) = 1, 518, 000$

3. $C(10; 7) + C(10; 8) + C(10; 9) + C(10; 10)$

5. $16\,x^4 - 96\,x^3\,y + 216\,x^2\,y^2 - 216\,x\,y^3 + 81\,y^4$

7. (a) $C(52; 5) = 2, 598, 960$

(b) $C(52; 5) \cdot C(47; 5) \cdot C(42; 5) \cdot C(37; 5)$

9. $C(4; 2)\,C(48; 3)$

11. $C(12; 3) \cdot C(9; 4) \cdot C(5; 5)$

13. (a) $C(10; 2) = 45$ (b) $C(10; 3) = 120$

15. Assume $|A| = n$. If we let $x = y = 1$ in the Binomial Theorem, we obtain

$2^n = C(n; 0) + C(n; 1) + \cdots + C(n; n)$, and as a consequence of Example

2.4.7 we realize that the right side of this equation says the sum of all subsets

of A. Hence $|P(A)| = 2^{|A|}$

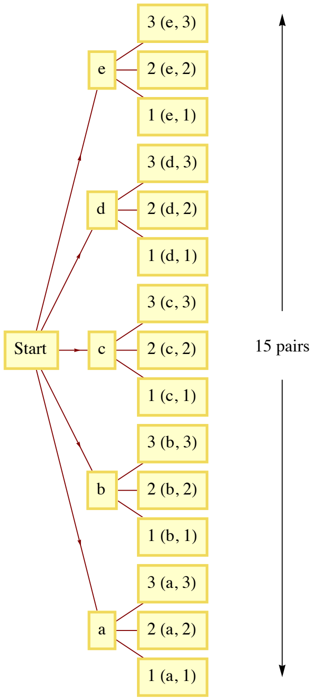
17. 999, 400, 119, 992.

Supplementary Exercises—Chapter 2

1. (a) $10 \cdot 9 \cdot 8 = 720$

(b) $10 \cdot 10 \cdot 10 = 1000$

3. (a)



(b) If you imagine drawing a tree diagram for this general case, from the starting point, there will be m branches, one for each element of A. From the end of each of the "A branches" there will be n branches, one for each element of B. Therefore, there are $m \cdot n$ pairs in $A \times B$.

5. (a) If couple A is seated, couple B can be either to their left or right and couple C sits in the other position; therefore, there are two possible arrangements.

(b) $2 \cdot 2^3 = 48$

7. (a) $5 != 120$ (b) $5! - 2 \cdot 4 != 72$. (Here, we subtract the ways that the

two could be seated together from the total number of arrangements.)

9. (a) $P(10;\, 4)$ (b) $C(10;\, 4) \cdot C(6;\, 3)$

11. $C(10;\, 2) \cdot 8 = 360$

13. (a) $C(11;\, 5) = 462$ (b) $C(10;\, 4) = 210$

(c) $C(2;\, 1) \cdot C(9;\, 4) + C(9;\, 3)$

15. (a) $3\, P(3;\, 2) = 18$ (b) $2\, P(3;\, 2) = 12$

CHAPTER 3

Section 3.1

1. (a) $d \bigwedge c$ (b) $s \vee \neg c$

(c) $\neg (d \bigwedge s)$ (d) $\neg s \wedge \neg c$

3. (a) $2 > 5$ and 8 is an even integer. False.

(b) If $2 \leqslant 5$ then 8 is an even integer. True.

(c) If $2 \leqslant 5$ and 8 is an even integer then 11 is a prime number. True.

(d) If $2 \leqslant 5$ then either 8 is an even integer or 11 is not a prime number. True.

(e) If $2 \leqslant 5$ then either 8 is an odd integer or 11 is not a prime number. False.

(f) If 8 is not an even integer then $2 > 5$. True.

5. Only the converse of d is true.

Section 3.2

1. (a)

p	$p \vee p$
0	0
1	1

(b)

p	$\neg p$	$p \wedge p$
0	1	0
1	0	0

(c)

p	$\neg p$	$p \wedge (\neg p)$
0	1	1
1	0	1

(d)

p	$p \wedge p$
0	0
1	1

3. (a) $\neg (p \wedge q) \vee s$ (b) $(p \vee q) \wedge (r \vee q)$

5. $2^4 = 16$

Section 3.3

1. $a \Leftrightarrow e,\ d \Leftrightarrow f,\ g \Leftrightarrow h$

3. No. In symbolic form the question is: Is $(p \to q) \Leftrightarrow (q \to p)$?

p	q	$p \to q$	$q \to p$	$(p \to q) \leftrightarrow (q \to p)$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	1	1	1

This table indicates that an implication is not always equivalent to its converse.

5. Let x be any proposition generated by p and q. The truth table for x has 4 rows

and there are 2 choices for a truth value for x for each row, so there are

$2 \cdot 2 \cdot 2 \cdot 2 = 2^4$ possible propositions.

(See Table 13.6.1 for an illustration.)

7. $0 \to p$ and $p \to 1$ are tautologies.

Section 3.4

1. Let s = "I will study", t = "I will learn." The argument is: $((s \to t) \wedge (\neg t)) \to (\neg s)$, call the argument a.

s	t	$s \to t$	$(s \to t) \wedge (\neg t)$	a
0	0	1	1	1
0	1	1	0	1
1	0	0	0	1
1	1	1	0	1

Since a is a tautology, the argument is valid.

3. In any true statement S, replace; $\wedge$ with $\vee$, $\vee$with $\wedge$, 0 with 1, 1 with 0, $\Leftarrow$ with $\Rightarrow$, and $\Rightarrow$ with $\Leftarrow$. Leave all other connectives unchanged.

5. (a)

```
If not EOF then repeat
    Read (ch);
    Count := Count + 1
    Until EOF
```

Law used: involution law, Not Not EOF$\Leftrightarrow$ EOF}

(b)

```
    $S := 0;\ K := 1;\ N := 100;$
    If $K <= N$ then do
    Repeat
    $S := S + K$;
    $K := K + 1$
    Until $K > N$
```

No Law of logic is really used here, only a law of integers:

Not $(K \leq N) \Leftrightarrow K > N$.

Section 3.5

1. (a)

p	q	$(p \vee q) \wedge \neg q$	$((p \vee q) \wedge \neg q) \rightarrow p$
0	0	0	1
0	1	0	1
1	0	1	1
1	1	0	1

(b)

p	q	$(p \rightarrow q) \wedge \neg q$	$\neg p$	$(p \rightarrow q) \wedge (\neg q)$
0	0	1	1	1
0	1	0	1	1
1	0	0	0	1
1	1	0	0	1

3. (a) Direct proof:

(1) $d \rightarrow (a \vee c)$

(2) d

(3) $a \vee c$

(4) $a \rightarrow b$

(5) $\neg a \vee b$

(6) $c \rightarrow b$

(7) $\neg c \vee b$

(8) $(\neg a \vee b) \wedge (\neg c \vee b)$

(9) $(\neg a \wedge \neg c) \vee b$

(10) $\neg (a \vee c) \vee b$

(11) b ■

Indirect proof:

(1) $\neg b$	Negated conclusion
(2) $a \rightarrow b$	Premise
(3) $\neg a$	Indirect Reasoning (1), (2)
(4) $c \rightarrow b$	Premise
(5) $\neg c$	Indirect Reasoning (1), (4)
(6) $(\neg a \wedge \neg c)$	Conjunctive (3), (5)
(7) $\neg (a \vee c)$	DeMorgan's law (6)
(8) $d \rightarrow (a \vee c)$	Premise
(9) $\neg d$	Indirect Reasoning (7), (8)
(10) d	Premise
(11) 0	(9), (10) ■

(b) Direct proof:

(1) $(p \to q) \bigwedge (r \to s)$

(2) $p \to q$

(3) $(p \to t) \bigwedge (s \to u)$

(4) $q \to t$

(5) $p \to t$

(6) $r \to s$

(7) $s \to u$

(8) $r \to u$

(9) $p \to r$

(10) $p \to u$

(11) $p \to (t \land u)$ Use $(x \to y) \bigwedge (x \to z) \Leftrightarrow x \to (y \bigwedge z)$

(12) $\neg (t \land u) \to \neg p$

(13) $\neg (t \land u)$

(14) $\neg p$ ■

Indirect proof:

(1) p

(2) $p \to q$

(3) q

(4) $q \to t$

(5) t

(6) $\neg (t \land u)$

(7) $\neg t \lor \neg u$

(8) $\neg u$

(9) $s \to u$

(10) $\neg s$

(11) $r \to s$

(12) $\neg r$

(13) $p \to r$

(14) r

(15) 0 ■

(c) Direct proof:

(1) $\neg s \bigvee p$	Premise
(2) s	Added premise (conditional conclusion)
(3) $\neg (\neg s)$	Involution (2)
(4) p	Disjunctive simplification (1), (3)
(5) $p \to (q \to r)$	Premise

(6) $q \to r$ Detachment (4), (5)

(7) q Premise

(8) r Detachment (6), (7) ■

Indirect proof:

(1) $\neg (s \to r)$ Negated conclusion

(2) $\neg (\neg s \vee r)$ Conditional equivalence (I)

(3) $s \wedge \neg r$ DeMorgan (2)

(4) s Conjunctive simplification (3)

(5) $\neg s \vee p$ Premise

(6) $s \to p$ Conditional equivalence (5)

(7) p Detachment (4), (6)

(8) $p \to (q \to r)$ Premise

(9) $q \to r$ Detachment (7), (8)

(10) q Premise

(11) r Detachment (9), (10)

(12) $\neg r$ Conjunctive simplification (3)

(13) 0 Conjunction (11), (12) ■

(d) Direct proof:

(1) $p \to q$

(2) $q \to r$

(3) $p \to r$

(4) $p \vee r$

(5) $\neg p \vee r$

(6) $(p \vee r) \wedge (\neg p \vee r)$

(7) $(p \wedge \neg p) \vee r$

(8) $0 \vee r$

(9) r ■

Indirect proof:

(1) $\neg r$ Negated conclusion

(2) $p \vee r$ Premise

(3) p (1), (2)

(4) $p \to q$ Premise

(5) q Detachment (3), (4)

(6) $q \to r$ Premise

(7) r Detachment (5), (6)

(8) 0 (1), (7) ■

5. (a) Let W stand for "wages will increase," I stand for "there will be inflation," and C stand for "cost of living will increase." Therefore the

argument is: $W \to I$, $\neg I \to \neg C$, $W \Rightarrow C$.. The argument is invalid. The easiest way to see this is through a truth table. Let x be the conjunction of all premises.

W	I	C	$\neg I$	$\neg C$	$W \to I$	$\neg I \to \neg C$	x	$x \to C$
0	0	0	1	1	1	0	0	1
0	0	1	1	0	1	1	0	1
0	1	0	0	1	1	1	0	1
0	1	1	0	0	1	1	0	1
1	0	0	1	1	0	0	0	1
1	0	1	1	0	0	1	0	1
1	1	0	0	1	1	1	1	1
1	1	1	0	0	1	1	1	0

(b) Let r stand for "the races are fixed," c stand for "casinos are crooked," t stand for "the tourist trade will decline," and p stand for "the police will be happy." Therefore, the argument is:

$(r \vee c) \to t$, $t \to p$, $\neg p \to \neg r$. The argument is valid. Proof:

(1) $t \to p$ Premise

(2) $\neg p$ Premise

(3) $\neg t$ Indirect Reasoning (1), (2)

(4) $(r \vee c) \to t$ Premise

(5) $\neg (r \vee c)$ Indirect Reasoning (3), (4)

(6) $(\neg r) \wedge (\neg c)$ DeMorgan (5)

(7) $\neg r$ Conjunction simplification (6) ■

7. $p_1 \to p_k$ and $p_k \to p_{k+1}$ implies $p_1 \to p_{k+1}$. It takes two steps to get to $p_1 \to p_{k+1}$ from $p_1 \to p_k$ This means it takes $2\,(100 - 1)$ steps to get to $p_1 \to p_{100}$ (subtract 1 because $p_1 \to p_2$ is stated as a premise). A final step is needed to apply detachment to imply p_{100}

Section 3.6

1. (a) $\{\{1\}, \{3\}, \{1, 3\}, \emptyset\}$

(b) $\{\{3\}, \{3, 4\}, \{3, 2\}, \{2, 3, 4\}\}$

(c) $\{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{1, 2, 3, 4\}\}$

(d) $\{\{2\}, \{3\}, \{4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$

(e) $\{A \subseteq U : |A| = 2\}$

3. There are $2^3 = 8$ subsets of U, allowing for the possibility of 2^8nonequivalent

propositions over U.

5. s is odd and $(s - 1)\,(s - 3)\,(s - 5)\,(s - 7) = 0$

7. b and c

Section 3.7

1. We wish to prove that $P(n) : 1 + 3 + 5 + \cdots + (2 - n) = n^2$ is true for $n \geqslant 1$. *Note*: The nth odd positive integer is 2n - 1.

Basis: for $n = 1 : 1 = 1^2$

Induction: Assume that for some$n \geqslant 1$, $p(n)$ is true. Then:

$$\begin{aligned}1 + 3 + \cdots + (2\,(n + 1) - 1) + 1 &= [1 + 3 + \cdots + (2\,n - 1)] \\ &\quad +(2\,(n + 1) - 1) \\ &= n^2 + (2\,n + 1) \text{ by } p(n) \text{ and basic algebra} \\ &= (n + 1)^2 \ ■\end{aligned}$$

3. Proof: (a) Basis: $1 = 1\,(2)\,(3)/6 = 1$

(b) Induction: $\sum_{1}^{n+1} k^2 = \sum_{1}^{n} k^2 + (n+1)^2$

$$= \frac{n(n+1)(2n+1)}{6} + (n+1)^2$$
$$= \frac{(n+1)\left(2n^2+7n+6\right)}{6}$$
$$= \frac{(n+1)(n+2)(2n+3)}{6} \quad \blacksquare$$

5. Basis: For $n = 1$, we observe that $\frac{1}{(1\cdot 2)} = \frac{1}{(1+1)}$

Induction: Assume that for some $n \geqslant 1$, the formula is true.

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

$$= (n+2)(n) + \frac{1}{((n+1)(n+2))}$$
$$= \frac{(n+1)^2}{((n+1)(n+2))}$$
$$= \frac{(n+1)}{(n+2)} \quad \blacksquare$$

7. Let A_n be the set of strings of zeros and ones of length n (we assume that $|A_n| = 2^n$ is known), E_n = the even strings, and E_n^c = the odd strings. The problem is to prove that for $n \geqslant 1$, $|E_n| = 2^{n-1}$. Clearly, $|E^1| = 1$, and, if for some $n \geqslant 1$, $|E_n| = 2^{n-1}$, it follows that $|E_{n+1}| = 2^n$ by the following reasoning:

$E_{n+1} = \{1\,s : s \text{ in } E_n^c\} \bigcup \{0\,s : s \text{ in } E_n\}$

Since $\{1\,s : s \text{ in } E_n^c\}$ and $\{0\,s : s \text{ in } E_n\}$ are disjoint, we can apply the addition law. Therefore, $|E_{n+1}| = |E_n^c| + |E_n|$

$$= 2^{n-1} + (2^n - 2^{n-1}) = 2^n. \ \blacksquare$$

9. Assume that for n persons $(n \geqslant 1)$, $\frac{(n-1)n}{2}$ handshakes take place. If one more person enters the room, he or she will shake hands with n people, $\frac{(n-1)n}{2} + n = \frac{\left(n^2-n+2n\right)}{2} = \frac{n(n+1)}{2}$

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

Also, for $n = 1$, there are no handshakes: $\frac{(1-1)(1)}{2} = 0$. $\blacksquare$

11. Let $p(n)$ be "$a_1 + a_2 + \cdots + a_n$ has the same value no matter how it is evaluated."

Basis: $a_1 + a_2 + a_3$ may be evaluated only two ways. Since + is associative, $(a_1 + a_2) + a_3 = a_1 + (a_2 + a_3)$. Hence $p(3)$ is true.

Induction: Assume that for some $n \geqslant 3$ $p(3)$, $p(4)$, $\ldots$, $p(n)$ are all true. Now consider the sum $a_1 + a_2 + \cdots + a_{n+1}$. Any of the n additions in this expression can be applied last. If the jth addition is applied last, we have $c_j = \left(a_1 + a_2 + \cdots + a_j\right) + \left(a_{j+1} + \cdots + a_{n+1}\right)$. No matter how the expression to the left and right of the j^{th} addition are evaluated, the result will always be the same by the induction hypothesis, specifically $p(j)$ and $p(n+1-j)$. We now can prove that $c_1 = c_2 = \cdots = c_n$. If $i < j$,

$$c_i = (a_1 + a_2 + \cdots + a_i) + \left(\left(a_{i+1} + \cdots + a_j\right) + \left(a_{j+1} + \cdots + a_{n+1}\right)\right.$$
$$= (a_1 + a_2 + \cdots + a_i) + \left(\left(a_{i+1} + \cdots + a_j\right) + \left(a_{j+1} + \cdots + a_{n+1}\right)\right.$$
$$= \left((a_1 + \cdots + a_i) + \left(a_{i+1} + \cdots + a_j\right)\right) + \left(a_{j+1} + \cdots + a_{n+1}\right) \qquad \text{by } p(3)$$
$$= c_j$$

$$c_i = (a_1 + a_2 + \cdots + a_i) + \left(a_{i+1} + \cdots + a_j + a_{j+1} + \cdots + a_{n+1}\right) \qquad \text{definition of } c_i$$
$$= (a_1 + a_2 + \cdots + a_i) + \left(\left(a_{i+1} + \cdots + a_j\right) + \left(a_{j+1} + \cdots + a_{n+1}\right)\right) \qquad \text{by } p(n+1-i)$$
$$= \left((a_1 + \cdots + a_i) + \left(a_{i+1} + \cdots + a_j\right)\right) + \left(a_{j+1} + \cdots + a_{n+1}\right) \qquad \text{by } p(3)$$
$$= \left(a_1 + \cdots + a_i + a_{i+1} + \cdots + a_j\right) + \left(a_{j+1} + \cdots + a_{n+1}\right) \qquad \text{by } p(i)$$
$$= c_j \qquad \text{definition of } c_j \ \blacksquare$$

13. For $m \geqslant 1$, let $p(m)$ be $x^{n+m} = x^n\, x^m$ for all $n \geqslant 1$. The basis for this proof follows directly from the basis for the definition of exponentiation.

Induction: Assume that for some $m \geqslant 1$, $p(m)$ is true. Then

$x^{n+(m+1)} = x^{(n+m)+1}$ by associativity of integer addition

$= x^{n+m}\, x^1$ by recursive definition

$= x^n\, x^m\, x^1$ inductive hypothesis

$= x^n\, x^{m+1}$ recursive definition ■

Section 3.8

1. (a) $(\forall\, x)\,(F(x) \rightarrow G(x))$

(b) There are objects in the sea which are not fish.

Every fish lives in the sea.

3. (a) There is a book with a cover that is not blue.

(b) Every mathematics book that is published in the United States has a blue cover.

(c) There exists a mathematics book with a cover that is not blue.

(d) There exists a book that appears in the bibliography of every mathematics book.

(e) $(\forall\, x)\,(B(x) \rightarrow M(x))$

(f) $(\exists\, x)\,(M(x) \bigwedge \neg\, U(x))$

(g) $(\exists\, x)\,((\forall\, y)\,(\neg\, R(x,\, y))$

5. The equation $4\,u^2 - 9 = 0$ has a solution in the integers. (False)

7. (a) Every subset of U has a cardinality different from its complement. (True)

(b) There is a pair of disjoint subsets of U both having cardinality 5. (False)

(c) $A - B = B^c - A^c$ is a tautology. (True)

9.$(\forall\, a)_{\mathbb{Q}}\ (\forall\, b)_{\mathbb{Q}}(a + b$ is a rational number.)

11. Let $I = \{1,\, 2,\, 3,\, \ldots,\, n\}$

(a) $(\exists\, i)_I\,(x \in A_i)$

(b) $(\forall\, i)_I\,(x \in A_i)$

Section 3.9

1. The given statement can be written in if … , then … format as: If x and y are two odd positive integers, then $x + y$ is an even integer.

Proof: Assume x and y are two positive odd integers. It can be shown that $x + y = 2\,\cdot$(some positive integer).

x odd $\Rightarrow x = 2\,m + 1$ for some $m \in \mathbb{P}$,

y odd $\Rightarrow y = 2\,n + 1$ for some$n \in \mathbb{P}$.

Therefore, $x + y = (2\,m + 1) + (2\,n + 1) = 2\,((m + n) + 1) = 2\cdot$(some positive integer) so $x + y$ is even. ■

3. Proof: (Indirect) Assume to the contrary, that $\sqrt{2}$ is a rational number. Then there exists $p,\, q \in \mathbb{Z},\ (q \neq 0)$ where $\frac{p}{q} = \sqrt{2}$ and where $\frac{p}{q}$ is in lowest terms, that is, p and q have no common factor other than 1.

$\frac{p}{q} = \sqrt{2} \Rightarrow \frac{p^2}{q^2} = 2 \Rightarrow p^2 = 2\,q^2 \Rightarrow p^2$is an even integer $\Rightarrow p$ is an even integer (see Exercise 2) 4 is a factor of $p^2 \Rightarrow q^2 \Rightarrow$ is even $\Rightarrow q$ is even. Hence both p and q have a common factor, namely 2. Contradiction. ■

5. Proof: (Indirect) Assume $x,\, y \in \mathbb{R}$ and $x + y \leqslant 1$. Assume to the contrary that $\left(x \leqslant \frac{1}{2} \text{ or } y \leqslant \frac{1}{2}\right)$ is false, which is equivalent to $x > \frac{1}{2}$ and $y > \frac{1}{2}$. Hence $x + y > \frac{1}{2} + \frac{1}{2} = 1$. This contradicts the assumption that $x + y \leqslant 1$. ■

Supplementary Exercises—Chapter 3

1.(a)

p	$p \vee p$
0	0
1	1

(b)

p	$\neg p$	$p \wedge \neg p$
0	1	0
1	0	0

(c)

p	$\neg p$	$p \vee \neg p$
0	1	1
1	0	1

(d)

p	$p \wedge p$
0	0
1	1

3.

p	q	$\neg p$	$q \wedge \neg p$	$p \vee (q \wedge \neg p)$
0	0	1	0	0
0	1	1	1	1
1	0	0	0	1
1	1	0	0	1

5. Let $a = p \rightarrow \neg q$, $b = q \vee r$, and $c = (p \rightarrow \neg q) \wedge (q \vee r) \wedge \neg r$

p	q	r	$\neg q$	a	b	$a \wedge b$	$\neg r$	c	$\neg p$	$c \rightarrow \neg p$
0	0	0	1	1	0	0	1	0	1	1
0	0	1	1	1	1	1	0	0	1	1
0	1	0	0	1	1	1	1	1	1	1
0	1	1	0	1	1	1	0	0	1	1
1	0	0	1	1	0	0	1	0	0	1
1	0	1	1	1	1	1	0	0	0	1
1	1	0	0	0	1	0	1	0	0	1
1	1	1	0	0	1	0	0	0	0	1

7. An implication is always equivalent to its contrapositive, as can be seen in the table below.

p	q	$p \Rightarrow q$	$\neg q \Rightarrow \neg p$	$(p \Rightarrow q) \leftrightarrow (\neg q \Rightarrow \neg p)$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	1
1	1	1	1	1

9. The truth tables of $p \rightarrow (p \wedge q)$ and x must be equal.

p	q	$p \rightarrow (p \wedge q)$	x
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

11. (a) "3 is not a prime number or it is odd," or "3 is a composite number or it is odd."

(b) "4 is not a prime number and it is even," or "4 is a composite number and it is even."

(c) I can exhibit an example of a statement and I cannot prove it.

(d) $x^2 - 7x + 12 = 0$ and $x \neq 3$ and $x \neq 8$

13. (a)

p	q	$p \rightarrow q$	$\neg q \rightarrow \neg p$	$(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	1
1	1	1	1	1

(b)

p	q	$p \leftrightarrow q$	$p \to q$	$q \to p$	$(p \to q) \wedge (q \to p)$
0	0	1	1	1	1
0	1	0	1	0	0
1	0	0	0	1	0
1	1	1	1	1	1

Columns 3 and 6 are the same so $(p \leftrightarrow q) \Leftrightarrow [(p \to q) \wedge (q \to p)]$ is a tautology.

15. Let q = "I quit my job," s = "will starve," and w = "I did my work." In symbolic form, the argument is $(q \to s) \wedge (\neg w \to q) \wedge w \Rightarrow \neg s$. The truth table for $x = (q \to s) \wedge (\neg w \to q) \wedge w \to \neg s$ does not consist of all ones. For example, when q is false, s is true and when w is true, x is false. Therefore, x is not a tautology and the argument is not valid.

17. $[(m \to p) \wedge (e \vee \neg p) \wedge \neg e] \Rightarrow \neg m$. Valid

Proof: (Direct)

(1) $e \vee \neg p$ Premise

(2) $\neg e$ Premise

(3) $\neg p$ (1), (2), disjunctive simplification

(4) $m \to p$ Premise

(5) $\neg m$ (3), (4), indirect reasoning ■

19. $[(\neg p \to \neg q \wedge \neg r \wedge (p \to s) \wedge (q \vee r) \Rightarrow s$. Valid

Proof: (Direct)

(1) $\neg p \to \neg q$ Premise

(2) $q \to p$ (1), Contrapositive

(3) $p \to s$ Premise

(4) $q \to s$ (2), (3), Chain rule

(5) $q \vee r$ Premise

(6) $\neg r$ Premise

(7) q (5), (6), Disjunctive simplification

(8) s (4), (7), Detachment ■

(Indirect)

(1) $\neg s$ Negated conclusion

(2) $p \to s$ Premise

(3) $\neg p$ (1), (2), Indirect Reasoning

(4) $\neg p \to \neg q$ Premise

(5) $\neg q$ (3), (4), Detachment

(6) $q \vee r$ Premise

(7) r (5), (6), Disjunctive simplification

(8) $\neg r$ Premise

(9) 0 (7), (8) ■

21. $e \to i,\ i \to d,\ d \to w \Rightarrow e \to w$

Proof:

(1) $e \to i$	Premise
(2) $i \to d$	Premise
(3) $e \to d$	(1), (2), Chain rule
(4) $d \to w$	Premise
(5) $e \to w$	(3), (4), Chain rule ■

23. Valid. Statement: $t \lor d,\ \neg e \lor j,\ \neg j \lor r \Rightarrow \neg t \to r$

Proof: (direct)

(1) $t \lor d$	Premise
(2) $\neg t \to d$	(1), Conditional equivalence
(3) $\neg d \lor j$	Premise
(4) $d \to j$	(3), Conditional equivalence
(5) $\neg j \lor r$	Premise
(6) $j \to r$	(5), Conditional equivalence
(7) $\neg t \to r$	(2), (4), (6), Chain rule ■

25. (1) First show $T_{p \land q} \subseteq T_p \cap T_q$

$a \in T_{p \land q}$ $\Rightarrow a$ makes $p \land q$ true

$\Rightarrow a$ makes p true and a makes q true

$\Rightarrow a \in T_p$ and $a \in T_q$

$\Rightarrow a \in T_p \cap T_q$

(2) To prove $T_p \cap T_q \subseteq T_{p \land q}$ reverse the above steps. ■

27. $60 = 6 \cdot 10 = 2 \cdot 3 \cdot 2 \cdot 5 = 2^2 \cdot 3 \cdot 5$
$120 = 2 \cdot 60 = 2^3 \cdot 3 \cdot 5$

29 (a) $\binom{n}{k-1} + \binom{n}{k} = \dfrac{n!}{(n-(k-1))!\,(k-1)!} + \dfrac{n!}{(n-k)!\,k!}$

$$= \frac{n!}{(n-k+1)!\,(k-1)} + \frac{n!}{(n-k)!\,k!}$$

$$= \frac{n!\,k + n!\,(n-k+1)}{(n-k+1)!\,k!}$$

$$= \frac{n!\,(n+1)}{(n-k+1)!\,k!} = \frac{(n+1)!}{(n+1-k)!\,k!}$$

$$= \binom{n+1}{k} \quad ■$$

(b) Basis: $(n = 1) : (x+y)^1 = x + y$.

$$\sum_{k=0}^{1} \binom{1}{k} x^{1-k} y^k = \binom{1}{0} x + \binom{1}{1} y = x + y$$

Induction: Assume $n \geqslant 1$ and $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$.

We will now prove $(x+y)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k$.

$(x+y)^{n+1} = (x+y)\,(x+y)^n$

$= (x+y)\sum_{k=0}^{n}\binom{n}{k}x^{n-k}\,y^k$ By induction hypothesis

$= x\sum_{k=0}^{n}\binom{n}{k}x^{n-k}\,y^k + y\sum_{k=0}^{n}\binom{n}{k}x^{n-k}\,y^k$ distribution

$= \sum_{k=0}^{n}\binom{n}{k}x^{n+1-k}\,y^k + \sum_{k=0}^{n}\binom{n}{k}x^{n-k}\,y^k + 1$

Let $k = k - 1$ in the second summation; remember to increase top.

$= \sum_{k=0}^{n}\binom{n}{k}x^{n+1-k}\,y^k + \sum_{k=1}^{n+1}\binom{n}{k-1}x^{n-k+1}\,y^k$ +

$= \binom{n}{0}x^{n+1} + \sum_{k=1}^{n}\binom{n}{k}x^{n+1-k}\,y^k + \sum_{k=1}^{n}\binom{n}{k-1}x^{n+1-k}\,y^k + \binom{n}{n}y^{n+1}$

$= \binom{n}{0}x^{n+1} + \sum_{k=1}^{n}\left[\binom{n}{k}+\binom{n}{k-1}\right]x^{n+1-k}\,y^k + \binom{n}{n}y^{n+1}$

$= \binom{n}{0}x^{n+1} + \sum_{k=1}^{n}\binom{n+1}{k}x^{n+1-k}\,y^k + \binom{n}{n}y^{n+1},$

But $\binom{n}{0} = \binom{n+1}{0} = 1$ and $\binom{n}{n} = \binom{n+1}{n+1} = 1$

$= \sum_{k=0}^{n+1}\binom{n+1}{0}x^{n+1-k}\,y^k.$

31. $\neg\,(\exists\, x)\,((\forall\, y)\,(D(x) \land T(y))) \Rightarrow (\forall\, x)\,(\neg\,(\forall\, y)\,(D(x) \land T(y)))$
$\Rightarrow (\forall\, x)\,((\exists\, y)\,(\neg\,(D(x) \land T(y))))$
$\Rightarrow (\forall\, x)\,((\exists\, y)\,(\neg\, D(x) \lor \neg\, T(y)))$
⇒ All sailing is not dangerous or some fishing is not tedious.

33. (a) Let U be the universe of all fish, $k(x)$ ="x is kind to children," and $s(x)$ ="x is a shark." $(\forall\, x)_U\,(\neg\, s(x) \to k(x))$

(b) Let $w(x)$ = "x is a wine drinker,"

$c\,(x)$ ="x is very communicative,"

$p(x)$ = "x is a pawnbroker,"

and $h(x)$ = "x is honest";

then $(\forall\, x)\,((\exists\, y)\,((w(x) \to c(x)) \lor (p(y) \to (h(x) \land \neg\, w(y)))))$

(c) Let $p(x)$ = "x is a clever philosopher,"

$c(x)$ = "x is a cynic,"

and $w(x)$ = "x is a woman"; then

$(\forall\, x)\,((\exists\, y)\,(((p(x) \to c(x)) \land (w(x) \to p(x))) \to (p(y) \to (w(y) \to c(y)))))$

35. $(\forall\, a)_{\mathbb{R}} + (\forall\, b)_{\mathbb{R}} + (\exists\, n)_{\mathbb{P}}\,(na > b)$

CHAPTER 4

Section 4.1

1. (a) Assume that $x \in A$ (condition of the conditional conclusion $A \subseteq C$). Since $A \subseteq B$, $x \in B$ by the definition of $\subseteq$. $B \subseteq C$ and $x \in B$ implies that $x \in C$ Therefore, if $x \in A$, then $x \in C$. ■

(b) (Proof that $A - B \subseteq A \cap B^c$) Let x be in $A - B$. Therefore, x is in A, but it is not in B; that is, $x \in A$ and $x \in B^c \Rightarrow x \in A \cap B^c$. ■

(c) (⇒) Assume that $A \subseteq B$ and $A \subseteq C$. Let $x \in A$. By the two premises, $x \in B$ and $x \in C$. Therefore, by the definition of intersection, $x \in B \cap C$. ■

(d) (⇒) (Indirect) Assume that $A \subseteq C$ and B^c is not a subset of A^c . Therefore, there exists $x \in B^c$ that does not belong to A^c. $x \notin A^c \Rightarrow x \in A$. Therefore, $x \in A$ and $x \notin B$, a contradiction to the assumption that $A \subseteq B$. ■

3. (a) If $A = \mathbb{Z}$ and $B = \emptyset$, $A - B = \mathbb{Z}$, while $B - A = \emptyset$.

(b) If $A = \{0\}$ and $B = \{1\}$, $(0, 1) \in A \times B$, but $(0, 1)$ is not in $B \times A$.

(c) Let $A = \emptyset$, $B = \{0\}$, and $C = \{1\}$.

5. Proof: Let $p(n)$ be

$$A \bigcap (B_1 \bigcup B_2 \bigcup \cdots \bigcup B_n) \\ = (A \bigcap B_1) \bigcup (A \bigcap B_2) \bigcup \cdots \bigcup (A \bigcap B_n).$$

Basis: We must show that $p(2) : A \bigcap (B_1 \bigcup B_2) = (A \bigcap B_1) \bigcup (A \bigcap B_2)$ is true. This was done by several methods in section 4.1.

Induction: Assume for some $n \geq 2$ that $p(n)$ is true. Then

$A \bigcap (B_1 \bigcup B_2 \bigcup \cdots \bigcup B_{n+1}) = A \bigcap [(B_1 \bigcup B_2 \bigcup \cdots \bigcup B_n) \bigcup B_{n+1}]$

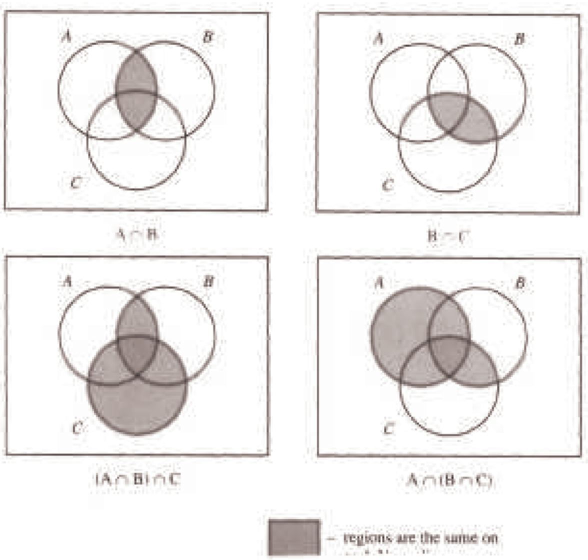
$= (A \bigcap (B_1 \bigcup B_2 \bigcup \cdots \bigcup B_n)) \bigcup (A \bigcap B_{n+1})$
by $p(2)$

$= ((A \bigcap B_1) \bigcup \cdots \bigcup (A \bigcap B_n)) \bigcup (A \bigcap B_{n+1})$
by the induction hypothesis

$= (A \bigcap B_1) \bigcup \cdots \bigcup (A \bigcap B_n) \bigcup (A \bigcap B_{n+1})$ ■

Section 4.2

1. (a)



(b)

A	B	A^c	B^c	$A \bigcup B$	$(A \bigcup B)^c$	$A^c \bigcap B^c$
0	0	1	1	0	1	1
0	1	1	0	1	0	0
1	0	0	1	1	0	0
1	1	0	0	1	0	0

The last two columns are the same so the two sets must be equal.

(c) (i)$x \in A \bigcup A \Rightarrow x \in A$ or $x \in A$ by the definition of $\bigcap$
$\Rightarrow x \in A$ by the idempotent law of logic
Therefore, $A \bigcup A \subseteq A$.

(ii) $x \in A \Rightarrow x \in A$ and $x \in A$ by conjunctive addition
$\Rightarrow x \in A \bigcup A$
Therefore, $A \subseteq A \bigcup A$ and so we have $A \bigcup A = A$. ■

3. For all parts of this exercise, a reason should be supplied for each step. We have supplied reasons for part a only and left them out of the other parts to give you further practice.

(a) $A \bigcup (B - A) = A \bigcup (B \bigcap A^c)$ by Exercise 2b of Section 4.1
$= (A \bigcup B) \bigcap (A \bigcup A^c)$ by the distributive law
$= (A \bigcup B) \bigcap U$ by the null law
$= (A \bigcup B)$ by the identity law ■

(b) $A - B = A \bigcap B^c$
$= B^c \bigcap A$
$= B^c \bigcap (A^c)^c$
$= B^c - A^c$

(c) Select any element, x, in $A \bigcap C$. One such element exists since $A \bigcap C$ is not empty.
$x \in A \bigcap C \Rightarrow x \in A$ and $x \in C$
$\Rightarrow x \in B$ and $x \in C$
$\Rightarrow x \in B \bigcap C$
$\Rightarrow B \bigcap C \neq \emptyset$ ■

(d) $A \bigcap (B - C) = A \bigcap (B \bigcap C^c)$
$= (A \bigcap B \bigcap A^c) \bigcup (A \bigcap B \bigcap C^c)$
$= (A \bigcap B) \bigcap (A^c \bigcup C^c)$
$= (A \bigcap B) \bigcap (A \bigcup C)^c$
$= (A - B) \bigcap (A - C)$ ■

(e) $A - (B \bigcup C) = A \bigcap (B \bigcup C)^c$

$= A \bigcap (B^c \bigcap C^c)$

$= (A \bigcap B^c) \bigcap (A \bigcap C^c)$

$= (A - B) \bigcap (A - C)$ ■

5. (a) $A \overset{3}{\bigcup} B^{\overset{1}{c}} \overset{2}{\bigcap} C$ (b) $A \overset{1}{\bigcap} B \overset{3}{\bigcup} C \overset{2}{\bigcap} B$ (c) $A \overset{2}{\bigcup} B \overset{3}{\bigcup} C^{\overset{1}{c}}$

Section 4.3

1. (a) {1}, {2, 3, 4, 5}, {6}, {7, 8}, {9, 10}

(b) 2^5 , as compared with 2^{10}. {1, 2} is one of the 992 sets that can't be generated.

3. $B_1 = \{00, 01, 10, 11\}$ and $B_2 = \{0, 00, 01\}$ generate minsets {00, 01}, {0}, {10, 11}, and $\{\lambda, 1\}$. *Note:* λ is the null string, which has length zero.

5. (a) $B_1 \bigcap B_2 = \emptyset$

$B_1 \bigcap B^c{}_2 = \{0, 2, 4\}$

$B^c{}_1 \bigcap B_2 = \{1, 5\}$

$B^c{}_1 \bigcap B^c{}_2 = \{3\}$

(b) 2^3 , since there are 3 nonempty minsets.

7. Let $a \in A$. For each i, $a \in B_i$, or $a \in B_i{}^c$, since $B_i \bigcup B_i{}^c = A$ by the complement law. Let $D_i = B_i$ if $a \in B_i$, and $D = B_i{}^c$ otherwise. Since a is in each D_i, it must be in the minset $D_1 \bigcap D_2 \cdots \bigcap D_n$. Now consider two different minsets $M_1 = D_1 \bigcap D_2 \cdots \bigcap D_n$, and $M_2 = G_1 \bigcap G_2 \cdots \bigcap G_n$, where each D_i and G_i is either B_i or $B_i{}^c$. Since these minsets are not equal, $D_i \neq G_i$, for some i. Therefore, $M_1 \bigcap M_2 = D_1 \bigcap D_2 \cdots \bigcap D_n \bigcap G_1 \bigcap G_2 \cdots \bigcap G_n = \emptyset$, since two of the sets in the intersection are disjoint. Since every element of A is in a minset and the minsets are disjoint, the nonempty minsets must form a partition of A. ■

Section 4.4

1. (a) $A \bigcap (B \bigcup A) = A$

(b) $A \bigcap ((B^c \bigcap A) \bigcup B)^c = \emptyset$

(c) $(A \bigcap B^c)^c \bigcup B = A^c \bigcup B$

3. (a) $(p \land \neg (\neg q \land p) \lor g)) \Leftrightarrow 0$

(b) $(\neg (p \lor (\neg q)) \land q) \Leftrightarrow ((\neg p) \land q)$

5. The maxsets are:

$B_1 \bigcup B_2 = \{1, 2, 3, 5\}$

$B_1 \bigcup B_2{}^c = \{1, 3, 4, 5, 6\}$

$B_1{}^c \bigcup B_2 = \{1, 2, 3, 4, 6\}$

$B_1{}^c \bigcup B_2{}^c = \{2, 4, 5, 6\}$

They do not form a partition of A since it is not true that the intersection of any two of them is empty. A set is said to be in *maxset normal form* when it is expressed as the intersection of distinct nonempty maxsets or it is the universal set U.

Supplementary Exercises—Chapter 4

1. (a) Proof: (⇒) (Indirect) Assume $A \subseteq B$ and $A \bigcup (U - B) \neq \emptyset$. To prove that this cannot occur, let $x \in A \bigcap (U - B)$.

$x \in A \bigcap (U - B)$
Definition of complement $\Rightarrow x \in A \bigcap B^c$
Definition of $\bigcap$ $\Rightarrow x \in A$ and $x \in B^c$
Definition of complement $\Rightarrow x \in A$ and $x \notin B$
Definition of subset $\Rightarrow A$ is not a subset of B

This contradicts the premise that $A \subseteq B$. Hence this part of the statement is proven.

(⇐) (Indirect) Assume $A \bigcap (U - B) = \emptyset$, and A is not a subset of B. To prove that this cannot occur, let $x \in A$ such that $x \notin B$.

$x \in A$ and $x \notin B$
Definition of complement $\Rightarrow x \in A$ and $x \in B^c$
Definition of $\bigcap$ $\Rightarrow x \in A \bigcap B^c$
Definition of complement $\Rightarrow x \in A \bigcap (U - B)$
Definition of disjoint $\Rightarrow A \bigcap (U - B) \neq \emptyset$

But this cannot happen because it contradicts the assumption that $A \bigcap (U - B) = \emptyset$. Hence this part of the statement is proven and the proof is complete.

(b) Proof: (Indirect) Assume $U = A \bigcup B$, $A \bigcap B = \emptyset$, and $A \neq U - B$. One way in which A and $U - B$ can be not equal is that A is not a subset of $U - B$. Let $x \in A$ and $x \notin U - B$.

$x \in A$ and $x \notin U - B$
Definition of complement $\Rightarrow x \in A$ and $x \in B$
Definition of $\bigcap$ $\Rightarrow x \in A \bigcap B$
Definition of disjoint $\Rightarrow A \bigcap B \neq \emptyset$

But this cannot happen because it contradicts the assumption that $A \bigcap B = \emptyset$. The other way A and $U - B$ can differ is if $U - B$ is not a subset of A, Let $x \notin A$ and $x \in U - B$. We could infer from this assumption that $x \notin A \bigcup B$. Therefore, any way that we assume that $A \neq U - B$ leads to a contradiction.

(c) Proof: (⇒) (Direct) Let $x \in A$.
A and B are disjoint
Definition of disjoint $\Rightarrow x \notin B$
Definition of complement $\Rightarrow x \in B^c$
Therefore, $A \subseteq B^c$

(⇐) (Indirect) Assume that $A \subseteq B^c$ and $x \in A \bigcap B$.
$x \in A \bigcap B$
Definition of intersection $\Rightarrow x \in A$ and $x \in B$
Definition of complement $\Rightarrow x \in A$ and $x \notin B^c$
Definition of subset $\Rightarrow$ A is not a subset of B^c ■

3. (a) Proof: (Direct) Let A, B, and C be sets.
Let $(x, y) \in (A \bigcup B) \times C$.
Definition of Cartesian product $\Rightarrow x \in (A \bigcup B)$ and $y \in C$
Definition of $\bigcup$ $\Rightarrow (x \in A$ or $x \in B)$ and $y \in C$
Distributive law of logic $\Rightarrow$ $(x \in A$ and $y \in C)$ or $(x \in B$ and $y \in C)$
Definition of Cartesian product $\Rightarrow$ $((x, y) \in A \times C)$ or
$((x, y) \in B \times C)$
Definition of $\bigcup$ $\Rightarrow$ $(x, y) \in (A \times C) \bigcup (B \times C)$ ■

(b) We proved $(A \bigcup B) \times C \subseteq (A \times C) \bigcup (B \times C)$ in part a; we now must show $(A \times C) \bigcup (B \times C) \subseteq (A \bigcup B) \times C$ and we will be finished.

5. Proof: (Indirect) Assume A, B, and C are subsets of U, $A \subseteq B$, $B \subseteq C$ and C^c is not a subset of A^c. To prove that this cannot occur, let $x \in C^c$ and $x \notin A^c$ by definition of subset.

$x \in C^c$ and $x \notin A^c$
Definition of complement $\Rightarrow x \notin C$ and $x \in A$
Premise $\Rightarrow A \subseteq B$
Definition of subset $\Rightarrow x \in B$
Premise $\Rightarrow B \subseteq C$
Definition of subset $\Rightarrow x \in C$ (Contradiction) ■

7. (a) Proof: (Indirect) Let A, B, and C be sets. Assume $A \cup C \neq B \cup C$ and $A = B$.

$A = B \Rightarrow A \subseteq B$
$x \in A \cup C$
Definition of union $\Rightarrow x \in A$ or $x \in C$
Definition of subset $\Rightarrow x \in B$ or $x \in C$
Definition of union $\Rightarrow x \in B \cup C$

Therefore, $A \cup C \subseteq B \cup C$. By a similar line of reasoning we can infer $B \cup C \subseteq A \cup C$, which proves that $A \cup C = B \cup C$, a contradiction.

(b) Proof: (Direct) Assume $A \neq B$ and show $A^c \neq B^c$. Since $A \neq B$ we can assume that A is not a subset of B. The alternative is that B is not a subset of A and the remaining logic would be identical.

A not a subset of B
Definition of subset $\Rightarrow x \in A$ and $x \notin B$
Definition of complement $\Rightarrow x \notin A^c$ and $x \in B^c$
Definition of subset $\Rightarrow B^c$ is not a subset of A^c
Definition of inequality $\Rightarrow A^c \neq B^c$ ■

9. (a) The minsets are $B_1 \cap B_2 = \{3\}$, $B_1{}^c \cap B_2 = \{2, 5\}$, $B_1 \cap B_2{}^c = \{1\}$, and $B_1{}^c \cap B_2{}^c = \{4, 6\}$

(b) The minsets are disjoint and
$(B_1 \cap B_2) \cup (B_1{}^c \cap B_2) \cup (B_1 \cap B_2{}^c) \cup (B_1{}^c \cap B_2{}^c) = U$,
so the minsets form a partition of U.

CHAPTER 5

Sections 5.1-5.3

1. For parts c, d and i of this exercise, only a verification is needed. Here, we supply the result that will appear on both sides of the equality.

(a) $AB = \begin{pmatrix} -3 & 6 \\ 9 & -13 \end{pmatrix}$ $BA = \begin{pmatrix} 2 & 3 \\ -7 & -18 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 0 \\ 5 & -2 \end{pmatrix}$

(c) $\begin{pmatrix} 3 & 0 \\ 15 & -6 \end{pmatrix}$ (d) $\begin{pmatrix} 18 & -15 & 15 \\ -39 & 35 & -35 \end{pmatrix}$ (e) $\begin{pmatrix} -12 & 5 & -5 \\ 5 & -25 & 25 \end{pmatrix}$

(f) $B + 0 = B$ (g) $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ (h) $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ (i) $\begin{pmatrix} 5 & -5 \\ 10 & 15 \end{pmatrix}$

3. $\begin{pmatrix} 1/2 & 0 \\ 0 & 1/3 \end{pmatrix}$

5. $A^3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 27 \end{pmatrix}$ $A^{15} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 32\,768 & 0 \\ 0 & 0 & 14\,348\,907 \end{pmatrix}$

7. (a) $Ax = \begin{pmatrix} 2x_1 + 1x_2 \\ 1x_1 - 1x_2 \end{pmatrix}$ equals $\begin{pmatrix} 3 \\ 1 \end{pmatrix}$ if and only if both of the equalities
$2x_1 + x_2 = 3$ and $x_1 - x_2 = 1$ are true.

(b) (i) $A = \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$ $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ $B = \begin{pmatrix} 4 \\ 0 \end{pmatrix}$

(ii) $A = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & -1 \\ 1 & 3 & 1 \end{pmatrix}$ $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ $B = \begin{pmatrix} 1 \\ -1 \\ 5 \end{pmatrix}$

(iii) $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 3 \end{pmatrix}$ $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ $B = \begin{pmatrix} 3 \\ 5 \\ 6 \end{pmatrix}$

Section 5.4

1. (a) $\begin{pmatrix} -1/5 & 3/5 \\ 2/5 & -1/5 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$ (c) No inverse exists.

(d) $A^{-1} = A$ (e) $\begin{pmatrix} 1/3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1/5 \end{pmatrix}$

3. Let A and B be n by n invertible matrices. Prove $(AB)^{-1} = B^{-1} A^{-1}$.

Proof: $$\begin{aligned}(B^{-1} A^{-1})(AB) &= (B^{-1})(A^{-1}(AB)) \\ &= (B^{-1})((A^{-1} A) B)) \\ &= (B^{-1})(IB) \\ &= (B^{-1})(B) \\ &= I\end{aligned}$$

Similarly, $(AB)(B^{-1} A^{-1}) = I$.

By Theorem 5.4.1, $B^{-1} A^{-1}$ is the only inverse of AB, If we tried to invert AB with $A^{-1} B^{-1}$, we would be unsuccessful since we cannot rearrange the order of the matrices.

5. (b) $1 = \det I = \det\left(A A^{-1}\right) = \det A \ \det A^{-1}$. Now solve for $\det A^{-1}$.

7. **Basis**: $(n = 1)$: $\det A^1 = \det A = (\det A)^1$.

Induction: Assume $\det A^n = (\det A)^n$ for some $n \geq 1$.

$$\begin{aligned}\det A^{n+1} &= \det(A^n A) && \text{by the definition of exponents} \\ &= \det(A^n)\det(A) && \text{by exercise 5} \\ &= (\det A)^n (\det A) && \text{by the induction hypothesis} \\ &= (\det A)^{n+1}\end{aligned}$$

9. (a) Assume $A = BDB^{-1}$

Basis:$(m = 1)$: A^1 $= BD^1 B^{-1}$ is given.

Induction: Assume that for some positive integer m, $A^m = BD^m B^{-1}$

$$\begin{aligned}A^{m+1} &= A^m A \\ &= (\mathrm{BD}^m B^{-1})\left(\mathrm{BDB}^{-1}\right) && \text{by the induction hypothesis} \\ &= BD^m DB^{-1} && \text{by associativity, definition of inverse} \\ &= BD^{m+1} B^{-1}\end{aligned}$$

(b) $A^{10} = BD^{10} B^{-1} = \begin{pmatrix} -9206 & 15\,345 \\ -6138 & 10\,231 \end{pmatrix}$

Section 5.5

1. (1) Let A and B be m by n matrices. Then $A + B = B + A$,
(2) Let A, B, and C be m by n matrices. Then $A + (B + C) = (A + B) + C$.
(3) Let A and B be m by n matrices, and let $c \in \mathbb{R}$. Then $c(A + B) = cA + cB$,
(4) Let A be an m by n matrix, and let $c_1, c_2 \in \mathbb{R}$. Then $(c_1 + c_2) A = c_1 A + c_2 A$.
(5) Let A be an m by n matrix, and let $c_1, c_2 \in \mathbb{R}$. Then $c_1(c_2 A) = (c_1 c_2) A$
(6) Let $\mathbf{0}$ be the zero matrix, of size m by n, and let A be a matrix of size n by r. Then $\mathbf{0} A = \mathbf{0}$ = the m by r zero matrix.
(7) Let A be an m by n matrix, and 0 = the number zero. Then $0 A = 0$ = the m by n zero matrix.
(8) Let A be an m by n matrix, and let $\mathbf{0}$ be the m by n zero matrix. Then $A + \mathbf{0} = A$.
(9) Let A be an m by n matrix. Then $A + (-1) A = \mathbf{0}$, where $\mathbf{0}$ is the m by n zero matrix.
(10) Let A, B, and C be m by n, n by r, and n by r matrices respectively. Then $A(B + C) = AB + AC$.
(11) Let A, B, and C be m by n, r by m, and r by m matrices respectively. Then $(B + C) A = \mathrm{BA} + \mathrm{CA}$.
(12) Let A, B, and C be m by n, n by r, and r by p matrices respectively. Then $A(BC) = (AB) C$.
(13) Let A be an m by n matrix, I_m the m by m identity matrix, and I_n the n by n identity matrix. Then $I_m A = AI_n = A$
(14) Let A be an n by n matrix. Then if A^{-1} exists, $(A^{-1})^{-1} = A$.
(15) Let A and B be n by n matrices. Then if A^{-1} and B^{-1} exist, $(AB)^{-1} = B^{-1} A^{-1}$.

3. (a) $\mathrm{AB} + \mathrm{AC} = \begin{pmatrix} 21 & 5 & 22 \\ -9 & 0 & -6 \end{pmatrix}$

(b) $A(B + C) = AB + AC$

(c) $A^{-1} = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} = A$

(d) $(A^2)^{-1} = (AA)^{-1} = \left(AA^{-1}\right)^{-1} = I^{-1} = I$ by part c

Section 5.6

1. In elementary algebra (the algebra of real numbers), each of the given oddities does not exist.

(i) AB may be different from BA. Not so in elementary algebra, since $ab = ba$ by the commutative law of multiplication.
(ii) There exist matrices A and B such that $AB = \mathbf{0}$, yet $A \neq \mathbf{0}$ and $B \neq \mathbf{0}$. In elementary algebra, the only way $ab = 0$ is if either a or b is zero. There are no exceptions.
(iii) There exist matrices A, $A \neq \mathbf{0}$, yet $A^2 = \mathbf{0}$. In elementary algebra, $a^2 = 0 \Leftrightarrow a = 0$.
(iv) There exist matrices $A^2 = A$. where $A \neq \mathbf{0}$ and $A \neq I$. In elementary algebra, $a^2 = a \Leftrightarrow a = 0$ or 1.
(v) There exist matrices A where $A^2 = I$ but $A \neq I$ and $A \neq -I$. In elementary algebra, $a^2 = 1 \Leftrightarrow a = 1$ or -1.

3. (a) $\det A \neq 0 \Rightarrow A^{-1}$ exists, and if you multiply the equation $A^2 = A$ on both sides by A^{-1} , you obtain $A = I$.

(b) Counterexample: $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

5. (a) $A^{-1} = \begin{pmatrix} 1/3 & 1/3 \\ 1/3 & -2/3 \end{pmatrix}$ $x_1 = 4/3$, and $x_2 = 1/3$

(b) $A^{-1} = \begin{pmatrix} 1 & -1 \\ 1 & -2 \end{pmatrix}$ $x_1 = 4$, and $x_2 = 4$

(c) $A^{-1} = \begin{pmatrix} 1/3 & 1/3 \\ 1/3 & -2/3 \end{pmatrix}$ $x_1 = 2/3$, and $x_2 = -1/3$

(d) $A^{-1} = \begin{pmatrix} 1/3 & 1/3 \\ 1/3 & -2/3 \end{pmatrix}$ $x_1 = 0$, and $x_2 = 1$

(e) The matrix of coefficients for this system has a zero determinant; therefore, it has no inverse. The system cannot be solved by this method. In fact, the system has no solution.

Supplementary Exercises—Chapter 5

1. $\begin{pmatrix} x+y & 5 \\ -2 & x-y \end{pmatrix} = \begin{pmatrix} 3 & 5 \\ -2 & 4 \end{pmatrix} \Rightarrow \begin{cases} x+y=3 \\ x-y=4 \end{cases} \Rightarrow \begin{cases} y=-1/2 \\ x=7/2 \end{cases}$

3. For $n \geq 1$ let $p(n)$ be $AB^n = B^n A$

Basis:($n = 1$): $\mathrm{AB}^1 = B^1 A$ is true as given in the statement of the problem. Therefore, $p(1)$ is true.

Induction: Assume $n \geq 1$ and $p(n)$ is true.

$$\begin{aligned} AB^{n+1} &= (AB^n)B \\ &= (B^n A)B && \text{By the induction hypothesis} \\ &= (B^n B)A && \text{By } p(l) \\ &= B^{n+1}A && \blacksquare \end{aligned}$$

5. $A^{-1} A^3 = A^2 = \begin{pmatrix} 7 & 18 \\ 6 & 19 \end{pmatrix}$

7. D has no inverse if $\det D = 0$.

$\det D = 0 \Leftrightarrow 3c - f(15) = 3c - 60 = 0 \Leftrightarrow c = 20$

9. (a) $(A+B)^2 = A^2 + AB + BA + B^2$
(b) $(A+B)^2 = A^2 + 2AB + B^2$ only if $AB = BA$.

11. The implication is false. Both $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ are self-inverting, but their product is not.

13. Yes, matrices of the form $A = \begin{pmatrix} a & b \\ (1-a)^2/b & -a \end{pmatrix}$ also solve $A^2 = I$

CHAPTER 6

Section 6.1

1. (a) $(2, 4),\ (2, 8)$ (b) $(2,\ 3),\ (2,\ 4),\ (5, 8)$ (c) $(1, 1),\ (2, 4)$

3. (a) $r = \{(1, 2),\ (2, 3),\ (3, 4),\ (4, 5)\}$

(b) $r^2\ = \{(1, 3),\ (2, 4),\ (3, 5)\} = \{(x, y)\ :\ y = x + 2,\ x, y \in A\}$

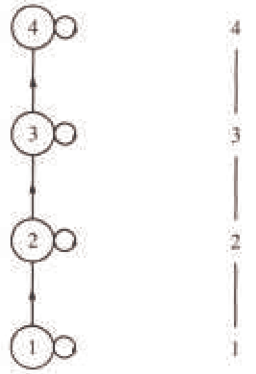
(c) $r^3 = \{(1, 4),\ (2, 5)\} = \{(x, y)\ :\ y = x + 3,\ x, y\ \in\ A\}$

5. (a) When $n = 3$, there are 27 pairs in the relation.

(b) Imagine building a pair of disjoint subsets of S. For each element of S there are three places that it can go: into the first set of the ordered pair, into the second set, or into neither set. Therefore the number of pairs in the relation is 3^n, by the product rule.

Section 6.2

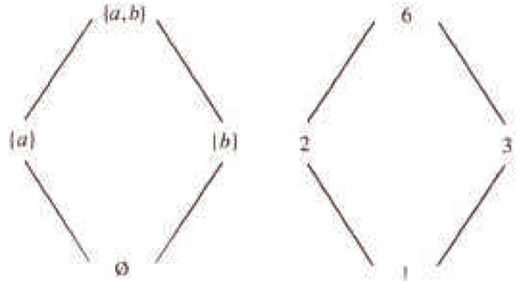
1.



3. See Figure 13.1.1 of Section 13.1.

5. A Hasse diagram cannot be used because not every set is related to itself. Also, $\{a\}$ and $\{b\}$ are related in both directions.

Section 6.3



(c) The graphs are the same if we disregard the names of the vertices.

3. (a)	(i)	reflexive not symmetric not antisymmetric transitive	(ii)	reflexive not symmetric antisymmetric transitive	(iii)	not reflexive not symmetric not antisymmetric not transitive
	(iv)	not reflexive symmetric antisymmetric transitive	(v)	reflexive symmetric not antisymmetric transitive	(vi)	reflexive not symmetric antisymmetric transitive
	(vii)	not reflexive not symmetric not antisymmetric not transitive				

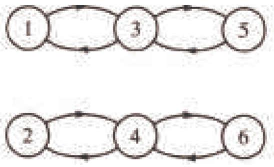
(b) Graphs ii and vi show partial ordering relations. Graph v is of an equivalence relation.

5. (a) No, since for example $|1 - 1| = 0 \neq 2$

(b) Yes, since $|i - j| = |j - i|$

(c) No, since $|2 - 4| = 2$ and $|4 - 6| = 2$, but $|2 - 6| = 4 \neq 2$.

(d)



7. (b) $c(0) = \{0\}$, $c(1) = \{1, 2, 3\} = c(2) = c(3)$

(c) $c(0) \bigcup c(1) = A$ and $c(0) \bigcap c(1) = \emptyset$

(d) Let A be any set and let r be an equivalence relation on A. Let a be any element of A. $a \in c(a)$ since r is reflexive, so each element of A is in some equivalence class. Therefore, the union of all equivalence classes equals A. Next we show that any two equivalence classes are either identical or disjoint and we are done. Let $c(a)$ and $c(b)$ be two equivalence classes, and assume that $c(a) \bigcap c(b) \neq \emptyset$. We want to show that $c(a) = c(b)$. To show that $c(a) \subseteq c(b)$, let$x \in c(a)$. $x \in c(a) \Rightarrow arx$. Also, there exists an element, y, of A that is in the intersection of $c(a)$ and $c(b)$ by our assumption. Therefore,

$$\begin{aligned} ary \text{ and } bry &\Rightarrow ary \text{ and } yrb \ (r \text{ is symmetric}) \\ &\Rightarrow arb \ (\text{transitivity of } r) \end{aligned}$$

Next,

$$\begin{aligned} arx \text{ and } arb &\Rightarrow xra \text{ and } arb \\ &\Rightarrow xrb \\ &\Rightarrow brx \\ &\Rightarrow x \in c(b) \end{aligned}$$

Similarly, $c(b) \subseteq c(a)$. ■

9. (a) Equivalence Relation
$c(0) = \{0\}$, $c(1) = \{1\}$, $c(2) = \{2, 3\} = c(3)$, $c(4) = \{4, 5\} = c(5)$,
$c(6) = \{6, 7\} = c(7)$

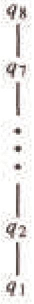
(b) Not an Equivalence Relation

(c) Equivalence Relation
$c(0) = \{0, 2, 4, 6\} = c(2) = c(4) = c(6)$
$c(1) = \{1, 3, 5, 7\} = c(3) = c(5) = c(7)$

11. (b) The proof follows from the biconditional equivalence in Table 3.4.2.

(c) Apply the chain rule.

(d)



Section 6.4

1. (a)
$$\begin{array}{cc} \square & \begin{array}{ccc} 4 & 5 & 6 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \end{array} & \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{array} \quad \text{and} \quad \begin{array}{cc} \square & \begin{array}{ccc} 6 & 7 & 8 \end{array} \\ \begin{array}{c} 4 \\ 5 \\ 6 \end{array} & \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \end{array}$$

(b)
$$\begin{array}{cc} \square & \begin{array}{ccc} 6 & 7 & 8 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \end{array} & \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \end{array}$$

3. R : xry if and only if $|x - y| = 1$.
S : xsy if and only if x is less than y.

5. The diagonal entries of the matrix for such a relation must be 1. When the three entries above the diagonal are determined, the entries below are also determined. Therefore, the answer is 2^3.

7. (a)
$$\begin{array}{cc} \square & \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \end{array} & \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array} \quad \text{and} \quad \begin{array}{cc} \square & \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \end{array} & \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

(b)
$$PQ = \begin{array}{cc} \square & \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \end{array} & \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

$$P^2 = \begin{array}{cc} \square & \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \end{array} & \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array} = Q^2$$

9. (a) Reflexive: $R_{ij} = R_{ij}$ for all i, j, therefore $R_{ij} \leq R_{ij}$
Antisymmetric: Assume $R_{ij} \leq S_{ij}$ and $S_{ij} \leq R_{ij}$ for all $1 \leq i, j \leq n \Rightarrow R_{ij} \leq S_{ij}$
Transitive: Assume R, S, and T are matrices where $R_{ij} \leq S_{ij}$and $S_{ij} \leq T_{ij}$, for all $1 \leq i, j \leq n$. Then $R_{ij} \leq T_{ij}$ for all $1 \leq i, j \leq n$, and so $R \leq T$.

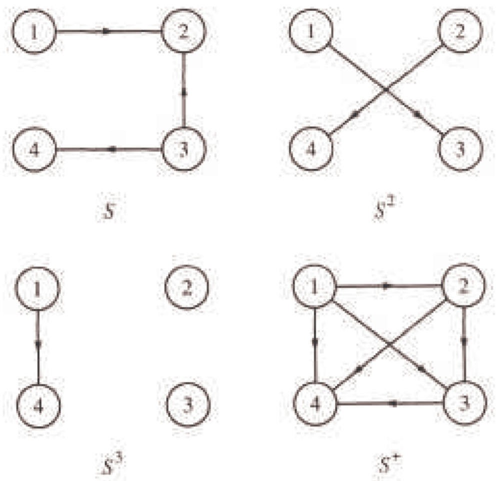
(b) $(R^2)_{ij} = R_{i1} R_{1j} + R_{i2} R_{2j} + \cdots + R_{in} R_{nj}$
$\leq S_{i1} S_{1j} + S_{i2} S_{2j} + \cdots + S_{in} S_{nj} = (S^2)_{ij} \Rightarrow R^2 \leq S^2$

To verify that the converse is not true we need only one example. For $n = 2$, let $R_{12} = 1$ and all other entries equal 0, and let S be the zero matrix. Since R^2 and S^2 are both the zero matrix, $R^2 \leq S^2$, but since $R_{12} > S_{12}$, $R \leq S$ is false.

(c) The matrices are defined on the same set $A = \{a_1, a_2, \ldots, a_n\}$. Let $c(a_i)$, $i = 1, 2, \ldots, n$ be the equivalence classes defined by R and let $d(a_i)$ be those defined by S. Claim: $c(a_i) \subseteq d(a_i)$. Let $a_j \in c(a_i) \Rightarrow a_i r a_j \Rightarrow R_{ij} = 1 \Rightarrow S_{ij} = 1 \Rightarrow a_i s a_j \Rightarrow a_j \in d(a_i)$.

Section 6.5

3. (a)



S S^2

S^3 S^+

(b) Example, $1\,s\,4$ and using S one can go from 1 to 4 using a path of length 3.

5. (a) **Definition**: Reflexive Closure. *Let r be a relation on A. A reflexive closure of r is the smallest reflexive relation that contains r.*

Theorem: *The reflexive closure of r is the union of r with* $\{(x,\ x)\ :\ x \in A\}$

7. (a) By the definition of transitive closure, r^+ is the smallest relation which contains r; therefore, it is transitive. The transitive closure of r^+, $(r^+)^+$, is the smallest transitive relation that contains r^+. Since r^+ is transitive, $(r^+)^+ = r^+$.

(b) The transitive closure of a symmetric relation is symmetric, but it may not be reflexive. If one element is not related to any elements, then the transitive closure will not relate that element to others.

Supplementary Exercises—Chapter 6

1. If Andy is the parent of Barbara and Barbara is the parent of Charles, then Andy is the grandparent of Charles.

3. (a) $r = \{(-1, 0), (0,\ 1), (1, 2)\}$

(b) $s = \{(-1, -1), (-1, 1), (0, 0), (1, -1), (1, 1), (2, 2)\}$

(c) $t = \{(-1,\ 0),\ (-1,\ 1),\ (-1,\ 2),\ (0,\ -1),\ (0,\ 1),\ (0,\ 2),$
$(1, -1), (1, 0), (1, 2), (2, -1), (2, 0), (2, 1)\}$

5. His main office should be at node 2. The least desirable location is at node 1. The arrows in both directions between nodes 1 and 2 represent a two-way street.

7. (a) No.

(b) Person a is friendly toward the most people so he/she would be chair person.

(c) If "great personality" has any effect then person b becomes chairperson.

(d) A seating arrangement does not exist, since persons c and d are only friendly toward one person each and they have to be seated between *two* people they are friendly toward.

9. In order for the relation "living in the same house" to be an equivalence relation we must assume that a person lives in only one house.

11.(a) r is an equivalence relation.

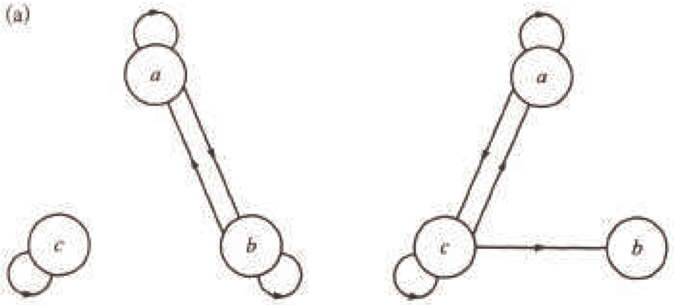
(b) s is neither since s is not reflexive.

(c) In order for s to be a partial ordering we rephrase it slightly; xsy iff x taller than y or x equals y. Why would xsy iff x is the same height as or taller than y be wrong?

13. There are 16 places in the adjacency matrix for a relation on four elements, but for a symmetric relation those entries below the diagonal will be the same as above. Hence we are only concerned with $16 - 6 = 10$ places. Each of the remaining entries may take on a value of either 0 or 1, so by the rule of products we have 2^{10} possible symmetric relations on a four element set.

15.

15. (a)



(b) (i) $\{(a, a), (a, b), (b, a), (b, b), (c, c)\}$

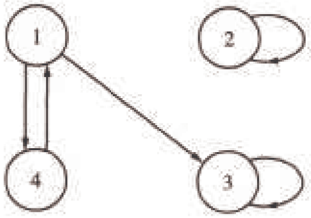
(ii) $\{(a, a), (a, c), (c, a), (c, b), (c, c)\}$

(c) (i) $R^2 = R = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

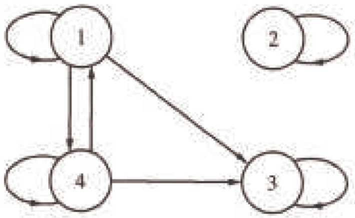
(ii) $R^2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$

17.

(a)



(b)



(b) r is not reflexive, not symmetric, not antisymmetric, and not transitive.

(c) $R^+ = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$

19. (a) A_5 is friendly to no one.

(b) The U.S. Ambassador (A_1) should be the chairman of this committee, since he is friendly toward the most people.

(c) The U.S. Ambassador can communicate to everyone on the committee.

CHAPTER 7

Section 7.1

1. (a) Yes (b) Yes (c) No (d) No (e) Yes

3. (a) Range of $f = f(A) = \{a, b, c, d\} = B$

(b) Range of $g = g(A) = \{a, b, d\}$

(c) Range of $L = L(A) = \{1\}$

5. For each of the $\mid A \mid$ elements of A, there are $\mid B \mid$ possible images, so there are $\mid B \mid \cdot \mid B \mid \cdot \ldots \cdot \mid B \mid = \mid B \mid^{|A|}$ functions from A into B.

Section 7.2

1. The only one-to-one function and the only onto function is f.

3. (a) onto but not one-to-one ($f_1(0) = f_1(1)$)
(b) one-to-one and onto
(c) one-to-one but not onto
(d) onto but not one-to-one
(e) one-to-one but not onto
(f) one-to-one but not onto

5. Let $X = \{\text{socks selected}\}$ and $Y = \{\text{pairs of socks}\}$ and define $f : X \to Y$ where $f(x)$ =the pair of socks that x belongs to . By the Pigeonhole principle, there exist two socks that were selected from the same pair.

7. (a) $f(n) = n$, for example

(b) $f(n) = 1$, for example

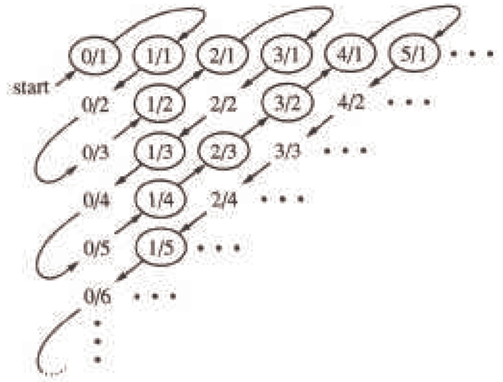
(c) None exist.

(d) None exist.

9. (a) Use $s : \mathbb{N} \to \mathbb{P}$ defined by $s(x) = x + 1$.

(b) Use the function$f : \mathbb{N} \to \mathbb{Z}$ defined by $f(x0 = x/2$ if x is even and $f(x) = -(x + 1)/2$ if x is odd.

(c)The proof is due to Georg Cantor (1845-1918), and involves listing the rationals through a definite procedure so that none are omitted and duplications are avoided. In the first row list all nonnegative rationals with denominator 1, in the second all nonnegative rationals with denominator 2, etc. In this listing, of course, there are duplications, for example, $0/1 = 0/2 = 0$, $1/1 = 3/3 = 1$, $6/4 = 9/6 = 3/2$, etc. To obtain a list without duplications follow the arrows in the given array listing only the circled numbers.



We obtain: 0, 1, 1/2, 2, 3, 1/3, 1/4, 2/3, 3/2, 4/1, ... Each nonnegative rational appears in this list exactly once. We now must insert in this list the negative rationals, and follow the same scheme to obtain: 0, 1, −1, 1/2, −1/2, 2, −2, 3, −3, 1/3, −1/3, ... , which can be paired off with the elements of $\mathbb{N}$.

11. Let f be any function from A into B. By the Pigeonhole principle with $n = 1$, there exists an element of B that is the image of at least two elements of A. Therefore, f is not an injection.

13. The proof is indirect and follows a technique called the Cantor diagonal process. Assume to the contrary that the set is countable, then the elements can be listed:

$n_1, n_2, n_3, \ldots$ where each n_i is an infinite sequence of 0s and 1s. Consider the array:

$$\begin{array}{l} n_1 = n_{11}\, n_{12}\, n_{13} \cdots \\ n_2 = n_{21}\, n_{22}\, n_{23} \cdots \\ n_3 = n_{31}\, n_{32}\, n_{33} \cdots \\ \quad\vdots \end{array}$$

We assume that this array contains all infinite sequences of 0s and 1s. Consider the sequence s defined by

$$s_i = \begin{cases} 0 & \text{if } n_{\text{ii}} = 1 \\ 1 & \text{if } n_{\text{ii}} = 0 \end{cases}$$

s differs from each n_i in the ith position and so cannot be in the list. This is a contradiction, which completes our proof.

Section 7.3

1. (a) $g \circ f : A \to C$ is defined by $(g \circ f)\,(k) = \begin{cases} + & \text{if } k = 1 \text{ or } k = 5 \\ - & \text{if } k = 2, 3, 4 \end{cases}$

(b) No, since the domain of f is not equal to the codomain of g.

(c) No, since f is not surjective.

(d) No, since g is not injective.

3. (a) The permutations of A are i, r_1, r_2, f_1, f_2, and f_3, defined in section 15.3

(b, c)

Permutation	Inverse of the permutation	Square of permutation
i	i	i
r_1	r_2	r_2
r_2	r_1	r_1
f_1	f_1	i
f_2	f_2	i
f_3	f_3	i

(d) Apply both Theorems 7.3.3 and 7.3.4: If f and g are permutations of A, then they are both injections and their composition, $f \circ g$, is a injection, by Theorem 7.3.3. By 7.3.4, $f \circ g$ is also a surjection; therefore, $f \circ g$ is a bijection on A, a permutation.

(e) Proof by induction:

Basis: ($n = 1$) The number of permutations of A is one, the identity function, and $1! = 1$.

Induction: Assume that the number of permutations on a set with n elements, $n \geq 1$, is $n!$. Furthermore, assume that $\lvert A \rvert = n + 1$ and that A contains an element called x. Let $A' = A - \{x\}$. We can reduce the definition of a permutation, f, on A to two steps. First, we select any one of the $n!$ permutations on A'. (Note the use of the induction hypothesis.) Call it g. This permutation almost completely defines a permutation on A by $f(a) = g(a)$ for all a in A', Next, we select the image of x, which can be done $n + 1$ different ways. To keep our function bijective, we must adjust f as follows: If we select $f(x) = y$, then we must find the element, z, of A such that $g(z) = y$, and redefine the image of z to $f(z) = x$. If we had selected $f(x) = x$, then there is really no adjustment needed. By the rule of products, the number of ways that we can define f is $n!\,(n + 1) = (n + 1)!$ ■

7. (a) $f \circ g(n) = n + 3$ (b) $f^3(n) = n + 15$ (c) $f \circ h(n) = n^2 + 5$

9. **Theorem:** If $f : A \to B$ and f has an inverse, then that inverse is unique.

Proof: Suppose that g and h are both inverses of f.

$$\begin{aligned} g &= g \circ i_A\, g \\ &= g \circ (f \circ h) \\ &= (g \circ f) \circ h \\ &= i_A \circ h \\ &= h \qquad\qquad \Rightarrow g = h \qquad \# \end{aligned}$$

11. Proof of Theorem 7.3.2: Let x, x' be elements of A such that $g \circ f(x) = g \circ f(x')$; that is, $g\,(f(x)) = g(f\,(x'))$. Since g is injective, $f(x) = f(x')$ and since f is injective, $x = x'$. ■

Proof of Theorem 7.3.3: Let x be an element of C. We must show that there exists an element of A whose image under $g \circ f$ is x. Since g is surjective, there exists an element of B, y, such that $g(y) = x$. Also, since f is a surjection, there exists an element of A, z, such that $f(z) = y$, $g \circ f(z) = g(f(z)) = g(y) = x$. ■

13. **Basis:** ($n = 2$): $(f_1 \circ f_2)^{-1} = {f_2}^{-1} \circ {f_1}^{-2}$ by exercise 10.
Induction: Assume $n \geq 2$ and $(f_1 \circ f_2 \circ \cdots \circ f_n)^{-1} =$
${f_n}^{-1} \circ \cdots \circ {f_2}^{-1} \circ {f_1}^{-1}$
Consider $(f_1 \circ f_2 \circ \cdots \circ f_{n+1})^{-1}$.

$$\begin{array}{ll}
(f_1 \circ f_2 \circ \cdots \circ f_{n+1})^{-1} & = ((f_1 \circ f_2 \circ \cdots \circ f_n) \circ f_{n+1})^{-1} \\
\text{by the Basis} & = {f_{n+1}}^{-1} \circ (f_1 \circ f_2 \circ \cdots \circ f_n)^{-1} \\
\text{by Induction hypothesis} & = {f_{n+1}}^{-1} \circ \left({f_n}^{-1} \circ \cdots \circ {f_2}^{-1} \circ {f_1}^{-1}\right) \\
 & = {f_{n+1}}^{-1} \circ \cdots \circ {f_2}^{-1} \circ {f_1}^{-1}. \blacksquare
\end{array}$$

15. Assume all functions are functions on A.

$$\begin{array}{l}
(f \circ g) \circ h = f \circ (g \circ h) \\
f \circ i_A = i_A \circ f = f \\
\text{If } f^{-1} \text{ and } g^{-1} \text{ exist, } (g \circ f)^{-1} = f^{-1} \circ g^{-1} \text{ and} \\
\text{If } f^{-1} \text{ exists, } (f^{-1})^{-1} = f.
\end{array}$$

Supplementary Exercises—Chapter 7

1. (a) $\mathbb{Z}$ (b) $\mathbb{Z}$ (c) $f(-5) = 2\,|\,5\,|+1 = 11$

(d) $\{1, 3, 5, 7, 9, \ldots\}$ = the set of odd positive integers

(e) No, $a = 5$ or $a = -5$.

3. No. Relations (iii) and (iv) are not functions because the domain is not all of the set A. The others are not functions since in each case at least one element of A is mapped to 2 different elements. Example for relation (i), a is mapped to both a and b.

5. (a) The matrix of f can only have one 1 in each row. So if the domain of f has n elements the matrix of f will have n 1s.

(b) If f is a bijection, besides having only one 1 in each row, there can only be one 1 in each column.

7. (a) Let $f(n) = n^2$, ∀n∈ℕ. Since f is a bijection from ℕ into $A = \{n^2 \mid n \in \mathbb{N}\}$, ℕ and A have the same cardinality; so A is countable.

(b) Let $B = \{1/n \mid n \in \mathbb{P}\}$. $g : \mathbb{N} \to B$ defined by $g(n) = 1/(n+1)$ is the required bijection.

(c) That $C = C_1 \cup C_2 = \{3, 9, 27, 81, \ldots\} \cup \{2, 4, 8, 16, \ldots\}$ is countable follows from the proof of Exercise 8. Without using this proof, we can still prove that C is countable by using the list 2^1, 3^1, 2^2, 3^2, 2^3, 3^3 to define $h : \mathbb{N} \to C$ where $h(a)$ =the number in position $a + 1$ in the list,

9. $f : A \times B \to B \times A$ defined by $f(a, b) = (b, a)$ is a bijection, which is all that we need to prove that
$|\,A \times B\,| = |\,B \times A\,|$

11. This "code" can be viewed as a function, a, on the set of all finite sequences of letters. For example, a(hat) = qmh. This encoding function will not work very well because it is not a bijection. For example, no sequence with a or t in it is in the range. Although a is not one-to-one, it is difficult to find two English words with the same image.

13. (a) $10\,(a + 10)$ (b) $a + 20$ (c) $10a\ div\ 10 = a$

(d) $(a + 10)\ div\ 10 = a\ div\ 10 + 1$

15. (a) $f(b) = b$ and $f(c) = c$

(b) $f(b) = a$ and $f(c) = d$

17. Since $det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$ there are four permutations of $\{a, b, c, d\}$ that leave the determinant invariant. These permutations are the identity function, $\alpha_1 = \{(a, d), (b, b), (c, c), (d, a)\}$, $\alpha_2 = \{(a, d), (b, c), (c, b), (d, a)\}$, and $\alpha_3 = \{(a, a), (b, c), (c, b), (d, d)\}$.

19. (a) Domain = positive real numbers, Codomain = Real numbers.

CHAPTER 8

Section 8.1

1.
$$\begin{array}{rl}
C(5, 2) = & C(4, 2) + C(4, 1) \\
 & = C(3, 2) + C(3, 1) + C(3, 1) + C(3, 0) \\
 & = C(3, 2) + 2\,C(3, 1) + 1 \\
 & = C(2, 2) + C(2, 1) + 2\,(C(2, 1) + C(2, 0)) + 1 \\
 & = 3\,C(2, 1) + 4 \\
 & = 6 + 4 = 10
\end{array}$$

3. (a) $p\,(x)$ in telescoping form: $((((x + 3)\,x - 15)\,x + 0)\,x + 1)\,x - 10$

(b) $p(3) = ((((3 + 3)\,3 - 15)\,3 - 0)\,3 + 1)\,3 - 10 = 74$

5. The basis is not reached in a finite number of steps if you try to compute $f(x)$ for a nonzero value of x.

Section 8.2

1. **Basis**: $B(0) = 3 \cdot 0 + 2 = 2$, as defined

Induction: Assume: $B(k) = 3k + 2$ for some $k \geq 0$.

$$\begin{aligned} B(k+1) &= B(k) + 3 \\ &= (3k+2) + 3 && \text{by the induction hypothesis} \\ &= (3k+3) + 2 \\ &= 3(k+1) + 2, && \text{as desired. } \blacksquare \end{aligned}$$

3. Imagine drawing line k in one of the infinite regions that it passes through. That infinite region is divided into two infinite regions by line k. As line k is drawn through every one of the $k-1$ previous lines, you enter another region that line k divides. Therefore, the number of regions is increased by k.

5. For n greater than zero, $M(n) = M(n-1) + 1$, and $M(0) = 0$.

Section 8.3

1. $S(k) = 2 + 9^k$

3. $S(k) = 6\,(1/4)^k$

5. $S(k) = k^2 - 10\,k + 25$

7. $S(k) = (3 + k)\,5^k$

9. $S(k) = (12 + 3\,k) + (k^2 + 7\,k - 22)\,2^{k-1}$

11. $P(k) = 4\,(-3)^k + 2^k - 5^{k+1}$

13. (a) The characteristic equation is a $a^2 - a - 1 = 0$, which has solutions $\alpha = \left(1 + \sqrt{5}\right)/2$ and $\beta = \left(1 - \sqrt{5}\right)/2$, It is useful to point out that $\alpha + \beta = 1$ and $\alpha - \beta = \sqrt{5}$. The general solution is

$$F(k) = b_1\,\alpha^k + b_2\,\beta^k\ .$$

Using the initial conditions, we obtain the system: $b_1 + b_2 = 1$ and $b_1\,\alpha + b_2\,\beta = 1$. The solution to this system is

$$b_1 = \alpha/(\alpha - \beta) = \left(5 + \sqrt{5}\right)/2\sqrt{5}$$

$$\text{and} \qquad b_2 = \beta/(\alpha - \beta) = \left(5 - \sqrt{5}\right)/2\sqrt{5}$$

Therefore the final solution is

$$F(n) = \left(1/\sqrt{5}\right)\left[\left(\left(1 + \sqrt{5}\right)/2\right)^{n+1} - \left(\left(1 - \sqrt{5}\right)/2\right)^{n+1}\right]$$

(b) $C_r = F(r+1)$

15. (a) $D(n) = 2\,D(n-1) + 1$ for $n \geq 2$ and $D(1) = 0$.

(b) $D(n) = 2^{n-1} - 1$

17. Solutions to the recurrence relation and its approximation are $B(k) = (1 + c)^k + (1 - c)^k$ and $B_a(k) = 1$. Note how as k increases, $B(k)$ grows in size, while $B_a(k)$ stays constant.

Section 8.4

1. (a) $S(n) = 1/n!$ (c)$U(k) = 1/k$, an improvement.

(b) $T(k) = (-3)^k\,k!$, no improvement.

3. (a) $T(n) = 3\,(\lfloor \log_2 n \rfloor + 1)$ (c) $V(n) = \lfloor \log_8 n \rfloor + 1$

(b) $T(n) = 2$

5. The indicated substitution yields $S(n) = S(n+1)$. Since $S(0) = T(1)/T(0) = 6$, $S(n) = 6$ for all n. Therefore $T(n+1) = 6\,T(n) \Rightarrow T(n) = 6^n$.

7. (a) A good approximation to the solution of this recurrence relation is based on the following observation: n is a power of a power of two; that is, n is 2^m, where $m = 2^k$, then $Q(n) = 1 + Q\left(2^{m/2}\right)$. By applying this recurrence relation k times we obtain $Q(n) = k$. Going back to the original form of n, $\log_2 n = 2^k$ or $\log_2(\log_2 n) = k$. We would expect that in general, $Q(n)$ is $\lfloor \log_2(\log_2 n) \rfloor$. We do not see any elementary method for arriving at an exact solution.

(b) Suppose that n is a positive integer with $2^{k-1} \leq n < 2^k$. Then n can be written in binary form, $(a_{k-1}\, a_{k-2} \cdots a_2\, a_1\, a_0)_{\text{two}}$ with $a_{k-1} = 1$ and $R(n)$ is equal to the sum

$$\sum_{i=0}^{k-1} (a_{k-1}\, a_{k-2} \cdots a_i)_{\text{two}}$$

If $2^{k-1} \leq n < 2^k$, then we can estimate this sum to be between $2\,n - 1$ and $2\,n + 1$. Therefore, $R(n) \approx 2\,n$.

Section 8.5

1. (a) 1, 0, 0, 0, 0, … (b) $5\,(1/2)^k$ (c) 1, 1, 0, 0, 0, …
(d) $3\,(-2)^k + 3 \cdot 3^k$

3. (a) $1/(1 - 9\,z)$ (b) $(2 - 10\,z)/(1 - 6\,z + 5\,z^2)$
(c) $1/(1 - z - z^2)$

5. (a) $3/(1 - 2\,z) + 2/(1 + 2\,z)$, $3 \cdot 2^k + 2\,(-2)^k$
(b) $10/(1 - z) + 12/(2 - z)$, $10 + 6\,(1/2)^k$
(c) $-1/(1 - 5\,z) + 7/(1 - 6\,z)$, $7 \cdot 6^k - 5^k$

7. (a) $11\,k$
(b) $(5/3)\,k(k+1)\,(2\,k+1) + 5\,k(k+1)$
(c) $\displaystyle\sum_{j=0}^{k} (j)\,(10\,(k-j)) = 10\,k \sum_{j=0}^{k} j - 10 \sum_{j=0}^{k} j^2$
$= 5\,k^2\,(k+1) - (5\,k(k+1)\,(2\,k+1)/6)$
$= (5/3)\,k(k+1)\,(2\,k+1)$
(d) $k(k+1)\,(2\,k+7)/12$

9. Coefficients of z^0 through z^5 in $(1 + 5\,z)\,(2 + 4\,z)\,(3 + 3\,z)\,(4 + 2\,z)\,(5 + z)$

k	Number of ways of getting *a* score of k
0	120
1	1044
2	2724
3	2724
4	1044
5	120

Supplementary Exercises—Chapter 8

1. Let $v\,(n)$ be the quantity in question. Since any positive digit can appear in a one-digit positive integer, $v(1) = 9$. Given an n digit number, $n \geq 2$, it can be thought of as an $n - 1$ digit number times ten plus a digit. This digit cannot be the same as the units digit of the $n - 1$ digit number. Therefore, by the product rule $v(n) = 9\,v(n-1)$ for $n \geq 2$.

3. (a) To execute Split with L in = (1, 2, 3, 4), we must split the list into $L\,1$ = (1, 3) and $L\,2$ = (2, 4). If you carefully examine the algorithm for a list of length 2, you will see that the output equals the input; therefore $L\,1$ out = (1, 3) and $L\,2$ out = (2, 4) and L out = (1, 3, 2, 4).
(b) Examine the results for r = 1, 2, 3 with numbers in binary form. Notice the symmetry with respect to the vertical line.

$r = 1$

L in	L out
0	0
1	1

$r = 2$

L in	L out
00	00
01	10
10	01
11	11

$r = 3$

L in	L out
000	000
001	100
010	010
011	110
100	001
101	101
110	011
111	111

The integers in L out are sorted so that $(b_{r-1}\, b_{r-2} \cdots b_0)_{\text{two}}$ appears in position $(b_0\, b_1 \cdots b_{r-1})_{\text{two}}$.

5. This is not a closed form expression because the number of operations that are needed to compute the expression grows with n, $B\,(n)$ in this form requires n additions and $n-1$ multiplications.

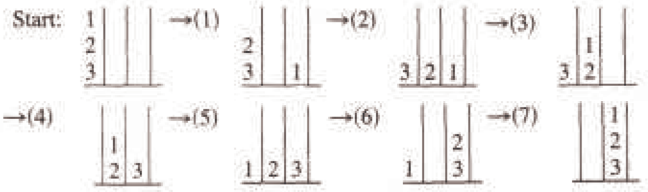
7. Kathryn's balance on her first birthday is $\$1 = B(1)$. If $B\,(n)$ is her balance on her nth birthday, $n \geq 2$, then $B(n) = 1.1\, B(n-1) + n$.

$$B(n) = B^{(n)}(n) + B^{(p)}(n) = b_1 (1.1)^n - (10\, n + 110)$$
$$B(1) = 1 \Rightarrow (1.1)\, b_1 = 121 \Rightarrow b_1 = 1.1$$

Therefore $B(n) = 121\,(1.1)^{n-1} - (10\, n + 110)$. On her 21st birthday, Kathryn will have $B(21) = 121\,(1.1)^{20} - (210 + 110) = \$494\,.03$.

9. (a) If it takes $X\,(n)$ moves to move n disks to peg 2, then we can transfer the $n+1$ disk to peg 3 in one move and then transfer the n disks from peg 2 to peg 3 in $X(n)$ moves, so $X(n+1) = X(n) + 1 + X(n) = 2\, X(n) + 1$, or equivalently $X(n) = 2\, X(n-1) + 1$.

(b) $X(n) = b_1 \cdot 2^n - 1$. Since it takes 1 move to transfer 1 disk from one peg to another, $X(1) = 1$; so $b_1 = 1$ and $X(n) = 2^n - 1$. We verify that $X\,(3) = 7$:



11. The solution for $n = 4^k$ is $Q\left(4^k\right) = \frac{1}{3}\left(4^{k+1} - 1\right)$, This can be obtained in one of two ways. Either use the substitution $S(k) = Q\left(4^k\right)$, which yields $S(k) = 4^k + S(k-1)$, or note that $Q\left(4^k\right) = 4^k + Q\left(4^{k-1}\right) = 4^k + 4^{k-1} + Q\left(4^{k-2}\right) = 4^k + 4^{k-1} + \cdots + 4 + 1$. This finite geometric series has the closed form expression above. By similar means, $Q\left(2 \cdot 4^k\right) = 2\, Q\left(4^k\right) = \frac{2}{3}\left(4^{k+1} - 1\right)$

13. $G(S;\, z) = 1 + z + 2\, z^2 + 4\, z^3 + 8\, z^4 \cdots$

15. $G(T;\, z) = G(S;\, cz) \;=\; \sum_{k=0}^{\infty} S(k)\,(cz)^k =$

$$= \sum_{k=0}^{\infty} \left(S(k)\, c^k\right) z^k$$

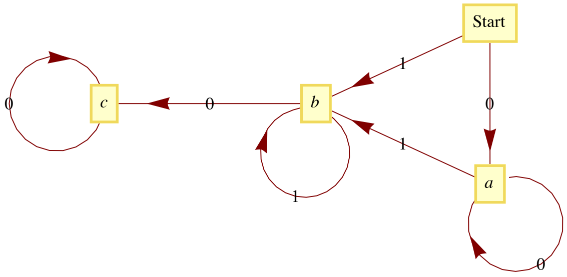
Therefore, $T(k) = S(k)\, c^k$.

CHAPTER 9

Section 9.1

1. In Figure 9.1.2, computer *b* can communicate with all other computers. In Figure 9.1.3, there are roads to and from city *b* to all other cities. In Figure 9.1.4, there is a door connecting room *b* to every other room in the house (including the outside).

3.



5. No, the maximum number of edges would be $\frac{(7)(8)}{2} = 28$.

7. (a) $C(n, 2) = \frac{(n-1)n}{2}$

(b) $n - 1$, one edge for each vertex except the champion vertex.

Section 9.2

A Exercises

1. Estimate the number of vertices and edges in each of the following graphs. Would the graph be considered sparse?

(a) A rough estimate of the number of vertices in the "world airline graph" would be the number of cities with population greater than or equal to 100,000. Using the Wolfram CityData function we can get this number:

```
CityData[All] // Select[#, CityData[#, "Population"] >= 10^5 &] & // Length
```

```
4257
```

There are many smaller cities that have airports, but some of the metropolitan areas with clusters of large cities are served by only a few airports. 4000-5000 is probably a good guess. As for edges, that's a bit more difficult to estimate. It's certainly not a complete graph. Looking at some medium sized airports such as Manchester, NH, the average number of cities that you can go to directly is in the 50-100 range. So a very rough estimate would be $\frac{75 \times 4500}{2} = 168\,750$.

(b) The number of ASCII characters is 128. Each character would be connected to 8 others and so there are $\frac{128 \times 8}{2} = 512$ edges.

(c) The Oxford English Dictionary as approximately a half-million words, although many are obsolete. *Mathematica* has a words database that is a bit less comprehensive, yet it isn't trivial. The nice thing about using the Wolfram data is that the number of vertices and edges can be counted. Here is the number of words and hence the number of vertices in the graph:

```
WordData[All] // Length
```

```
149 191
```

And here are the number of edges, determined in a not necessarily efficient manner.

```
(Length[WordData[# ~~ ___, "Lookup"]] & /@ WordData[All]) // Apply[Plus, #] &
```

```
876 547
```

The last output took about three hours using a MacBook Pro with a 2.5 GHz Intel Core 2 Duo Processor. It should also be pointed out that Wolfram's choice of "words" doesn't match the OED or a Scrabble player's dictionary. For example, "1900s" and "18-karat gold" are included among the list of words. Nevertheless, the number we have here are good ballpark estimates for Most interpretations of the "English words."

3. Each graph is isomorphic to itself. In addition, G_2 and G_4 are isomorphic; and G_3, G_5, and G_6 are isomorphic.

Section 9.3

1.

k	1	2	3	4	5	6
$V[k]$.found	T	T	T	F	F	T
$V[k]$.from	2	5	6	$*$	$*$	5
Depth Set	2	1	2	$*$	$*$	1

($*$ = undefined)

3. If the number of vertices is n, there can be $\frac{(n-1)(n-2)}{2}$ vertices with one vertex not connected to any of the others. One more edge and connectivity is assured.

5. Basis: ($k = 1$) Is the relation r^1defined by $v r^1 w$ if there is a path of length l from v to w? Yes, since $v r w$ if and only if an edge, which is a path of length l, connects v to w.

Induction: Assume that $v r^k w$ if and only if there is a path of length k from v to w. We must show that $v r^{k+1} w$ if and only if there is a path of length $k+1$ from v to w.

$v r^{k+1} w \Rightarrow v r^k y$ and $y r w$, for some vertex y. By the induction hypothesis, there is a path of length k from v to y. And by the basis, there is a path of length one from y to w. If we combine these two paths, we obtain a path of length $k+1$ from v to w. Of course, if we start with a path of length $k+1$ from v to w, we have a path of length k from v to some vertex y and a path of length l from y to w. Therefore, $v r^k y$ and $y r w \Rightarrow v r^{k+1} w$ ■

Section 9.4

1. Using a recent road map, it appears that a Eulerian circuit exists in New York City, not including the small islands that belong to the city. Lowell, Massachusetts, is located at the confluence of the Merrimack and Concord rivers and has several canals flowing through it. No Eulerian path exists for Lowell.

3. Gray Code for the 4-cube:

$$G_4 = \begin{pmatrix} 0000 \\ 0001 \\ 0011 \\ 0010 \\ 0110 \\ 0111 \\ 0101 \\ 0100 \\ 1100 \\ 1101 \\ 1111 \\ 1110 \\ 1010 \\ 1011 \\ 1001 \\ 1000 \end{pmatrix}$$

5. Any bridge between two land masses will be sufficient. To get a Eulerian circuit, you must add a second bridge that connects the two land masses that were not connected by the first bridge.

7. **Theorem:** *Let $G = (V, E)$ be a directed graph, G has a Eulerian circuit if (a) G is connected and (b)* $\text{indeg}(v) = \text{outdeg}(v)$ *for all v in V. There exists a Eulerian path from v_1 to v_2 if (a) g is connected and (b)* $\text{indeg}(v_1) = \text{outdeg}(v_1) - 1$, $\text{indeg}(v_2) = \text{outdeg}(v_2) + 1$ *and for all other vertices in V the indegree and outdegree are equal.*

9. A round-robin tournament graph is rarely Eulerian. It will be Eulerian if it has an odd number of vertices and each vertex (team) wins exactly as many times as it loses. Every round-robin tournament graph has a Hamiltonian path. This can be proven by induction on the number of vertices.

Section 9.5

1. The circuit would be Boston, Providence, Hartford, Concord, Montpelier, Augusta, Boston. It does matter where you start. If you start in Concord, for example, your mileage will be higher.

3. (a) Optimal cost $= 2\sqrt{2}$.

Phase 1 cost $= 2.4\sqrt{2}$.

Phase 2 cost $= 2.6\sqrt{2}$.

(b) Optimal cost $= 2.60$.

Phase 1 cost $= 3.00$.

Phase 2 cost $2\sqrt{2}$.

(c) $A = (0.0,\ 0.5),\ B = (0.5,\ 0.0),\ C = (0.5,\ 1.0),\ D = (1.0,\ 0.5)$

There are 4 points; so we will divide the unit square into two strips.

Optimal Path: (B, A, C, D)	Distance $= 2\sqrt{2}$
Phase I Path: (B, A, C, D)	Distance $= 2\sqrt{2}$
Phase II Path: (A, C, B, D)	Distance $= 2 + \sqrt{2}$

(d) $A = (0, 0),\ B = (0.2, 0.6),\ C = (0.4, 0.1),\ D = (0.6, 0.8),\ E = (0.7, 0.5)$

There are 5 points; so we will divide the unit square into three strips.

Optimal Path: (A, B, D, E, C)	Distance $= 2.31$
Phase I Path: (A, C, B, C, E)	Distance $= 2.57$
Phase II Path: (A, B, D, E, C)	Distance $= 2.31$

5. (a) $f(c, d) = 2,\ f(b, d) = 2,\ f(d, k) = 5,\ f(a, g) = 1,$ and $f(g, k) = 1$.

(b) There are three possible flow-augmenting paths.

s, b, d, k with flow increase of 1.

s, a, d, k with flow increase of 1, and

s, a, g, k with flow increase of 2.

(c) The new flow is never maximal, since another flow-augmenting path will always exist. For example, if s, b, d, k is used above, the new flow can be augmented by 2 units with s, a, g, k.

7. (a) Value of maximal flow $= 31$.

(b) Value of maximal flow $= 14$.

(c) Value of maximal flow $= 14$.

One way of obtaining this flow is:

Step	Flow – Augmenting Path	Flow Added
1	Source, A, Sink	2
2	Source, C, B, Sink	3
3	Source, E, D, Sink	4
4	Source, A, B, Sink	1
5	Source, C, D, Sink	2
6	Source, A, B, C, D, Sink	2

9. To locate the closest neighbor among the list of k other points on the unit square requires a time proportional to k. Therefore the time required for the closest-neighbor algorithm with n points is proportional to $(n-1) + (n-2) + \cdots + 2 + 1$, which is proportional to n^2. Since the strip algorithm takes a time proportional to $n(\log n)$, it is much faster for large values of n.

11. Let$P = P_1, P_2, \ldots, P_{2n}$ be a set of points in the unit square. If S is a subset of P, define $\min(S)$ to be the point in S with smallest x coordinate. If there is a tie, select the point with smallest y coordinate.

Matching Algorithm:

```
1. $S := P$
2. While $S \neq \emptyset$ Do
      2.1 $v := \min(S)$
      2.2 $w :=$ closest point to $v$ in $S - \{v\}$
      2.3 pair up $v$ and $w$
```

2.4 $S := S - \{v, w\}$

Although this could be classified as a closest-neighbor algorithm, there is a better one, but it is more time-consuming.

Section 9.6

1. Theorem 9.6.2 can be applied to infer that if $n \geqslant 5$, then K_n is nonplanar. A K_4 is the largest complete planar graph.

3. (a) 3(b) 3 (c) 3 (d) 3 (e) 2 (f) 4

5. n

7. Suppose that G' is not connected. Then G' is made up of 2 components that are planar graphs with less than k edges, G_1 and G_2. For $i = 1$ and 2, let v_i, r_i, and e_i be the number of vertices, regions and edges in G_i.
By the induction hypothesis:

$$v_1 + r_1 - e_1 = 2$$
$$\text{and } v_2 + r_2 - e_2 = 2$$

One of the regions, the infinite one, is common to both graphs. Therefore, when we add edge e back to the graph, we have $r = r_1 + r_2 - 1$, $v = v_1 + v_2$, and $e = e_1 + e_2 + 1$.

$$\begin{aligned} v + r - e + (v_1 + v_2) &+ (r_1 + r_2 - 1) - (e_1 + e_2 + 1) \\ &= (v_1 + r_1 - e_1) + (v_2 + r_2 - e_2) - 2 \\ &= 2 + 2 - 2 \\ &= 2 \quad \blacksquare \end{aligned}$$

9. Since $|E| + E^c = \frac{n(n-1)}{2}$, either E or E^c has at least $\frac{n(n-1)}{4}$ elements. Assume that it is E that is larger. Since $\frac{n(n-1)}{4}$ is greater than $3n - 6$ for $n \geqslant 11$, G would be nonplanar. Of course, if E^c is larger, then G' would be nonplanar by the same reasoning.

11. Suppose that (V, E) is bipartite (with colors red and blue), $|E|$ is odd, and $(v_1, v_2, \ldots, v_{2n+1}, v_1)$ is a Hamiltonian circuit. If v_1 is red, then v_{2n+1} would also be red. But then $\{v_{2n+1}, v_1\}$ would not be in E, a contradiction.

13. Draw a graph with one vertex for each edge, If two edges in the original graph meet at the same vertex, then draw an edge connecting the corresponding vertices in the new graph.

Supplementary Exercises—Chapter 9

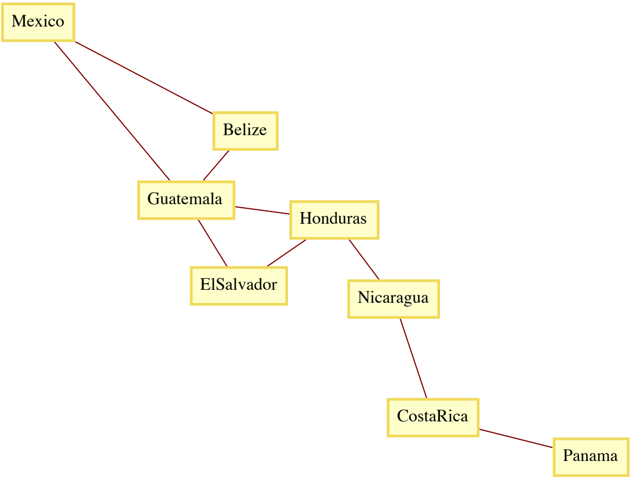
1. Graphs G_1 and G_2 are isomorphic. One isomorphism between them is $\{(a, e), (b, h), (c, f), (d, g)\}$. To see that G_3 is not isomorphic to the other two notice that k and j are not connected by an edge while in G_1 and G_2 every pair of vertices is connected.

3. (a) $\{a, e\}$ is a maximal independent set in Figure 9.1.2.

(b) (By contradiction) Assume that W is a maximal independent set in G. If V is not connected to any vertex, $W \cup \{v\}$ is independent, and since this is a larger set, W is not maximal.

(c) A single vertex is maximal; no larger set can be independent.

5. (a)



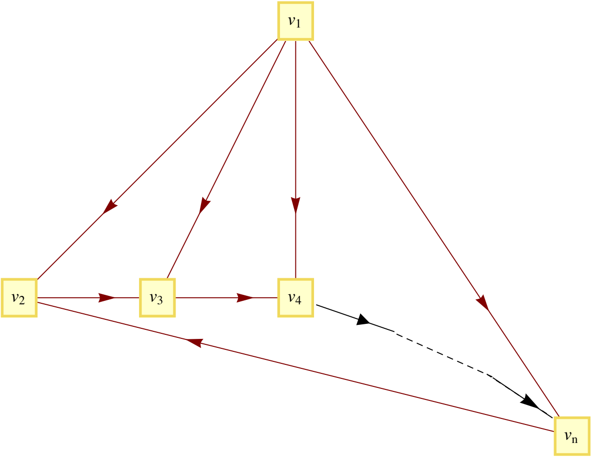
(b) (Mexico, Guatemala, Belize, Nicaragua, Costa Rica, Panama)

(c) This path could be a list of the countries that you would go through in your trip.

7. (a) If one source s exists, then (s, v) is on the edge of the round-robin tournament graph for each vertex v different from s. Therefore no other vertex could be a source. By similar reasoning, only one sink can exist. In a round-robin tournament, only one team can be unbeaten and only one can be winless.

(b) If $|V| = n$, $outdeg\,(\text{source}) = indeg\,(\text{sink}) = n - 1$

(c) Let $V = \{v_1, v_2, \ldots, v_n\}$. The following graph demonstrates that $p \wedge \neg q$ is possible. Similar graphs can be drawn for the other situations.



9.

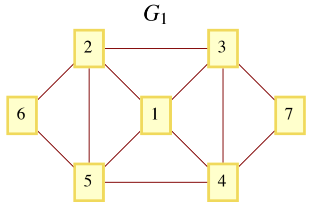
k	1	2	3	4	5	6	7	8	9
$V[k]$.name	a	b	c	d	e	f	g	h	i
$V[k]$.found	T	T	T	T	T	T	T	T	T
$V[k]$.from	4	1	5	5	1	3	5	5	6
depth set	3	1	2	2	1	3	2	2	4

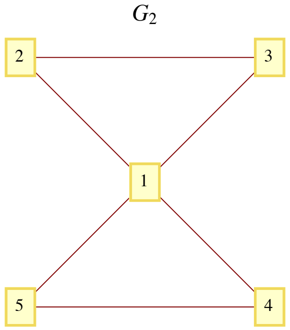
11. G_1 is randomly Eulerian from no vertex, yet it is Eulerian.

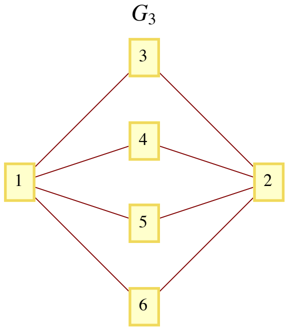
G_2 is randomly Eulerian from only vertex 1.

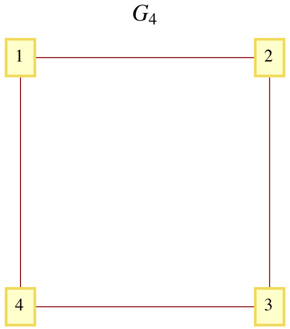
G_3 is randomly Eulerian from only vertices 1 and 2.

G_4 is randomly Eulerian from every vertex.

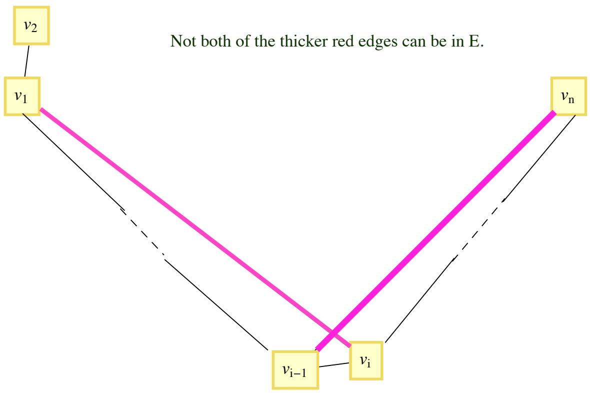








13. Addition of edges to E will certainly not decrease the degrees of each vertex. After adding some edges to E until no more can be added without allowing a Hamiltonian circuit, select $e = \{v_1, v_n\}$ not in the new, larger E. Since a Hamiltonian circuit exists in $(G, E \bigcup \{e\})$, there is a path in G that visits every vertex in the order $v_1, v_2, \ldots v_n$. Now for $2 \leq i \leq n$, if $\{v_1, v_i\} \in E$, then



$\{v_{i-1}, v_n\} \notin E$, for otherwise, $(v_1, v_2, \ldots, v_{i-1}, v_n, v_n, v_{n-1}, \ldots, v_i, v_1)$ is a Hamiltonian circuit.

Since $\{v_1, v_i\} \in E \Rightarrow \{v_{i-1}, v_n\} \notin E \Leftrightarrow \neg(\{v_1, v_i\} \in E$ and $\{v_{i-1}, v_n\} \in E)$, no more than $n - 1$ of the possible edges that connect v_1 and v_n to other vertices could be in E, even after adding edges to E. Therefore, for the original graph, with $\{v_1, v_n\} \notin E$, $deg\, v_1 + deg\, v_n < n$, a contradiction.

15. (a) $f(b, d) = f(c, d) = f(a, g) = f(y, t) = 1$, $f(d, t) = 2$, $V(f) = 3$.

(b) One flow-augmenting path is (s, a, g, t), which increased the flow value by 1, to 4. (A second one is (s, b, d, a, g, t).)

(c) The new flow is maximal since its value is equal to the sum of capacities into the sink.

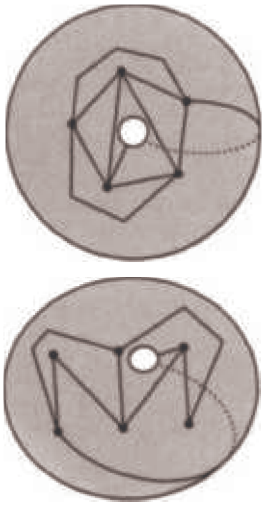
17.(a) (A, D, F, E, C, B, A)

(b) Starting at any city, it would take $n - 2$ seconds to decide where to go first. Then it would take $n - 3$ seconds from the next step, and so on. The total time would be

$$(n-2) + (n-3) + \cdots + 2 + 1 + 0 = \frac{1}{2\,(n-2)\,(n-1)} \text{ seconds}$$

$$\approx \frac{1}{2\,n^2} \text{ seconds, when } n \text{ is large.}$$

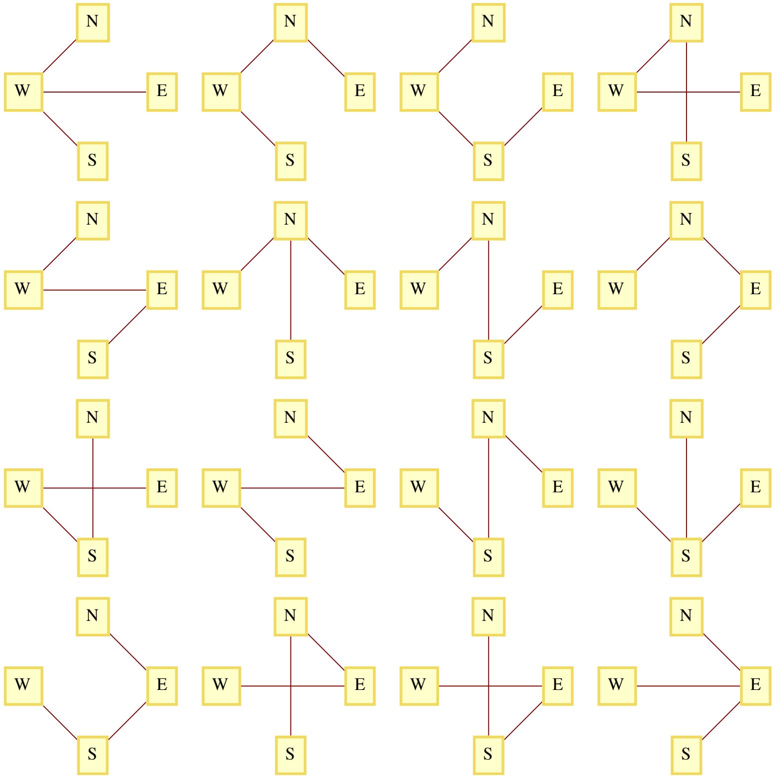
19.



CHAPTER 10

Section 10.1

1. The number of trees are: (a) 1, (b) 3, and (c) 16. The trees that connect V_c are:



3. *Hint:* Use induction on $|E|$.

5. (a) Assume that (V, E) is a tree with $|V| \geq 2$, and all but possibly one vertex in V has degree two or more.

$$2\,|E| = \sum_{v \in V} deg\,(v) \geq 2\,|V| - 1$$

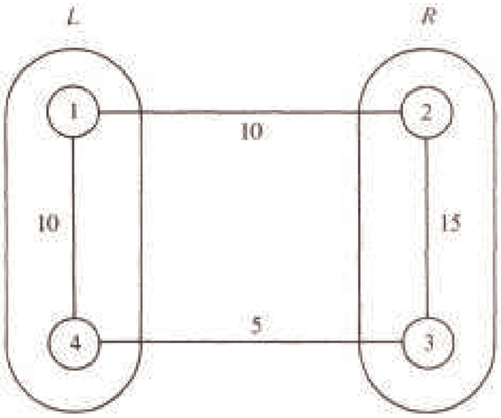
or $|E| \geq |V| - \frac{1}{2} \Rightarrow |E| \geq |V| \Rightarrow (V,\, E)$ is not a tree.

(b) The proof of this part is similar to part a in that we get $2\,|E| \geq 2\,|V| - 1$, since a tree that is not a chain has a vertex with degree three or more.

Section 10.2

1. It might not be most economical with respect to Objective 1. You should be able to find an example to illustrate this claim. The new system can always be made most economical with respect to Objective 2 if the old system were designed with that objective in mind.

3. In the figure below, {1, 2} is not a minimal bridge between $L = \{1, 4\}$ and $R = \{2, 3\}$, but it is part of the minimal spanning tree for this graph.



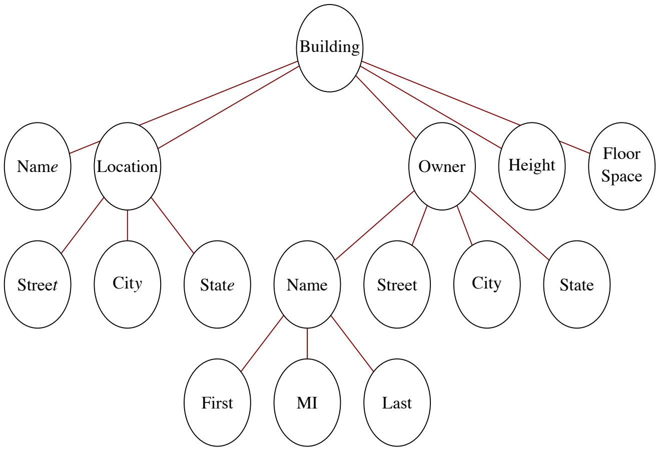
5, (a) Edges in one solution are: {8, 7}, {8, 9}, {8, 13}, {7, 6}, {9, 4}, {13, 12}, {13, 14}, {6, 11}, {6, 1}, {1, 2}, {4, 3}, {4, 5} {14, 15}, and {5, 10}

(b) Vertices 8 and 9 are at the center of the graph. Starting from vertex 8, a minimum diameter spanning tree is {{8, 3}, {8, 7}, {8, 13}, {8, 14}, {8, 9}, {3, 2}, {3, 4}, {7, 6}, {13, 12}, {13, 19}, {14, 15}, {9, 16}, {9, 10}, {6, 1}, {12, 18}, {16, 20}, {16, 17}, {10, 11}, {20, 21}, {11, 5}}. The diameter of the tree is 7.

Section 10.3

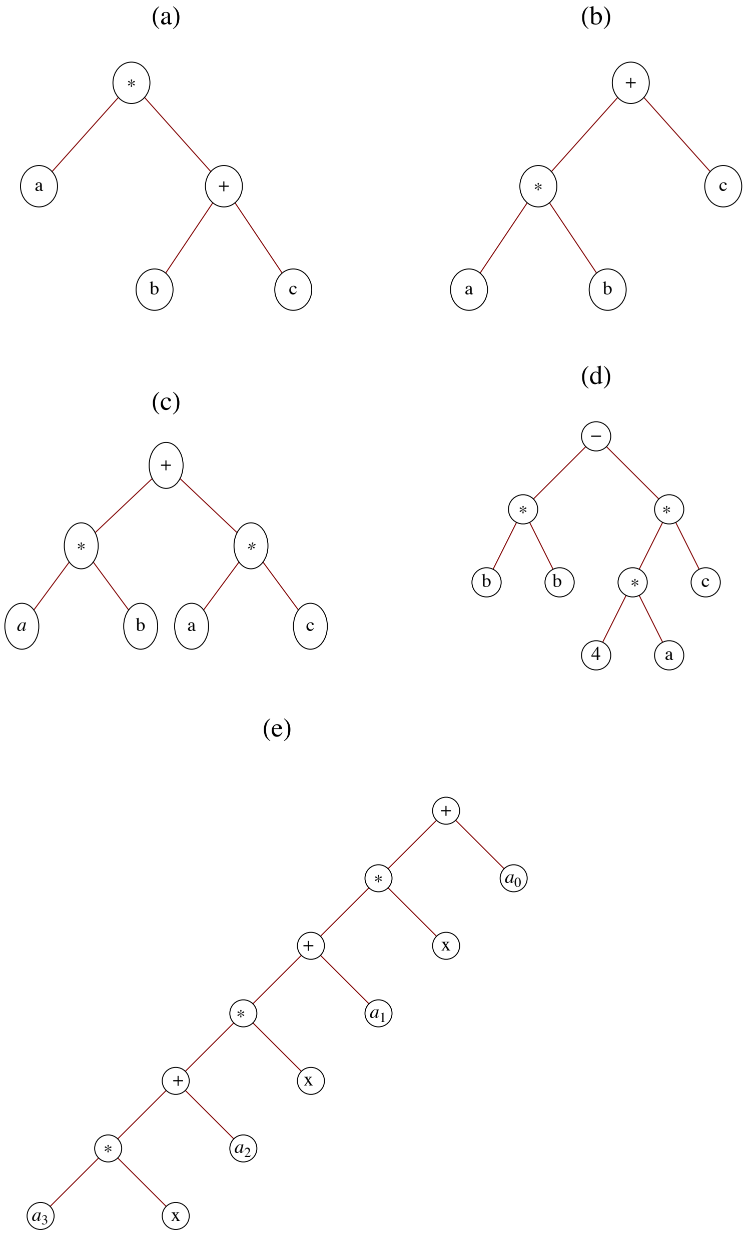
1. Locate any simple path of length d and locate the vertex in position $\lceil d/2 \rceil$on the path. The tree rooted at that vertex will have a depth of $\lceil d/2 \rceil$, which is minimal.

3.



Section 10.4

1.


(a)

(b)

(c)

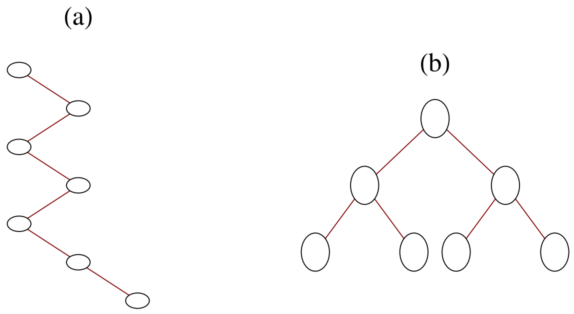
(d)

(e)

3.

	Preorder	Inorder	Postorder
(a)	$\cdot a+bc$	$a\cdot b+c$	$abc+\cdot$
(b)	$+\cdot abc$	$a\cdot b+c$	$ab\cdot c+$
(c)	$+\cdot ab\cdot ac$	$a\cdot b+a\cdot c$	$ab\cdot ac\cdot +$

5.



7. Solution #1:

Basis: A binary tree consisting of a single vertex, which is a leaf, satisfies the equation leaves = internal vertices + 1,

Induction: Assume that for some $k \geq 1$, all full binary trees with k or fewer vertices have one more leaf than internal vertices. Now consider any full binary tree with $k+1$ vertices. Let T_A and T_B be the left and right subtrees of the tree which, by the definition of a full binary tree, must both be full. If i_A and i_B are the numbers of internal vertices in T_A and T_B, and j_A and j_B are the numbers of leaves, then $j_A = i_A + 1$ and $j_B = i_B + 1$. Therefore, in the whole tree, the number of leaves $= j_A + j_B$
$= (i_A + 1) + (i_B + 1)$
$= (i_A + i_B + 1) + 1$
= (number of internal vertices) + 1

Solution #2: Imagine building a full binary tree starting with a single vertex. By continuing to add leaves in pairs so that the tree stays full, we can build any full binary tree. Our starting tree satisfies the condition that the number of leaves (1) is one more than the number of internal vertices (0). By adding a pair of leaves to a full binary tree, an old leaf becomes an internal vertex, increasing the number of internal vertices by one. Although we lose a leaf, the two added leaves create a net increase of one leaf. Therefore, the desired equality is maintained.

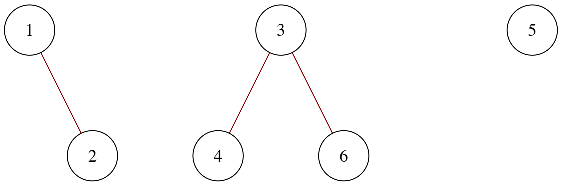
Supplementary Exercises—Chapter 10

1. Each of the $n-1$ edges of a tree contributes to the degrees of two vertices. Therefore the sum of all degrees of vertices in an n vertex tree is $2(n-1) = 2n - 2$.

3. (a) G_2 is graceful : $v_1 = 1,\ v_2 + 2,\ v_3 = 4$
G_4 is graceful : $v_1 = 2,\ v_2 = 1,\ v_3 = 3,\ v_4 = 4$

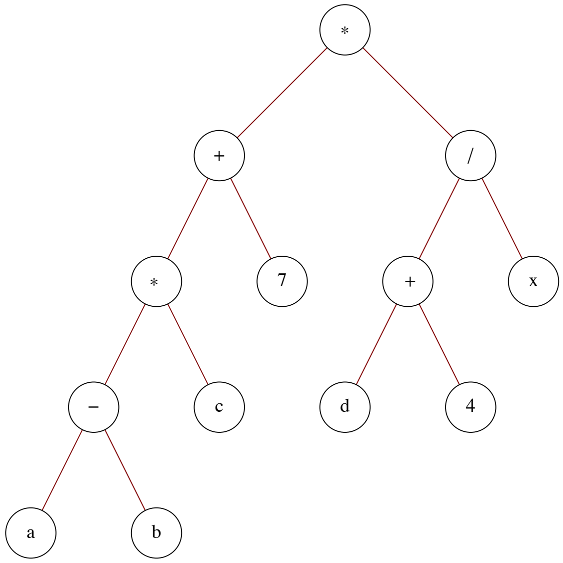
(b) Starting at either end of the chain label the first vertex $S(1) = 1$ and the $(k+1)$ st vertex, $k \geq 1$, $S(k+1) = S(k) + k$. The edge connecting the kth and $(k+1)$ st vertex is the kth edge and since $(S(k+1) - s(k)) = k$, the chain is graceful. The closed form expression for $S(k)$ is $1 + \left(k\left(k - \frac{1}{2}\right)\right)$.

5. First, {3, 6} is added to the edge set, then {1, 2} and {3, 4}. Then {4, 6} is rejected since it would complete a cycle. This can be seen from the forest.

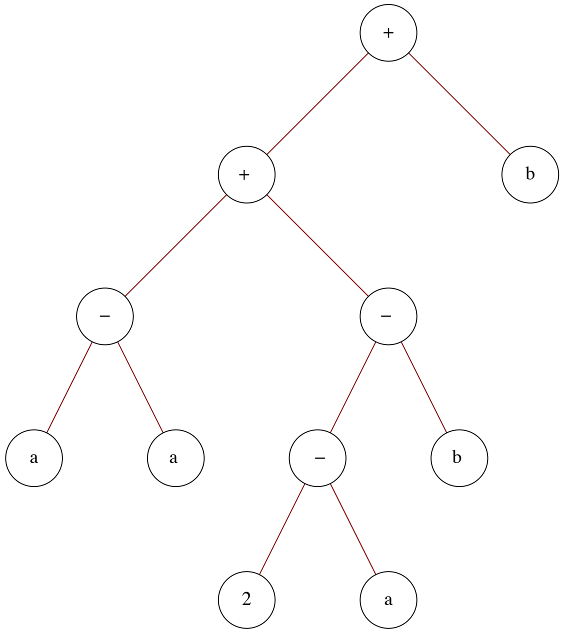


Vertices 4 and 6 have the same root in this tree; hence {4, 6} is rejected. {1, 5} and {2, 3} are the final edges that complete the minimal spanning tree. Notice that {4, 6} could have been the second edge selected. In that case, {3, 4} would be rejected.

7. The depth of the tree is four.



9. (a)



(b) $aa\cdot 2\,a\cdot b\cdot +b$ + is the postorder traversal of the tree. This is also the postfix version of the original expression.

CHAPTER 11

Section 11.1

1. (a) Commutative, and associative. Notice that zero is the identity for addition, but it is not a positive integer.)

(b) Commutative, associative, and has an identity (1)

(c) Commutative, associative, has an identity (1), and is idempotent

(d) Commutative, associative, and idempotent

(e) None. Note: $2 \ @ \ (3 \ @ \ 3) = 512$
$(2 \ @ \ 3) \ @ \ 3 = 64$

and while $a \ @ \ 1 = a$, $1 \ @ \ a = 1$.

3. $a,\ b \in A \bigcap B \ \Rightarrow \ a,\ b \in A$ by the definition of intersection
$\Rightarrow \ a * b \in A$ by the closure of A with respect to $*$

Similarly, $a,\ b \in A \bigcap B \Rightarrow a * b \in B$. Therefore, $a * b \in A \bigcap B$.

The set of positive integers is closed under addition, and so is the set of negative integers, but $1 + -1 - 0$. Therefore, their union, the nonzero integers, is not closed under addition.

5. Let $\mathbb{N}$ be the set of all nonnegative integers (the natural numbers).

(a) $*$ is commutative since $|a - b| = |b - a|$ for all $a,\ b \in \mathbb{N}$

(b) $*$ is not associative. Take $a = 1$, $b = 2$, and $c = 3$, then

$(a * b) * c = ||1 - 2| - 3| = 2$, and

$a * (b * c) = |1 - |2 - 3|| = 0$.

(c) Zero is the identity for $*$ on $\mathbb{N}$, since

$a * 0 = |a + 0| = a = |0 - a| = 0 * a$.

(d) $a^{-1} = a$ for each a $\in \mathbb{N}$, since

$a * a = |a - a| = 0$.

(e) $*$ is not idempotent, since, for $a \neq 0$,

$a * a = 0 \neq a$.

Section 11.2

1. The terms "generic" and "trade" for prescription drugs are analogous to "generic" and "concrete" algebraic systems. Generic aspirin, for example, has no name, whereas Bayer, Tylenol, Bufferin, and Anacin are all trade or specific types of aspirins. The same can be said of a generic group $[G,\ *]$ where G is a nonempty set and $*$ is a binary operation on G, When examples of typical domain elements can be given along with descriptions of how operations act on them, such as $\mathbb{Q}^*$ or $M_{2\times 2}(\mathbb{R})$, then the system is concrete (has a specific name, as with the aspirin). Generic is a way to describe a general algebraic system, whereas a concrete system has a name or symbols making it distinguishable from other systems.

3. b, d, e, and f.

5. (a) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, abelian

(b)

	I	R_1	R_2	F_1	F_2	F_3
I	I	R_1	R_2	F_1	F_2	F_3
R_1	R_1	R_2	I	F_2	F_3	F_1
R_2	R_2	I	R_1	F_3	F_1	F_2
F_1	F_1	F	F_2	I	R_2	R_1
F_2	F_2	F_1	F_3	R_1	I	R_2
F_3	F_3	F_2	F_1	R_2	R_1	I

This group is non-abelian since, for example, $F_1 F_2 = R_2$ and $F_2 F_1 = R_2$.

(c) 4! = 24, n!

7. The identity is e. $a*b = c, a*c = b, b*c = a$, and $[V, *]$ is abelian. (This group is commonly called the Klein-4 group.)

Section 11.3

1. (a) f is injective: $$\begin{aligned} f(x) = f(y) &\Rightarrow a * x = a * y \\ &\Rightarrow x = y \quad \text{(by left cancellation)} \end{aligned}$$

f is surjective: For all b, $f(x) = b$ has the solution $a^{-1} * b$.

(b) Functions of the form $f(x) = a + x$, where a is any integer, are bijections

3. Basis: $(n = 2)$ $(a_1 * a_2)^{-1} = {a_2}^{-1} * {a_1}^{-1}$ by Theorem 11.3.4.

Induction: Assume that for some $n \geq 2$,

$$(a_1 * a_2 * \cdots * a_n)^{-1} = {a_n}^{-1} * \cdots * {a_2}^{-1} * {a_1}^{-1}$$

We must show that

$$(a_1 * a_2 * \cdots * a_n * a_{n+1})^{-1} = {a_{n+1}}^{-1} * {a_n}^{-1} * \cdots * {a_2}^{-1} * {a_1}^{-1}$$

This can be accomplished as follows:

$$\begin{aligned} (a_1 * a_2 * \cdots * a_n * a_{n+1})^{-1} &= ((a_1 * a_2 * \cdots * a_n) * a_{n+1})^{-1} \quad \text{by the associative law} \\ &= {a_{n+1}}^{-1} * (a_1 * a_2 * \cdots * a_n)^{-1} \quad \text{by the basis} \\ &= {a_{n+1}}^{-1} * ({a_n}^{-1} * \cdots * {a_2}^{-1} * {a_1}^{-1}) \quad \text{by the induction hypothesis} \\ &= {a_{n+1}}^{-1} * {a_n}^{-1} * \cdots * {a_2}^{-1} * {a_1}^{-1} \quad \text{by the associative law } \blacksquare \end{aligned}$$

5. (a) Let $p(n)$ be, where a is any element of group $[G; *]$. First we will prove that $p(n)$ is true for all $n \geq 0$.

First, we would need to prove a lemma that we leave to the reader, that if $n \geq 0$, and a is any group element, $a * a^n = a^n * a$.

Basis: If $n = 0$, Using the definition of the zero exponent, $(a^0)^{-1} = e^{-1} = e$, while $(a^{-1})^0 = e$. Therefore, $p(0)$ is true.

Induction: Assume that for some $n \geq 0$, $p(n)$ is true.

$$\begin{aligned} (a^{n+1})^{-1} &= (a^n * a)^{-1} \quad \text{by the definition of exponentiation} \\ &= a^{-1} * (a^n)^{-1} \quad \text{by Theorem } 11.3\cdot 4 \\ &= a^{-1} * (a^{-1})^n \quad \text{by the induction hypothesis} \\ &= (a^{-1})^{n+1} \quad \text{by the lemma} \end{aligned}$$

If n is negative, then $-n$ is positive and

$$\begin{aligned} a^{-n} &= \left(\left((a^{-1})^{-1}\right)^{-n}\right) \\ &= (a^{-1})^{-(-n)} \quad \text{since the property is true for positive numbers} \\ &= (a^{-1})^n \end{aligned}$$

(b) For $m > 1$, let $p(m)$ be $a^{n+m} = a^n * a^m$ for all $n \geq 1$. The basis for this proof follows directly from the basis for the definition of exponentiation.

Induction: Assume that for some $m > 1$, $p(m)$ is true. Then

$$\begin{aligned} a^{n+(m+1)} &= a^{(n+m)+1} \quad \text{by the associativity of integer addition} \\ &= a^{n+m} * a^1 \quad \text{by the definition of exponentiation} \\ &= (a^n * a^m) * a^1 \quad \text{by the induction hypothesis} \\ &= a^n * (a^m * a^1) \quad \text{by associativity} \\ &= a^n * a^{m+1} \quad \text{by the definition of exponentiation} \end{aligned}$$

(c) Let $p(m)$ be $(a^n)^m = a^{n\,m}$ for all integers n.

Basis: $(a^m)^0 = e$ and $a^{m\cdot 0} = a^0 = e$ therefore, $p(0)$ is true.

Induction; Assume that $p(m)$ is true for some $m > 0$,

$$\begin{aligned} (a^n)^{m+1} &= (a^n)^m * a^n \quad \text{definition of exponentiation} \\ &= a^{n\,m} * a^n \quad \text{by the induction hypothesis} \\ &= a^{n\,m + n} \quad \text{by part } (a) \text{ of this problem} \\ &= a^{n(m+1)} \end{aligned}$$

Finally, if m is negative, we can verify that $(a^n)^m = a^{n m}$ using many of the same steps as the proof of part (a).

Section 11.4

1. (a) 2 (b) 5 (c) 0

(d) 0 (e) 2 (f) 2

(g) 1 (h) 3

3. (a) 1 (b) 1 (c) $m(4) = r(4)$, where $m = 11 q + r, 0 \leq r < 11$.

5. Since the solutions, if they exist, must come from $\mathbb{Z}_2$, substitution is the easiest approach.

(a) 1 is the only solution, since $1^2 +_2 1 = 0$ and $0^2 +_2 1 = 1$

(b) No solutions, since $0^2 +_2 0 +_2 1 = 1$, and $1^2 +_2 1 +_2 1 = 1$

7. Hint: Prove by induction on m that you can divide any positive integer into m, That is, let $p(m)$ be "For all n greater than zero, there exist unique integers q and r such that. . . ." In the induction step, divide n into m - n.

Section 11.5

1. a and c

3. $\{I, R_1, R_2\}$, $\{I, F_1\}$, $\{I, F_2\}$, and $\{I, F_3\}$ are all the proper subgroups of R_3.

5. (a) $\langle 1 \rangle = \langle 5 \rangle = \mathbb{Z}_6$

$\langle 2 \rangle = \langle 4 \rangle = \{2, 4, 0\}$

$\langle 3 \rangle = \{3, 0\}$

$\langle 0 \rangle = \{0\}$

(b) $\langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle = \mathbb{Z}_{12}$

$\langle 2 \rangle = \langle 10 \rangle = \{2, 4, 6, 8, 10, 0\}$

$\langle 3 \rangle = \langle 9 \rangle = \{3, 6, 9, 0\}$

$\langle 4 \rangle = \langle 8 \rangle = \{4, 8, 0\}$

$\langle 6 \rangle = \{6, 0\}$

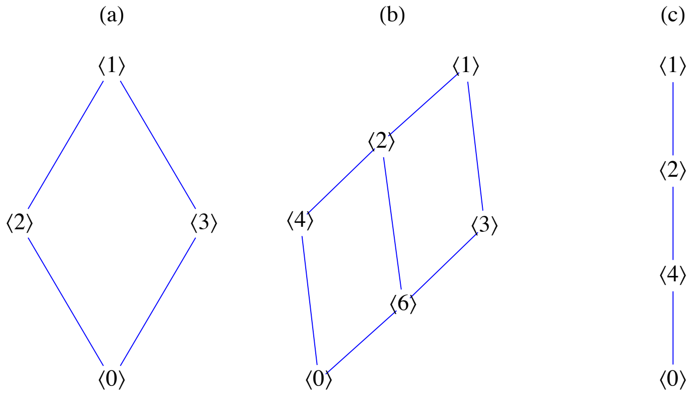
$\langle 0 \rangle = \{0\}$

(c) $\langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = \mathbb{Z}_8$

$\langle 2 \rangle = \langle 6 \rangle = \{2, 4, 6, 0\}$

$\langle 4 \rangle = \{4, 0\}$

$\langle 0 \rangle = \{0\}$



(d) Based on the ordering diagrams in parts a through c, we would expect to see an ordering diagram similar to the one for divides on $\{1, 2, 3, 4, 6, 8, 12, 24\}$ (the divisors of 24) if we were to examine the subgroups of $\mathbb{Z}_{24}$. This is indeed the case.

7. Assume that H and K are subgroups of group G, and that, as in Figure 11.5.1, there are elements $x \in H - K$ and $y \in K - H$. Consider the product $x * y$. Where could it be placed in the Venn diagram? If we can prove that it must lie in the outer region, $H^c \cap K^c = (H \cup K)^c$, then we have proven that $H \cup K$ is not closed under $*$ and can't be a subgroup of G, Assume that $x * y \in H$. Since x is in H, x^{-1} is in H and so by closure

$$x^{-1} * (x * y) = y \in H$$

which is a contradiction. Similarly, $x * y \notin K$. ■

One way to interpret this theorem is that no group is the union of two groups.

Section 11.6

1. Table of $\mathbb{Z}_2 \times \mathbb{Z}_3$:

y

x

*	{0, 0}	{0, 1}	{0, 2}	{1, 0}	{1, 1}	{1, 2}
{0, 0}	{0, 0}	{0, 1}	{0, 2}	{1, 0}	{1, 1}	{1, 2}
{0, 1}	{0, 1}	{0, 2}	{0, 0}	{1, 1}	{1, 2}	{1, 0}
{0, 2}	{0, 2}	{0, 0}	{0, 1}	{1, 2}	{1, 0}	{1, 1}
{1, 0}	{1, 0}	{1, 1}	{1, 2}	{0, 0}	{0, 1}	{0, 2}
{1, 1}	{1, 1}	{1, 2}	{1, 0}	{0, 1}	{0, 2}	{0, 0}
{1, 2}	{1, 2}	{1, 0}	{1, 1}	{0, 2}	{0, 0}	{0, 1}

The only two proper subgroups are $\{(0, 0), (1, 0)\}$ and $\{(0, 0), (0, 1), (0, 2)\}$

3. (a) (i) $a + b$ could be $(1, 0)$ or $(0, 1)$.

(ii) $a + b = (1, 1)$.

(b) (i) $a + b =$ could be $(1, 0, 0)$, $(0, 1, 0)$, or $(0, 0, 1)$.

(ii) $a + b = (1, 1, 1)$.

(c) (i) $a + b$ has exactly one 1.

(ii) $a + b$ has all 1's.

5. (a) No, 0 is not an element of $\mathbb{Z} \times \mathbb{Z}$.

(b) Yes.

(c) No, $(0, 0)$ is not an element of this set.

(d) No, the set is not closed: $(1, 1) + (2, 4) = (3, 5)$ and $(3, 5)$ is not in the set.

(e) Yes.

Section 11.7

1. (a) Yes, $f(n, x) = (x, n)$ for $(n, x) \in \mathbb{Z} \times \mathbb{R}$ is an isomorphism.

(b) No, $\mathbb{Z}_2 \times \mathbb{Z}$ has a finite proper subgroup while $\mathbb{Z} \times \mathbb{Z}$ does not.

(c) No.

(d) Yes.

(e) No.

(f) Yes, one isomorphism is defined by $f(a_1, a_2, a_3, a_4) = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$.

(g) Yes, one isomorphism is defined by $f(a_1, a_2) = (a_1, 10^{a_2})$.

(h) Yes.

(i) Yes $f(k) = k(1, 1)$.

3. Consider 3 groups G_1, G_2, and G_3 with operations $*$, $\diamond$, and $\square$, respectively.. We want to show that if G_1 is isomorphic to G_2 , and if G_2 is isomorphic to G_3 , then G_1 is isomorphic to G_3.

G_1 isomorphic to $G_2 \Rightarrow$ there exists an isomorphism $f : G_1 \to G_2$

G_2 isomorphic to $G_3 \Rightarrow$ there exists an isomorphism $g : G_2 \to G_3$

If we compose g with f, we get the function $g \circ f : G_1 \to G_3$, By Theorems 7.3.2 and 7.3.3, $g \circ f$ is a bijection, and if $a, b \in G_1$,

$$\begin{aligned}(g \circ f)(a * b) &= g(f(a * b))\\ &= g(f(a) \diamond f(b)) \text{ since } f \text{ is an isomorphism}\\ &= g(f(a)) \square g(f(b)) \text{ since } g \text{ is an isomorphism}\\ &= (g \circ f)(a) * (g \circ f)(b)\end{aligned}$$

Therefore, $g \circ f$ is an isomorphism from G_1 into G_3 , proving that “is isomorphic to" is transitive.

5. $\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4$, and $\mathbb{Z}_2{}^3$|. One other is the fourth dihedral group, introduced in Section 15.3.

7. Let G be an infinite cyclic group generated by a. Then, using multiplicative notation, $G = \{a^n \mid n \in \mathbb{Z}\}$.

The map $T : G \longrightarrow \mathbb{Z}$ defined by $T(a^n) = n$ is an isomorphism. This is indeed a function, since $a^n = a^m$ implies $n = m$. Otherwise, a would have a finite order and would not generate G.

(a) T is one-to-one, since $T(a^n) = T(a^m)$ implies $n = m$, so $a^n = a^m$.

(b) T is onto, since for any $n \in \mathbb{Z}$, $T(a^n) = n$.

(c) $$\begin{aligned}T(a^n * a^m) &= T(a^{n+m})\\ &= n + m\\ &= T(a^n) + T(a^m)\end{aligned}$$

Supplementary Exercises—Chapter 11

1. (a) With respect to V under $+$, the identity is a; and $-a = a$, $-b = c$, and $-c = b$.

(b) With respect to V under $\cdot$, the identity is b. Inverses: $b^{-1} = b$, $c^{-1} = c$, and a has no inverse,

(c) $\cdot$ is distributive over $+$ since $x \cdot (y + z) = x \cdot y + x \cdot z$ for each of the 27 ways that the variables x, y, and z can be assigned values from V. However, $+$ is not distributive over $\cdot$ since $b + (a \cdot c) = b$, while $(b + a) \cdot (b + c) = a$,

3. By Theorem 7.3.4 every bijection has an inverse, so $\circ$ has the inverse property on S. If $f \in S$,

$$f \circ f^{-1} = f^{-1} \circ f = i \;\Rightarrow\; f \text{ inverts } f^{-1}, \quad \text{or} \quad (f^{-1})^{-1} = f .$$

Therefore, inversion of functions has the involution property.

5. If a and b are odd integers, $a = 2j + 1$ and $b = 2k + 1$ for $j, k \in \mathbb{Z}$. $ab = (2j + 1)(2k + 1) = 2(2jk + j + k) + 1$, which is an odd integer. Since 1 is odd and $1 + 1$ is even, the odds are not closed under addition, The even integers are closed under both addition and multiplication. If a and b are even, $a = 2j$ and $b = 2k$ for some $j, k \in \mathbb{Z}$, $a + b = 2j + 2k = 2(j + k)$, which is even, and $ab = (2j)(2k) = 2(2jk)$, which is also even.

7. That $\text{GL}(2, \mathbb{R})$ is a group follows from laws of matrix algebra. In addition to being associative, matrix multiplication on two-by-two matrices has an identity I, and if $A \in \text{GL}(2, \mathbb{R})$, it has an inverse by the definition of $\text{GL}(2, \mathbb{R})$. The inverse of A is in $\text{GL}(2,\mathbb{R})$ since it has an inverse: $(A^{-1})^{-1} = A$.

9. If $a, b, c \in \mathbb{R}$,

$$\begin{aligned}(a * b) * c &= (a + b + 5) * c\\ &= a + b + 5 + c + 5\\ &= a + b + c + 10\end{aligned}$$

$a * (b * c)$ is also equal to $a + b + c + 10$, and so $*$ is associative. To find the identity we solve $a * e = a$ for e:

$$a * e = a \;\Rightarrow\; a + e + 5 = a \;\Rightarrow\; e = -5.$$

If a is a real number, the inverse of a is determined by solving the equation $a * x = -5$;

$$a * x = -5 \;\Rightarrow\; a + x + 5 = -5 \;\Rightarrow\; x = -a - 10$$

Since a is real, $-a - 10$ is real, and so $*$ has the inverse property.

11. By Supplementary Exercise 2 of this chapter, the identity for $*$ is 2 and $*$ is associative. All that is left to show is that * has the inverse property. If $a \in \mathbb{Q}^+$, $a * x = 2 \Rightarrow x = \frac{4}{a}$; hence $a^{-1} = \frac{4}{a}$, which is also a positive rational number.

13. Recall that matrix multiplication is the operation on GL(2, $\mathbb{R}$).

$$\begin{aligned} A\,X\,B = C \;&\Rightarrow\; X\,B = A^{-1}\,C \quad \text{(multiply on the left by } A^{-1}\text{)} \\ &\Rightarrow\; X = A^{-1}\,C\,B^{-1} \text{ (multiply on the right by } B^{-1}\text{)} \end{aligned}$$

$$X = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{3} \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{4} & 0 \\ -\frac{1}{6} & \frac{1}{3} \end{pmatrix}$$

15. (a) 1 (b) 4 (c) 0 (d) 3

17. (a) $\langle 1\rangle = \{1\}$, $\langle 3\rangle = \{1,\ 3\}$, $\langle 5\rangle = \{1,\ 5\}$, and $\langle 7\rangle = \{1,\ 7\}$.

(b) No, because no cyclic subgroup equals $U(\mathbb{Z}_8)$.

19. (a) $A,\ B \in$ SL(2, $\mathbb{R}$) $\Rightarrow |A| = |B| = 1$.

$$\begin{aligned} |A\,B| = |A|\cdot|B| = 1\cdot 1 = 1 \quad &\Rightarrow\quad A\,B \in \text{SL}(2, \mathbb{R}) \\ &\Rightarrow\ \text{SL}(2, \mathbb{R}) \text{ is closed with respect to matrix multiplication} \end{aligned}$$

(b) $|I| = 1 \;\Rightarrow\; I \in$ SL(2, $\mathbb{R}$)

(c) $A \in$ SL (2, $\mathbb{R}$) $\Rightarrow |A| = 1$

$$|A^{-1}| = |A|^{-1} = 1 \;\Rightarrow\; A^{-1} \in \text{SL}(2, \mathbb{R})$$

21. Yes, S is a submonoid of $B_{3\times 3}$. The zero matrix is in S since it is the matrix of the empty relation, which is symmetric. Furthermore, if A and B are matrices of symmetric relations,

$$\begin{aligned} (A + B)_{\text{ij}} &= A_{\text{ij}} + B_{\text{ij}} \quad \text{definition of matrix addition} \\ &= A_{\text{ji}} + B_{\text{ji}} \quad \text{since both } A \text{ and } B \text{ are symmetirc} \\ &= (A + B)_{\text{ji}} \quad \text{definition of matrix addition} \end{aligned}$$

Therefore, $A + B$ is symmetric, which means that it is the matrix of a symmetric relation and that relation is in S.

23. (a) (1, 4, 20) (b) (−1, 0, −1, −1) (c) (1 / 3 , 4) (d) (−2, −3, −5)

25. The groups in parts a and c are abelian, since each factor is abelian. The group in part b is non-abelian, since one of its factors, GL (2, $\mathbb{R}$), is non-abelian.

27, Since $\langle 4\rangle = \{0,\ 4,\ 8,\ 12\}$ is a cyclic group and has order four, it must be isomorphic to $\mathbb{Z}_4$,

29, (a) There exists a "dictionary" that allows us to translate between the two systems in such a way that any true fact in one is translated to a true fact in the other.

(b) If one system is familiar to you, the other one should be familiar too.

(c) If $(p \wedge \neg q) \Leftrightarrow 0$, and $(p \wedge q) \Leftrightarrow 0$, then $p \Leftrightarrow 0$.

31. The key to this exercise is to identify the fact that adding two complex numbers entails adding two pairs of numbers, the real and imaginary parts. If we simply rename these parts the first and second parts, then we are doing $\mathbb{R}^2$ addition. This suggests the function $T : \mathbb{C} \text{ — > } \mathbb{R}^2$ where $T(a + b\,i) = (a,\ b)$. For any two complex numbers $a + b\,i$ and $c + d\,i$,

$$\begin{aligned} T((a + b\,i) + (c + d\,i)) &= T\,((a + c) + (b + d)\,i) \quad \text{definition of } + \text{ in } \mathbb{C} \\ &= \{a + c,\ b + d) \quad \text{definition of } T \\ &= (a,\ b) + (c,\ d) \quad \text{definition of } + \text{ in } \mathbb{R}^2 \\ &= T(a + b\,i) + T(c + d\,i) \quad \text{definition of } T \end{aligned}$$

Since T has an inverse ($T^{-1}(a, b) = a + b\,i$), T is an isomorphism and so the two groups are isomorphic.

It should be noted that T is not the only isomorphism between these two groups. For example $U(a + b\,i) = (b,\ a)$ defines an isomorphism.

33. The key here is to realize that both groups consist of elements that are constructed from four real numbers and that you operate on elements by adding four different pairs of real numbers. An isomorphism from $\mathbb{R}^4$ into $M_{2\times 2}(\mathbb{R})$ is

$$T(a, b, c, d) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

There are an infinite number of isomorphism in this case. This one is the most obvious.

CHAPTER 12

Section 12.1

1. (a) $\{(4/3,\ 1/3)\}$

(b) $\{(-3\ -\ 0.5\,x_3,\ 11\ -\ 4\,x_3,\ x_3\,)\ |\ x_3\}$

(c) $\{(-5,\ 14/5,\ 8/5)\}$

(d) $\{(6.25\ -\ 2.5\,x_3,\ -0.75\ +\ 0.5\,x_3\ ,\ x_3)\ |\ x_3\ \in\ \mathbb{R}\}$

3. (a) $\{(1.2, 2.6, 4.5)\}$

(b) $\{(-6\,x_3 +\ 5,\ 2\,x_3\ +\ 1,\ x_3\,)\ |\ x_3\ \in\ \mathbb{R}\}$

(c) $\{(-9\,x_3\ +\ 3,\ 4,\ x_3\,)\ |\ x_3\ \in\ \mathbb{R}\}$

(d) $\{(3\,x_4\ +\ 1,\ -2\,x_4\ +\ 2,\ x_4\ +\ 1,\ x_4)\ |\ x_4\ \in\ \mathbb{R}\}$

5. (a) $\{(3, 0)\}$

(b)
$$\begin{pmatrix}1&1&2&1\\1&2&4&4\\1&3&3&0\end{pmatrix}\qquad \begin{matrix}\\-R_1+R_2\\-R_1+R_3\end{matrix}\ \rightarrow \begin{pmatrix}1&1&2&1\\0&1&2&3\\0&2&1&-1\end{pmatrix}$$

$$\begin{matrix}-R_2+R_1\\ \\ -2\,R_2+R_3\end{matrix}\ \rightarrow \begin{pmatrix}1&0&0&-2\\0&1&2&3\\0&0&-3&-7\end{pmatrix}$$

$$\begin{matrix}\\ \\ \frac{-1}{3}\,R_3\end{matrix}\ \rightarrow \begin{pmatrix}1&0&0&-2\\0&1&2&3\\0&0&1&\frac{7}{3}\end{pmatrix}$$

$$\frac{-1}{2}\,R_3+R_2 \rightarrow \begin{pmatrix}1&0&0&-2\\0&1&2&3\\0&0&1&\frac{7}{3}\end{pmatrix}$$

The row reduction can be done with *Mathematica*:

$$\texttt{RowReduce}\left[\begin{pmatrix}\mathbf{1}&\mathbf{1}&\mathbf{2}&\mathbf{1}\\\mathbf{1}&\mathbf{2}&\mathbf{4}&\mathbf{4}\\\mathbf{1}&\mathbf{3}&\mathbf{3}&\mathbf{0}\end{pmatrix}\right]$$

$$\begin{pmatrix}1&0&0&-2\\0&1&0&-\frac{5}{3}\\0&0&1&\frac{7}{3}\end{pmatrix}$$

In any case, the solution set is $\{(-2,\ -5/3,\ 7/3)\}$

7. Proof: Since b is the $n\times 1$ matrix of 0's, let's call it $\mathbf{0}$. Let S be the set of solutions to $A\,X\ =\ 0$. If X_1 and X_2 be in S. Then

$$A(X_1\ +\ X_2\,)\ =\ A\,X_1\ +\ A\,X_2\ =\ \mathbf{0}\ +\ \mathbf{0}\ =\ \mathbf{0}$$

so $X_1\ +\ X_2\ \in\ S$; that is, S is closed under addition.

The identity of $\mathbb{R}^n$ is $\mathbf{0}$, which is in S. Finally, let X be in S. Then

$$A(-X)\ =\ -(A\,X)\ =\ -\,\mathbf{0}\ =\ \mathbf{0}\ ,$$

and so $-X$ is also in S.

Section 12.2

(a) $\begin{pmatrix}\frac{15}{11}&\frac{30}{11}\\\frac{3}{11}&-\frac{5}{11}\end{pmatrix}$

(b) $\begin{pmatrix} -20 & \frac{21}{2} & \frac{9}{2} & -\frac{3}{2} \\ 2 & -1 & 0 & 0 \\ -4 & 2 & 1 & 0 \\ 7 & -\frac{7}{2} & -\frac{3}{2} & \frac{1}{2} \end{pmatrix}$

(c) The inverse does not exist. When the augmented matrix is row-reduced (see below), the last row of the first half cannot be manipulated to match the identity matrix.

(d) $\begin{pmatrix} 1 & 0 & 0 \\ -3 & 1 & 1 \\ -4 & 1 & 2 \end{pmatrix}$

(e) The inverse does not exist.

(f) $\begin{pmatrix} 9 & -36 & 30 \\ -36 & 192 & -180 \\ 30 & -180 & 180 \end{pmatrix}$

5. The solutions are in the solution section of Section 12.1, exercise 1, We illustrate with the outline of the solution to Exercise 1(c) of Section 12.1.

$$\begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & -1 \\ 1 & 3 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ 5 \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & -1 \\ 1 & 3 & 1 \end{pmatrix}^{-1} = \frac{1}{5} \begin{pmatrix} 5 & 5 & -5 \\ -2 & -1 & 3 \\ 1 & -2 & 1 \end{pmatrix}$$

$$\text{and} \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = A^{-1} \begin{pmatrix} 1 \\ -1 \\ 5 \end{pmatrix} = \begin{pmatrix} -5 \\ \frac{14}{5} \\ \frac{8}{5} \end{pmatrix}$$

Section 12.3

3. (b) Yes

7. If the matrices are named B, A_1, A_2 , A_3, and A_4 , then

$$B = \frac{8}{3} A_1 + \frac{5}{3} A_2 + \frac{-5}{3} A_3 + \frac{23}{3} A_4.$$

9. (a) If $x_1 = (1, 0), x_2 = (0, 1)$, and $y = (b_1, b_2)$, then

$$y = b_1 x_1 + b_2 x_2.$$

If $x_1 = (3, 2), x_2 = (2, 1)$, and $y = (b_1, b_2)$, then

$$y = (-b_1 + 2 b_2) x_1 + (2 b_1 - 3 b_2) x_2.$$

The second linear combination can be computed using *Mathematica* as follows.

```
Solve[c1 {3, 2} + c2 {2, 1} == {b1, b2}, {c1, c2}]
```

```
{{c1 → 2 b2 − b1, c2 → 2 b1 − 3 b2}}
```

(b) If $y = (b_1, b_2)$ is any vector in $\mathbb{R}^2$, then

$$y = (-3 b_1 + 4 b_2) x_1 + (-b_1 + b_2) x_2 + (0) x_3$$

(c) One solution is to add any vector(s) to x_1, x_2, and x_3 of part b.

(d) $2, n$

(e) If the matrices are A_1, A_2 , A_3, and A_4 , then

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} = x A_1 z + y A_2 + z A_3 + w A_4$$

(f) $a_0 + a_1 x + a_2 x^2 + a_3 x^3 = a_0(1) + a_1(x) + a_2(x^2) + a_3(x^3)$.

11. (a) The set is linearly independent: let a and b be scalars such that $a(4,\ 1)\ +\ b(1,\ 3)\ =\ (0,\ 0)$, then

$$\begin{aligned} 4a + b &= 0 \quad \text{and} \\ a + 3b &= 0 \end{aligned}$$

which has $a\ =\ b\ =\ 0$ as its only solutions. The set generates all of $\mathbb{R}^2$: let $(a,\ b)$ be an arbitrary vector in $\mathbb{R}^2$. We want to show that we can always find scalars β_1 and β_2 such that $\beta_1(4,\ 1)\ +\beta_2\,(1,3)\ =\ (a,\ b)$. This is equivalent to finding scalars such that $4\beta_1\ +\beta_2\ =\ a$ and $\beta_1\ +\ 3\beta_2\ =\ b$. This system has a unique solution $\beta_1\ =\ \frac{3a-b}{11}$, and $\beta_2\ =\ \frac{4b-a}{11}$. Therefore, the set generates $\mathbb{R}^2$.

13. (d) They are isomorphic. Once you have completed part (a) of this exercise, the following translation rules will give you the answer to parts (b) and (c),

$$(a, b, c, d) \leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \leftrightarrow a\ +\ b\,x + c\,x^2 +\ d\,x^2$$

Section 12.4

1. (a) Any nonzero multiple of $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$ is an eigenvector associated with $\lambda = 1$.

(b) Any nonzero multiple of $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ is an eigenvector associated with $\lambda = 4$.

(c) Let $x_1 = \begin{pmatrix} a \\ -a \end{pmatrix}$ and $x_2 = \begin{pmatrix} b \\ 2b \end{pmatrix}$. You can verify that $c_1\,x_1\ +\ c_2\,x_2 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ if and only if $c_1\ =\ c_2 = 0$. Therefore, $\{x_1,\ x_2\}$ is linearly independent.

3. (c) You should obtain $\begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$, depending on how you order the eigenvalues.

5. (a) If $P = \begin{pmatrix} 2 & 1 \\ 3 & -1 \end{pmatrix}$, then $P^{-1}\,A\,P = \begin{pmatrix} 4 & 0 \\ 0 & -1 \end{pmatrix}$.

(b) If $P = \begin{pmatrix} 1 & 1 \\ 7 & 1 \end{pmatrix}$, then $P^{-1}\,A\,P = \begin{pmatrix} 5 & 0 \\ 0 & -1 \end{pmatrix}$.

(c) If $P = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, then $P^{-1}\,A\,P = \begin{pmatrix} 3 & 0 \\ 0 & 4 \end{pmatrix}$.

(d) If $P = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 4 & 2 \\ -1 & 1 & 1 \end{pmatrix}$, then $P^{-1}\,A\,P = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

(e) A is not diagonalizable. Five is a double root of the characteristic equation, but has an eigenspace with dimension only 1.

(f) If $P = \begin{pmatrix} 1 & 1 & 1 \\ -2 & 0 & 1 \\ 1 & -1 & 1 \end{pmatrix}$, then $P^{-1}\,A\,P = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

7. (b) This is a direct application of the definition of matrix multiplication. Let $A_{(i)}$ stand for the i^{th} row of A, and let $P^{(j)}$ stand for the j^{th} column of P. Hence the j^{th} column of the product $A\,P$ is

$$\begin{pmatrix} A_{(1)}\,P^{(j)} \\ A_{(2)}\,P^{(j)} \\ \vdots \\ A_{(n)}\,P^{(j)} \end{pmatrix}$$

Hence, $(\mathrm{AP})^{(j)} = A\left(P^{(j)}\right)$ for $j\ = 1,\ 2,\ \ldots,\ n$. Thus, each column of $A\,P$ depends on A and the j^{th} column of P.

Section 12.5

3. If we introduce the superfluous equation $1\ =\ 0\cdot S_{k-1}\ +\ 1$ we have the system

$$\begin{aligned} S_k &= 5\,S_{k-1} + 4 \\ 1 &= 0\cdot S_{k-1}\ +\ 1 \end{aligned}$$

which, in matrix form, is:

$$\begin{aligned}\begin{pmatrix} S_k \\ 1 \end{pmatrix} &= \begin{pmatrix} 5 & 4 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} S_{k-1} \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} 5 & 4 \\ 0 & 1 \end{pmatrix}^k \begin{pmatrix} S_0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} 5 & 4 \\ 0 & 1 \end{pmatrix}^k \begin{pmatrix} 0 \\ 1 \end{pmatrix}\end{aligned}$$

Let A=$\begin{pmatrix} 5 & 4 \\ 0 & 1 \end{pmatrix}$. We want to diagonalize A; that is, find a matrix P such that $P^{-1} A P = D$, where D is a diagonal matrix, or

$$A = P D P^{-1} \Rightarrow A^k = P D^k P^{-1}$$

Diagonalizing A:

$$|A - c I| = \begin{vmatrix} 5-c & 4 \\ 0 & 1-c \end{vmatrix} = (5-c)(1-c)$$

The eigenvalues are $c = 1$ and $c = 5$. If $c = 1$,

$$\begin{pmatrix} 4 & 4 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

which implies $x_1 + x_2 = 0$, or $x_2 = -x_2$, and so $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$ is an eigenvector associated with 1.

If c = 5,

$$\begin{pmatrix} 0 & 4 \\ 0 & -4 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Rightarrow x_2 = 0.$$

Therefore, $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is an eigenvector associated with 5. Combining the two eigenvectors, we get

$$A = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

and

$$\begin{aligned}A^k &= \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}^k \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 5^k \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 5^k & 5^k - 1 \\ 0 & 1 \end{pmatrix}\end{aligned}$$

Hence, $\begin{pmatrix} S_k \\ 1 \end{pmatrix} = \begin{pmatrix} 5^k & 5^k - 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 5^k - 1 \\ 1 \end{pmatrix}$ and finally, $S_k = 5^k - 1$.

5. Since $A = A^1 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$, t here are 0 paths of length 1 from: node c to node a, node b to node h, and node a to node c; and there is 1 path of length 1 for every other pair of nodes.

(b) The characteristic polynomial is

$$|A - c I| = \begin{vmatrix} 1-c & 1 & 0 \\ 1 & -c & 1 \\ 0 & 1 & 1-c \end{vmatrix} = -c^3 + 2c^2 + c - 2$$

Solving the characteristic equation $-c^3 + 2c^2 + c - 2 = 0$ we find solutions 1, 2, and -1.

If $c = 1$, we find the associated eigenvector by finding a nonzero solution to

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & -1 & 1 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

One of these, which will be the first column of P, is $\begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$

If $c = 2$, the system $\begin{pmatrix} -1 & 1 & 0 \\ 1 & -2 & 1 \\ 0 & 1 & -1 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ yields eigenvectors, including $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$, which will be the second column of P.

If $c = -1$, then the system determining the eigenvectors is

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

and we can select $\begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$, although any nonzero multiple of this vector could be the third column of P.

(c) Assembling the results of (b) we have $P = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & -2 \\ -1 & 1 & 1 \end{pmatrix}$.

$$A^4 = P\begin{pmatrix} 1^4 & 0 & 0 \\ 0 & 2^4 & 0 \\ 0 & 0 & (-1)^4 \end{pmatrix}P^{-1} = P\begin{pmatrix} 1 & 0 & 0 \\ 0 & 16 & 0 \\ 0 & 0 & 1 \end{pmatrix}P^{-1}$$

$$= \begin{pmatrix} 1 & 16 & 1 \\ 0 & 16 & -2 \\ -1 & 16 & 1 \end{pmatrix}\begin{pmatrix} \frac{1}{2} & 0 & -\frac{1}{2} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{6} & -\frac{1}{3} & \frac{1}{6} \end{pmatrix}$$

$$= \begin{pmatrix} 6 & 5 & 5 \\ 5 & 6 & 5 \\ 5 & 5 & 6 \end{pmatrix}$$

Hence there are five different paths of length 4 between distinct vertices, and six different paths that start and end at the same vertex. The reader can verify these facts from Figure 12.4.1.

7. (a) $e^A = \begin{pmatrix} e & e \\ 0 & 0 \end{pmatrix}$, $e^B = \begin{pmatrix} 0 & 0 \\ 0 & e^2 \end{pmatrix}$, and $e^{A+B} = \begin{pmatrix} e & e^2 - e \\ 0 & e^2 \end{pmatrix}$

(b) Let $\mathbf{0}$ be the zero matrix, $e^{\mathbf{0}} = I + \mathbf{0} + \frac{\mathbf{0}^2}{2} + \frac{\mathbf{0}^3}{6} + \ldots = I$.

(c) Assume that A and B commute. We will examine the first few terms in the product $e^A e^B$. The pattern that is established does continue in general. In what follows, it is important that $A B = B A$. For example, in the last step, $(A + B)^2$ expands to $A^2 + A B + B A + B^2$, not $A^2 + 2 A B + B^2$, if we can't assume commutativity.

$$\begin{aligned} e^A e^B &= \left(\sum_{k=0}^{\infty} \frac{A^k}{k!}\right)\left(\sum_{k=0}^{\infty} \frac{B^k}{k!}\right) \\ &= \left(I + A + \frac{A^2}{2} + \frac{A^3}{6} + \cdots\right)\left(I + B + \frac{B^2}{2} + \frac{B^3}{6} + \cdots\right) \\ &= I + A + B + \frac{A^2}{2} + A B + \frac{B^2}{2} + \frac{A^3}{6} + \frac{A^2 B}{2} + \frac{A B^2}{2} + \frac{B^3}{6} + \cdots \\ &= I + (A + B) + \frac{1}{2}(A^2 + 2 A B + B^2) + \frac{1}{6}(A^3 + 3 A^2 B + 3 A B^2 + B^3) + \cdots \\ &= I + (A + B) + \frac{1}{2}(A + B)^2 + \frac{1}{6}(A + B)^3 + \cdots \\ &= e^{A+B} \end{aligned}$$

$(A + B)^2$ for $2AB + A^2 + B^2$.

$$e^A e^B = \left(\sum_{k=0}^{\infty} A^k/k!\right)\cdot\left(\sum_{k=0}^{\infty} B^k/k!\right)$$

(d) Since A and $-A$ commute, we can apply part d;

$$\begin{aligned} \mathbb{e}^{A}\, \mathbb{e}^{-A} &= \mathbb{e}^{A+(-A)} \\ &= \mathbb{e}^{\mathbf{0}} \\ &= I \qquad \text{by part } b \text{ of this problem.} \end{aligned}$$

Supplementary Exercises—Chapter 12

1. (a) $x_1 = x_2 = x_3 = 1$

(b) $x_1 = \frac{1}{2}, x_2 = 0, x_3 = \frac{1}{2}$

3. $\begin{pmatrix} -8 & -4 & 1 \\ 7 & 3 & -1 \\ -5 & -2 & 1 \end{pmatrix}$

5. Suppose that A^{-1} exists and that $\alpha_1(A\,x_1) + \alpha_2(A\,x_2)$ is equal to the zero vector, $\mathbf{0}$. By applying several laws of matrix algebra, this implies that

$$\begin{aligned} A(\alpha_1\, x_1 + \alpha_2\, x_2) = \mathbf{0} \quad &\Rightarrow\ \alpha_1\, x_1 + \alpha_2\, x_2 = \mathbf{0} \qquad \text{since } A^{-1} \text{ exists} \\ &\Rightarrow\ \alpha_1 = \alpha_2 = 0 \qquad \text{since } \{x_1, x_2\} \text{ is a basis} \\ &\Rightarrow\ \{A\,x_1, A\,x_2\} \text{ is linearly independent} \end{aligned}$$

To see that $\{A\,x_1, A\,x_2\}$ also spans $\mathbb{R}^2$, let $b \in \mathbb{R}^2$, we note that since $\{x_1, x_2\}$ is a basis, it will span $A^{-1}\,b$:

$$\alpha_1\, x_1 + \alpha_2\, x_2 = A^{-1}\, b \quad \text{for some } \alpha_1, \alpha_2 \in \mathbb{R}.$$

Using laws of matrix algebra:

$$\begin{aligned} \alpha_1\,(A\,x_1) + \alpha_2\,(A\,x_2) &= A(\alpha_1\, x_1 + \alpha_2\, x_2) \\ &= A(A^{-1}\, b) \\ &= b \end{aligned}$$

Hence, b is a linear combination of $A\,x_1$ and $A\,x_2$.

If A has no inverse, then $A\,x = \mathbf{0}$ has a nonzero solution y, which is spanned by the vectors x_1 and x_2 : $y = \alpha_1\, x_1 + \alpha_2\, x_2$, where not both of the α's are zero.

$$\begin{aligned} A\,y = 0 \ &\Rightarrow\ A(\alpha_1\, x_1 + \alpha_2\, x_2) = \mathbf{0} \\ &\Rightarrow\ \alpha_1(A\,x_1) + \alpha_2\,(A\,x_2) = 0 \\ &\Rightarrow \{A\,x_1, A\,x_2\} \text{ is linearly dependent} \end{aligned}$$

7. (b) $-X = X$

(c) $2^6 = 64$, since each entry can take on two possible values.

9. $A = P^{-1}\, D\, P \quad \Rightarrow \quad A^{100} = P^{-1}\, D^{100}\, P$

$$\begin{pmatrix} 0.6 & 0.2 \\ 0.4 & 0.8 \end{pmatrix} = \frac{1}{3}\begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}\begin{pmatrix} 1^{100} & 0 \\ 0 & 0.4^{100} \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix} \approx \begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{2}{3} & \frac{2}{3} \end{pmatrix}$$

Note: $0.4^{100} = 1.60694 \times 10^{-40} \approx 0$.

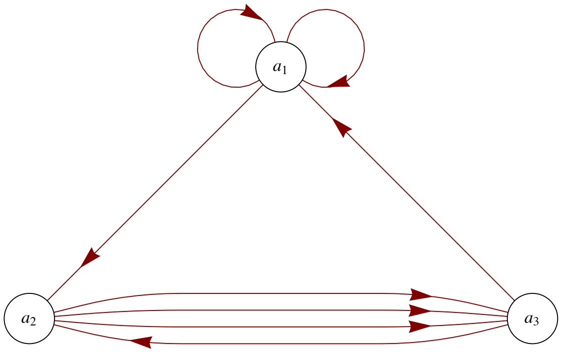
11. (a) $\lambda = 0, \ \pm\sqrt{2}$

(b) $B = P\,D\,P^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & -2 \end{pmatrix}\begin{pmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \frac{1}{2} \\ 0 & 0 & -\frac{1}{2} \end{pmatrix}$

13. (a) Let the vertices be a_1, a_2, and a_3; and use the convenient matrix representation

$$\begin{array}{c c} & \begin{array}{ccc} a_1 & a_2 & a_3 \end{array} \\ \begin{array}{c} a_1 \\ a_2 \\ a_3 \end{array} & \begin{pmatrix} 2 & 1 & 0 \\ 1 & 0 & 3 \\ 1 & 1 & 0 \end{pmatrix} \end{array}$$

one sees immediately, for example, that there are 3 different edges from a_2 to a_3, so that the multigraph is



(b) $A^2 = \begin{pmatrix} 5 & 2 & 3 \\ 5 & 4 & 0 \\ 3 & 1 & 3 \end{pmatrix}$ and by Theorem 12.5.1, $(A^2)_{i\,j}$ is the number of paths of length 2 from a_i to a_j. For example, the reader can verify from the graph that there are 3 different paths of length 2 from a_1 to a_3.

CHAPTER 13

Section 13.1

1. (a) 1, 5 (b) 5

(c) 30 (d) 30

(e) See Figure 13.4.1 with $0 = 1, a_1 = 2, a_2 = 3, a_3 = 5, b_1 = 6, b_2 = 10, b_3 = 15$, and $1 = 30$

3. Solution for Hasse diagram (b):

(a)

lub	a_1	a_2	a_3	a_4	a_5
a_1	a_1	a_2	a_3	a_4	a_5
a_2	a_2	a_2	a_4	a_4	a_5
a_3	a_3	a_4	a_3	a_4	a_5
a_4	a_4	a_4	a_4	a_4	a_5
a_5	a_5	a_5	a_5	a_5	a_5

glb	a_1	a_2	a_3	a_4	a_5
a_1	a_1	a_1	a_1	a_1	a_1
a_2	a_1	a_2	a_1	a_2	a_2
a_3	a_1	a_1	a_3	a_3	a_3
a_4	a_1	a_2	a_3	a_4	a_4
a_5	a_1	a_2	a_3	a_4	a_5

(b) a_1 is the least element and a_5 is the greatest element.

Partial solution for Hasse diagram (f):

(a) lub$(a_2,\ a_3)$ and lub(a_4, a_5) do not exist.

(b) No greatest element exists, but a_1 is the least element.

5. If 0 and 0' are distinct least elements, then

$$\left.\begin{array}{ll} 0 \le 0' & \text{since 0 is a least element} \\ 0' \le 0 & \text{since 0' is a least element} \end{array}\right\} \Rightarrow\ 0 = 0' \text{ by antisymmetry, a contradiction.} \blacksquare$$

Section 13.2

1. Assume to the contrary that a and b have two different greatest lower bounds, and call them g and h. Then $g \geq h$ since g is a greatest lower bound and $h \geq g$ since h is a greatest lower bound. Therefore, by antisymmetry $h = g$.

3. (a) See Table 13.3.1 for the statements of these laws. Most of the proofs follow from the definition of gcd and lcm.

(b) (partial) We prove two laws as examples.

Commutative law of join: Let $[L, \bigvee, \bigwedge]$ be a lattice, $a,\ b \in L$. We must prove that $a \bigvee b = b \bigvee a$.

Proof: By the definition of least upper bound, $a \bigvee b \geq b$ and $a \bigvee b \geq a$ therefore, by Exercise 4, part c, $a \bigvee b \geq b \bigvee a$. Similarly, $b \bigvee a \geq a \bigvee b$, and by antisymmetry $a \bigvee b = b \bigvee a$. $\blacksquare$

Idempotent law (for join): We must prove that for all $a \in L, a \vee a = a$.

Proof: By the reflexive property of $\leq$, $a \leq a$ and hence, by 4(c), $a \leq a \vee a$. But a is an upper bound for a; hence $a \geq a \vee a$. By antisymmetry, $a = a \vee a$. ■

Section 13.3

1.

B	Complement of B
$\emptyset$	A
$\{a\}$	$\{b, c\}$
$\{b\}$	$\{a, c\}$
$\{c\}$	$\{a, b\}$
$\{a, b\}$	$\{c\}$
$\{a, c\}$	$\{b\}$
$\{b, c\}$	$\{a\}$
A	$\emptyset$

This lattice is a Boolean algebra since it is a distributive complemented lattice.

3. a and g.

5. (a) $S^* : a \bigvee b = a$ if $a \geq b$

(b) $S : A \bigcap B = A$ if $A \subseteq B$

$S^* : A \bigcup B = A$ if $A \supseteq B$

(c) Yes

(d) $S : p \bigwedge q \Leftrightarrow p$ if $p \Rightarrow q$

$S^* : p \bigvee q \Leftrightarrow p$ if $q \Rightarrow p$

(e) Yes

7. **Definition: Boolean Algebra Isomorphism.** $[B, \bigwedge, \bigvee, -]$ is isomorphic to $[B', \bigwedge, \bigvee, \sim]$ if and only if there exists a function $T : B \rightarrow B'$ such that

(a) T is a bijection;

(b) $T(a \bigwedge b) = T(a) \bigwedge T(b)$ for all $a, b \in B$

(c) $T(a \bigvee b) = T(a) \bigvee T(b)$ for all $a, b \in B$

(d) $T(\overline{a}) = \widetilde{T(a)}$ for all $a \in B$.

Section 13.4

1. (a) For $a = 3$ we must show that for each $x \in D_{30}$ one of the following is true: $x \bigwedge 3 = 3$ or $x \bigwedge 3 = 1$. We do this through the following table:

x	verification
1	$1 \bigwedge 3 = 1$
2	$2 \bigwedge 3 = 1$
3	$3 \bigwedge 3 = 3$
5	$5 \bigwedge 3 = 1$
6	$6 \bigwedge 3 = 3$
10	$20 \bigwedge 3 = 1$
15	$15 \bigwedge 3 = 3$
30	$30 \bigwedge 3 = 3$

For $a = 5$, a similar verification can be performed.

(b) $6 = 2 \bigvee 3$, $10 = 2 \bigvee 5$, $15 = 3 \bigvee 5$, and $30 = 2 \bigvee 3 \bigvee 5$.

3. If $B = D_{30}$ 30 then $A = \{2, 3, 5\}$ and D_{30} is isomorphic to $\mathcal{P}(A)$, where

$$\begin{array}{cc} 1 \leftrightarrow \emptyset & 5 \leftrightarrow \{5\} \\ 2 \leftrightarrow \{2\} & 10 \leftrightarrow \{2,5\} \\ 3 \leftrightarrow \{3\} & 15 \leftrightarrow \{3,5\} \\ 6 \leftrightarrow \{2,3\} & 30 \leftrightarrow \{2,3,5 \end{array} \quad \text{and} \quad \begin{array}{c} \text{Join} \leftrightarrow \text{Union} \\ \text{Meet} \leftrightarrow \text{Intersection} \\ \text{Complement} \leftrightarrow \text{Set Complement} \end{array}$$

5. Assume that $x \neq 0$ or 1 is the third element of a Boolean algebra. Then there is only one possible set of tables for join and meet, all following from required properties of the Boolean algebra.

$\vee$	0	x	1
0	0	x	1
x	x	x	1
1	1	1	1

$\wedge$	0	x	1
0	0	0	0
x	0	x	x
1	0	x	1

Next, to find the complement of x we want y such that $x \wedge y = 0$ and $x \vee y = 1$. No element satisfies both conditions; hence the lattice is not complemented and cannot be a Boolean algebra. The lack of a complement can also be seen from the ordering diagram from which $\wedge$ and $\vee$ must be derived.

7. Let X be any countably infinite set, such as the integers. A subset of X is *cofinite* if it is finite or its complement is finite. The set of all cofinite subsets of X is:

(a) Countably infinite - this might not be obvious, but here is a hint. Assume $X = \{x_0, x_1, x_2, \ldots\}$. For each finite subset A of X, map that set to the integer

$$\sum_{i=0}^{\infty} \chi_A(x_i)\, 2^i$$

You can do a similar thing to sets that have a finite complement, but map them to negative integers. Only one minor adjustment needs to be made to accommodate both the empty set and X.

(b) Closed under union

(c) Closed under intersection, and

(d) Closed under complementation.

Therefore, if $B = \{A \subseteq X : A \text{ is cofinite}\}$, then B is a countable Boolean algebra under the usual set operations.

Section 13.5

1. (a)

$\vee$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,1)$	$(1,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,0)$	$(1,1)$
$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$

$\wedge$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(0,1)$	$(0,0)$	$(0,1)$	$(0,0)$	$(0,1)$
$(1,0)$	$(0,0)$	$(0,0)$	$(1,0)$	$(1,0)$
$(1,1)$	$(0,0)$	$(0,1)$	(10)	$(1,1)$

u	$\overline{u}$
$(0,0)$	$(1,1)$
$(0,1)$	$(1,0)$
$(1,0)$	$(0,1)$
$(1,1)$	$(0,0)$

(b) The graphs are isomorphic.

(c) $(0,1)$ and $(1,0)$

3. (a) $(1, 0, 0, 0)$, $(0, 1, 0, 0)$, $(0, 0, 1, 0)$, and $(0, 0, 0, 1)$ are the atoms.

(b) The n-tuples of 0's and 1's with exactly one 1.

Section 13.6

1 (a)

$$
\begin{aligned}
&M_1(x_1, x_2) = 0\\
&M_2(x_1, x_2) = (\overline{x_1} \wedge \overline{x_2})\\
&M_3(x_1, x_2) = (\overline{x_1} \wedge x_2)\\
&M_4(x_1, x_2) = (x_1 \wedge \overline{x_2})\\
&M_5(x_1, x_2) = (x_1 \wedge x_2)\\
&M_6(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \bigvee (\overline{x_1} \wedge x_2)) = \overline{x_1}\\
&M_7(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \bigvee (x_1 \wedge \overline{x_2})) = \overline{x_2}\\
&M_8(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \bigvee (x_1 \wedge x_2)) = ((x_1 \wedge x_2) \bigvee (\overline{x_1} \wedge \overline{x_2}))\\
&M_9(x_1, x_2) = ((\overline{x_1} \wedge x_2) \bigvee (x_1 \wedge \overline{x_2})) = ((x_1 \wedge \overline{x_2}) \bigvee (\overline{x_1} \wedge x_2))\\
&M_{10}(x_1, x_2) = ((\overline{x_1} \wedge x_2) \bigvee (x_1 \wedge x_2)) = x_2\\
&M_{11}(x_1, x_2) = ((x_1 \wedge \overline{x_2}) \bigvee (x_1 \wedge x_2)) = x_1\\
&M_{12}(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \bigvee (\overline{x_1} \wedge x_2) \bigvee (x_1 \wedge \overline{x_2})) = (\overline{x_1} \vee \overline{x_2})\\
&M_{13}(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \bigvee (\overline{x_1} \wedge x_2) \bigvee (x_1 \wedge x_2)) = (\overline{x_1} \vee x_2)\\
&M_{14}(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \bigvee (x_1 \wedge \overline{x_2}) \bigvee (x_1 \wedge x_2)) = (x_1 \vee \overline{x_2})\\
&M_{15}(x_1, x_2) = ((\overline{x_1} \wedge x_2) \bigvee (x_1 \wedge \overline{x_2}) \bigvee (x_1 \wedge x_2)) = (x_1 \vee x_2)\\
&M_{16}(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \bigvee (\overline{x_1} \wedge x_2) \bigvee (x_1 \wedge \overline{x_2}) \bigvee (x_1 \wedge x_2)) = 1
\end{aligned}
$$

(b) The truth table for the functions in part (a) are

x_1	x_2	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}	M_{16}
0	0	0	1	0	0	0	1	1	1	0	0	0	1	1	1	0	1
0	1	0	0	1	0	0	1	0	0	1	1	0	1	1	0	1	1
1	0	0	0	0	1	0	0	1	0	1	0	1	1	0	1	1	1
1	1	0	0	0	0	1	0	0	1	0	1	1	0	1	1	1	1

(c) $f_1(x_1, x_2) = M_{15}(x_1, x_2)$

$f_2(x_1, x_2) = M_{12}(x_1, x_2)$

$f_3(x_1, x_2) = M_1(x_1, x_2)$

$f_4(x_1, x_2) = M_{16}(x_1, x_2)$

3. (a) The number of elements in the domain of f is $16 = 4^2 = |B|^2$

(b) With two variables, there are $4^3 = 256$ different Boolean functions. With three variables, there are $4^8 = 65\,536$ different Boolean functions.

(c) $f(x_1, x_2) = (1 \bigwedge \overline{x_1} \bigwedge \overline{x_2}) \bigvee (1 \bigwedge \overline{x_1} \bigwedge x_2) \bigvee (1 \bigwedge x_1 \bigwedge \overline{x_2}) \bigvee (0 \bigwedge x_1 \bigwedge x_2)$

(d) Consider $f : B^2 \to B$, defined by $f(0, 0) = 0$, $f(0, 1) = 1$, $f(1, 0) = a$, $f(1, 1) = a$, and $f(0, a) = b$, with the images of all other pairs in B^2 defined arbitrarily. This function is not a Boolean function. If we assume that it is Boolean function then f can be computed with a Boolean expression $M(x_1, x_2)$. This expression can be put into minterm normal form:

$$M(x_1, x_2) = (c_1 \wedge \overline{x_1} \wedge \overline{x_2}) \bigvee (c_2 \wedge \overline{x_1} \wedge x_2) \bigvee (c_3 \wedge x_1 \wedge \overline{x_2}) \bigvee (c_4 \wedge x_1 \wedge x_2)$$

$$
\begin{aligned}
&f(0, 0) = 0 \Rightarrow M(0, 0) = 0 \Rightarrow c_1 = 0\\
&f(0, 1) = 1 \Rightarrow M(0, 0) = 1 \Rightarrow c_1 = 1\\
&f(1, 0) = a \Rightarrow M(0, 0) = a \Rightarrow c_1 = a\\
&f(1, 1) = a \Rightarrow M(0, 0) = a \Rightarrow c_1 = a
\end{aligned}
$$

Therefore,

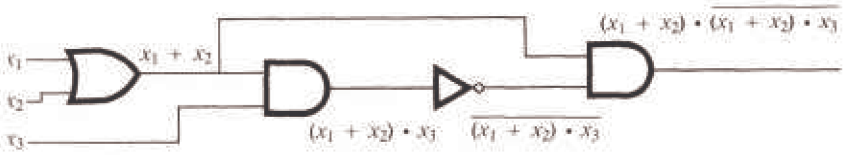
$$M(x_1, x_2) = (\overline{x_1} \wedge x_2) \bigvee (a \wedge x_1 \wedge \overline{x_2}) \bigvee (a \wedge x_1 \wedge x_2)$$

$$M(0, a) = \left(\overline{0} \wedge a\right) \bigvee (a \bigwedge 0 \bigwedge \overline{a}) \bigvee (a \bigwedge 0 \bigwedge a) = a$$

This contradicts $f(0, a) = b$, and so f is not a Boolean function.

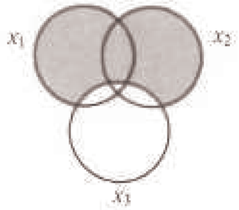
Section 13,7

1. (a)


x_1
x_2
x_3
$x_1 + x_2$
$(x_1 + x_2) \cdot x_3$
$\overline{(x_1 + x_2) \cdot x_3}$
$(x_1 + x_2) \cdot \overline{(x_1 + x_2) \cdot x_3}$

(b) $$\begin{aligned} f(x_1, x_2, x_3) &= \overline{((x_1 + x_2) \cdot x_3)} \cdot (x_1 + x_2) \\ &= \left(\overline{(x_1 + x_2)} + \overline{x_3}\right) \cdot (x_1 + x_2) \\ &= \overline{(x_1 + x_2)} \cdot (x_1 + x_2) + \overline{x_3} \cdot (x_1 + x_2) \\ &= 0 + \overline{x_3} \cdot (x_1 + x_2) \\ &= \overline{x_3} \cdot (x_1 + x_2) \end{aligned}$$

(c) The Venn diagram for the function is:

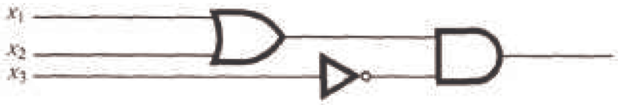


We can read off the minterm normal form from this diagram:

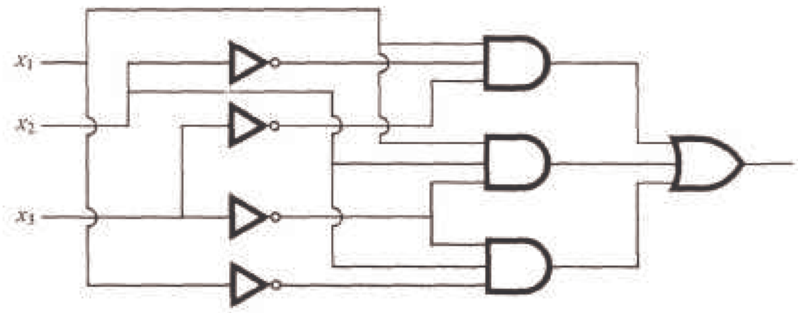
$$f(x_1, x_2, x_3) = x_1 \cdot \overline{x_2} \cdot \overline{x_3} + x_1 \cdot x_2 \cdot \overline{x_3} + \overline{x_1} \cdot x_2 \cdot \overline{x_3}$$

(d)

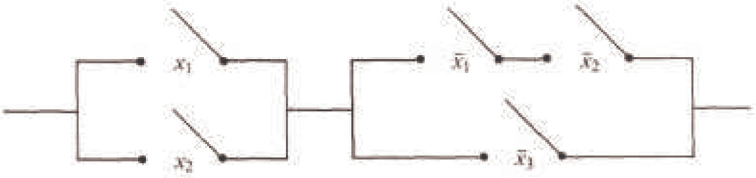
Simplified form:



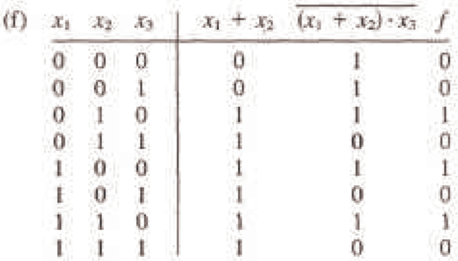
Minterm form:



(e)

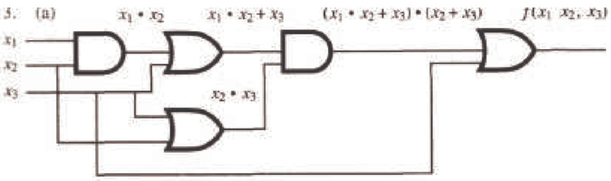


(f)



x_1	x_2	x_3	$x_1 + x_2$	$\overline{(x_1 + x_2) \cdot x_3}$	f
0	0	0	0	1	0
0	0	1	0	1	0
0	1	0	1	1	1
0	1	1	1	0	0
1	0	0	1	1	1
1	0	1	1	0	0
1	1	0	1	1	1
1	1	1	1	0	0

Current will flow only when one of the switches x_1 or x_2 is On and x_3 is Off.



(b) $f(x_1, x_2, x_3) = (((x_1 \cdot x_2) + x_3) \cdot (x_2 + x_3)) + x_3$

placing ( )' s to indicate order of evaluation

$= (((x_1 \cdot x_2) \cdot (x_2)) + x_3) + x_3$

by the distributive law of + over ·

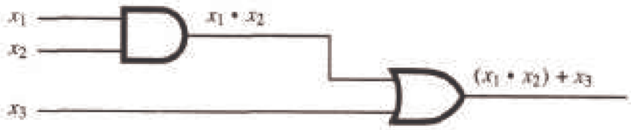
$= (x_1 \cdot (x_2 \cdot x_2)) + (x_3 + x_3)$

by the associative laws of · and +

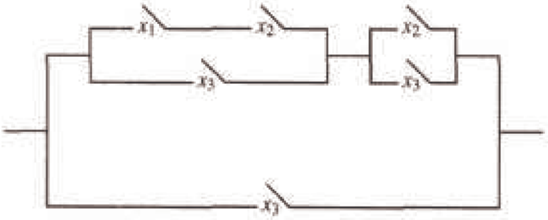
$= (x_1 \cdot x_2) + x_3$

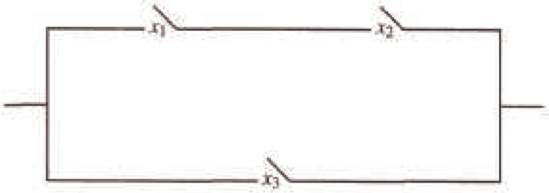
by the idempotent laws of · and +

(c)



(d)

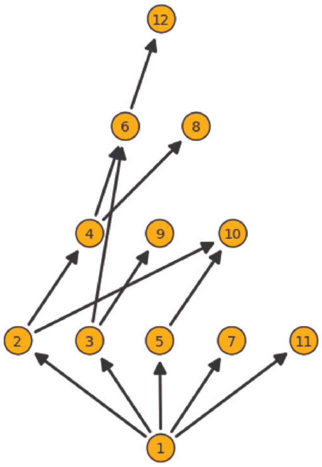




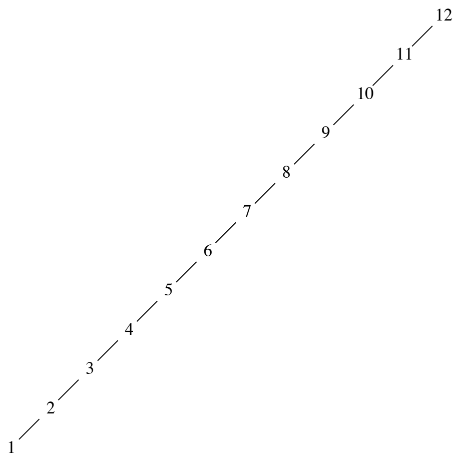
Supplementary Exercises—Chapter 13

1. (a) The following Sage input generates an ordering diagram.

Poset({1:[2,3,5,7,11],2:[4,6,10],3:[6,9],4:[6,8,12],5:[10],6:[12]}).plot()



(b) The ordering diagram for ≤ is a chain



3. (a) $4 \bigvee 8 = 8, 3 \bigvee 15 = 15, 4 \bigwedge 8 = 4, 3 \bigwedge 15 = 3, 3 \bigwedge 5 - 15.$

(b) Yes. Let $a,\ b,\ c \in P$ and assume that there are n primes, $p_1, p_2, \ldots, p_n$ that appear as factors of a, b and c. Then we can write

$$a = {p_1}^{i_1}\, {p_2}^{i_2} \cdots {p_n}^{i_n}$$

$$b = {p_1}^{j_1}\, {p_2}^{j_2} \cdots {p_n}^{j_n}$$

$$c = {p_1}^{k_1}\, {p_2}^{k_2} \cdots {p_n}^{k_n}$$

where each exponent is a nonnegative integer. The greatest common divisor and least common multiple of two integers such as a and b can be expressed in terms of these exponents.

$$a \bigwedge b = \gcd(a,\ b) = {p_1}^{m_1}\, {p_2}^{m_2} \cdots {p_n}^{m_n}$$

where $m_r = \min(i_r,\ j_r)$ and

$$a \bigvee b = \operatorname{lcm}(a,\ b) = {p_1}^{M_1}\, {p_2}^{M_2} \cdots {p_n}^{M_n}$$

where $M_r = \max(i_r,\ j_r)$.

Based on this observation, we can compare $a \bigwedge (b \bigvee c)$ and $(a \bigwedge b) \bigvee (a \wedge c)$. The exponent of p, is $\min(i_r, \max(j_r,\ k_r))$ in $a \bigwedge (b \bigvee c)$ and $\max(\min(i_r,\ j_r), \min(i_r,\ k_r))$ in $(a \bigwedge b) \bigvee (a \wedge c)$. These two exponents are equal; this is easiest to verify by checking the possible relative sizes of i_r, j_r and k_r. Therefore, the lattice is distributive.

(c) The least element is 1. There is no greatest element.

5. (a) The ordering diagram is the one-cube in Figure 9.4.5. It is interesting to note that the poset relation is really the logical implication, ⇒, since $0 \Rightarrow 0,\ 0 \Rightarrow 1, 1 \Rightarrow 1$ are all true statements.

(b) From the definitions of lub and glb and part (a) we have the tables

$\bigwedge$	0	1
0	0	0
1	0	1

$\bigvee$	0	1
0	0	1
1	1	1

which are the logical tables for the connectives "and" and "or."

(c) $L^2 = L \times L = \{(0,\ 0),\ (0,\ 1),\ (1,\ 0),\ (1,\ 1)\}$ where the poset relation $\leq$ on L^2 and the binary operations $\wedge$ and $\vee$ are all defined componentwise so that, for example, $(0,\ 1) \leq (1,\ 1)$, since in the two first coordinates, $0 \leq 1$ and in the two second coordinates, $1 \leq 1$. Also, for example, $(0,\ 1) \bigwedge (1,\ 0) = (0 \bigwedge 1,\ 1 \bigwedge 0) = (0,\ 0)$. The operation tables are given in the solution of Exercise 1 Section 13.5. The Hasse diagram for L^2 is the two-cube.

(d) The Hasse diagram for L^3 is the three-cube. Tables for $\wedge$ and $\vee$ can

easily be constructed where, for example,

$$(1,\ 0,\ 0) \bigvee (0,\ 1,\ 0) = (1 \bigvee 0, 0 \bigvee 1, 0 \bigvee 0) = (1, 1, 0)$$

7. (a) No. It is not true that every pair of elements in A has both a *lub* and a *glb*

in A. For example, $10 \bigvee 4$ does not exist in A.

(b) Yes. For all $a,\ b \in A, a \neq b$,

$a \bigvee b =$ the maximum of a and b,

$a \bigwedge b =$ the minimum of a and b.

9. $(x + y) \cdot (x + \overline{y}) = x + (y \cdot \overline{y})$ by the distributive law of $+$ over $\cdot$
$= x + 0$ by the complement law
$= x$ by the identity law

The switching circuit diagram has a single switch labeled x.

11. (a)

x	complement(s) of x
0	1
a_1	a_2, a_3, a_4, a_6
a_2	a_1, a_5
a_3	a_1, a_5
a_4	a_1, a_5
a_5	a_2, a_3, a_4, a_6
a_6	a_1, a_5
1	0

(b) No, it is not distributive, for if it were, complements would be unique.

13. (a) $D_{20} = \{1, 2, 4, 5, 10, 20\}$ contains 6 elements and so cannot be a Boolean algebra by Corollary 13.4.1.

(b) $D_{27} = \{1, 3, 9, 27\}$ has four elements and so we cannot use Corollary 13.4.1 to rule it out as a Boolean algebra. However, 3 has no complement, which means that D_{27} is not a Boolean algebra.

(c) $D_{35} = \{1, 5, 7, 35\}$ has $4 = 2^2$ elements, and so that it may be a Boolean algebra by Corollary 13.4.1. We can confirm through the definition of a Boolean algebra that it is.

(d) Notice that $210 = 2 \cdot 3 \cdot 5 \cdot 7$, which means that $|D_{210}| = 16 = 2^4$ and so Corollary 13.4.1 can’t be used to rule it out as a Boolean algebra. Indeed, D_{210} is a Boolean algebra, which can be confirmed by applying the definition of a Boolean algebra.

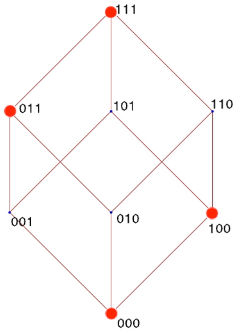
15. (a) First, by definition of subsystem in Section 11.5, a sub-Boolean algebra of a Boolean algebra B is a subset W of B which is a Boolean algebra under the same operations as B. Specifically, W must satisfy the conditions:

(i) The 0 and 1 of B must be in W,

(ii) $a \in W \Rightarrow \overline{a} \in W$

(iii) $a, b \in W \Rightarrow a \bigvee b \in W$ and $a \bigwedge b \in W$.

Hence if W is to contain 4 elements it must be of the form $\{0, \beta, \overline{\beta}, 1\}$. $W_1 = \{(0, 0, 0), (0, 1, 1), (1, 0, 0), (1, 1, 1)\}$ is one such set. The 3-cube below illustrates this sub-Boolean algebra.



There are two others that are isomorphic to this one, where Corollary 13.4.2, assures us of this isomorphism.

(b) Again, the form of the sub-Boolean algebra with four elements must be $\{0, \beta, \overline{\beta}, 1\}$. Since the 2^n elements of ${B_2}^n$ can be paired up with their complements to give us 2^{n-1} pairs, there are $2^{n-1} - 1$ ways to select the elements β and $\overline{\beta}$ (0 and its complement, 1, are already selected). Of course, all of these sub-Boolean algebras are isomorphic.

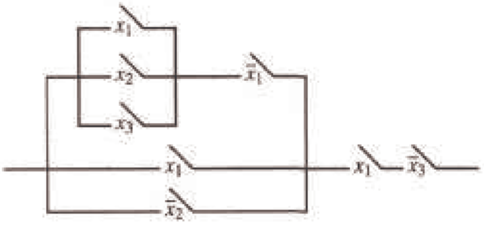
(c) A sub-Boolean algebra with 2^k elements must have k atoms; so the selection of k elements that will act as atoms can be considered in counting numbers of sub-Boolean algebras of a certain size. What is the number? We leave it to the reader in the general case.

17. $(\overline{x_1} \wedge x_2 \wedge x_3) \bigvee (\overline{x_1} \wedge \overline{x_2} \wedge x_3) \bigvee (x_1 \wedge x_2 \wedge x_3)$

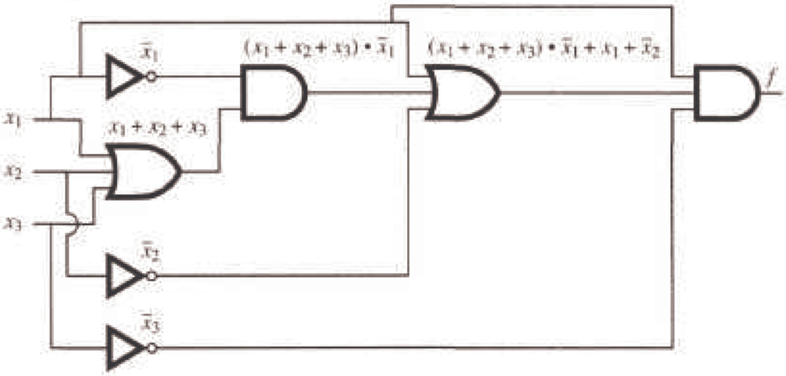
19. (a) Since each of the three variables can be any one of two values there are 2^3 rows, (See Table 13.6.3 for an example.) For n variables there are 2^n rows.

(b) For each row, there can be any one of two truth values. Since there are $2^3 = 8$ rows there are $2^8 = 256$ functions. For n variables and $m = 2^n$ rows, there are $2^m = 2^{2^n}$ functions.

21. (a)



(b)


$\overline{x}_1$
$(x_1 + x_2 + x_3) \bullet \overline{x}_1$
$(x_1 + x_2 + x_3) \bullet \overline{x}_1 + x_1 + \overline{x}_2$
f
x_1
$x_1 + x_2 + x_3$
x_2
x_3
$\overline{x}_2$
$\overline{x}_3$

(c) $f(x_1, x_2, x_3) = ((x_1 + x_2 + x_3)\cdot\overline{x_1} + x_1 + \overline{x_2})\cdot x_1 \cdot \overline{x_3}$

$$= (x_1 \cdot \overline{x_1} + x_2 \cdot \overline{x_1} + x_3 \cdot \overline{x_1} + x_1 + \overline{x_2}) \cdot x_1 \cdot \overline{x_3}$$
$$= (0 + x_2 \cdot \overline{x_1} + x_3 \cdot \overline{x_1} + x_1 + \overline{x_2}) \cdot x_1 \cdot \overline{x_3}$$
$$= (x_2 \cdot \overline{x_1} + x_3 \cdot \overline{x_1} + x_1 + \overline{x_2}) \cdot x_1 \cdot \overline{x_3}$$
$$= x_2 \cdot \overline{x_1} \cdot x_1 \cdot \overline{x_3} + x_3 \cdot \overline{x_1} \cdot x_1 \cdot \overline{x_3} + x_1 \cdot x_1 \cdot \overline{x_3} + \overline{x_2} \cdot x_1 \cdot \overline{x_3}$$
$$= x_2 \cdot 0 \cdot \overline{x_3} + x_3 \cdot 0 \cdot \overline{x_3} + x_1 \cdot \overline{x_3} + \overline{x_2} \cdot x_1 \cdot \overline{x_3}$$
$$= x_1 \cdot \overline{x_3} + \overline{x_2} \cdot x_1 \cdot \overline{x_3}$$
$$= x_1 \cdot \overline{x_3} \cdot (1 + \overline{x_2})$$

Switching and gate diagrams to be added.

23. (a) $z = (\overline{x_1} + x_2) + \overline{x_2 \cdot x_3}$

(b) $z = (\overline{x_1} + x_2) + \overline{x_2 \cdot x_3}$

$$= (\overline{x_1} + x_2) + (\overline{x_2} + \overline{x_3})$$
$$= \overline{x_1} + (x_2 + \overline{x_2}) + \overline{x_3}$$
$$= \overline{x_1} + 1 + \overline{x_3}$$
$$= 1$$

The circuit is always on, no gates are necessary.

CHAPTER 14

Section 14.1

1. (a) S_1 is not a submonoid since the identity of $[\mathbb{Z}_8, \times_8]$, which is 1, is not in S_1. S_2 is a submonoid since $1 \in S_2$ and S_2 is closed under multiplication; that is, for all $a,\ b \in S_2, a \times_8 b$ is in S_2.

(b) The identity of $\mathbb{N}^{\mathbb{N}}$ is the identity function $i : \mathbb{N} \rightarrow \mathbb{N}$ defined by $i(a) = a, \forall a \in \mathbb{N}$. If $a \in \mathbb{N}, i(a) = a \leq a$, thus the identity of $\mathbb{N}^{\mathbb{N}}$ is in S_1.

However, the image of 1 under any function in S_2 is 2, and thus the identity of $\mathbb{N}^{\mathbb{N}}$ is not in S_2, so S_2 is not a submonoid. The composition of any two functions in S_1, f and g, will be a function in S_1:

$$\begin{aligned}(f \circ g)(n) = f(g(n)) &\leq g(n) \quad \text{since } f \text{ is in } S_1 \\ &\leq n \quad \text{since } g \text{ is in } S_1\end{aligned}$$

Thus $f \circ g \in S_1$, and the two conditions of a submonoid are satisfied and S_1 is a submonoid of $\mathbb{N}^{\mathbb{N}}$.

(c) The first set is a submonoid, but the second is not since the null set has a non-finite complement.

3. The set of $n \times n$ real matrices is a monoid under matrix multiplication. This follows from the laws of matrix algebra in Chapter 5. To prove that the set of stochastic matrices is a monoid over matrix multiplication, we need only show that the identity matrix is stochastic (this is obvious) and that the set of stochastic matrices is closed under matrix multiplication. Let A and B be $n \times n$ stochastic matrices.

$$(A\,B)_{i\,j} = \sum_{k=1}^{n} a_{i\,k}\, b_{k\,j}$$

The sum of the j^{th} column is

$$\begin{aligned}\sum_{j=1}^{n} (A\,B)_{i\,j} &= \sum_{k=1}^{n} a_{1\,k}\, b_{k\,j} + \sum_{k=1}^{n} a_{1\,k}\, b_{k\,j} + \cdots + \sum_{k=1}^{n} a_{n\,k}\, b_{k\,j} \\ &= \sum_{k=1}^{n} \left(a_{1\,k}\, b_{k\,j} + a_{1\,k}\, b_{k\,j} + \cdots + a_{n\,k}\, b_{k\,j}\right) \\ &= \sum_{k=1}^{n} b_{k\,j}(a_{1\,k} + a_{1\,k} + \cdots + a_{n\,k}) \\ &= \sum_{k=1}^{n} b_{k\,j} \qquad \text{since } A \text{ is stochastic} \\ &= 1 \qquad \text{since } B \text{ is stochastic}\end{aligned}$$

Section 14.2

1. (a) For a character set of 350 symbols, the number of bits needed for each character is the smallest n such that 2^n is greater than or equal to 350. Since $2^9 = 512 > 350 > 2^8$, 9 bits are needed,

(b) $2^{12} = 4096 > 3500 > 2^{11}$; therefore, 12 bits are needed.

3. This grammar defines the set of all strings over B for which each string is a palindrome (same string if read forward or backward).

5. (a) Terminal symbols: The null string, 0, and 1.

Nonterminal symbols: S, E.

Starting symbol: S.

Production rules: $S \to 00\,S,\ S \to 01\,S,\ S \to 10\,S,\ S \to 11\,S,\ S \to E,\ E \to 0,\ E \to 1$

This is a regular grammar.

(b) Terminal symbols: The null string, 0, and 1.

Nonterminal symbols: S, A, B, C

Starting symbol: S

Production rules: $S \to 0\,A, S \to 1\,A, \mathrm{S} \to \lambda, A \to 0\,B, A \to 1\,B, A \to \lambda, B \to 0\,C, B \to 1\,C, B \to A, C \to 0, C \to 1, C \to \lambda$

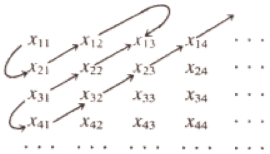
This is a regular grammar.

(c) See Exercise 3. This language is not regular.

7. If s is in A^* and L is recursive, we can answer the question “Is s in L^c?” by

negating the answer to “Is s in L?"

9. (a) List the elements of each set x_i in a sequence $x_{i\,1}, x_{i\,2}, x_{i\,3}, \ldots$.

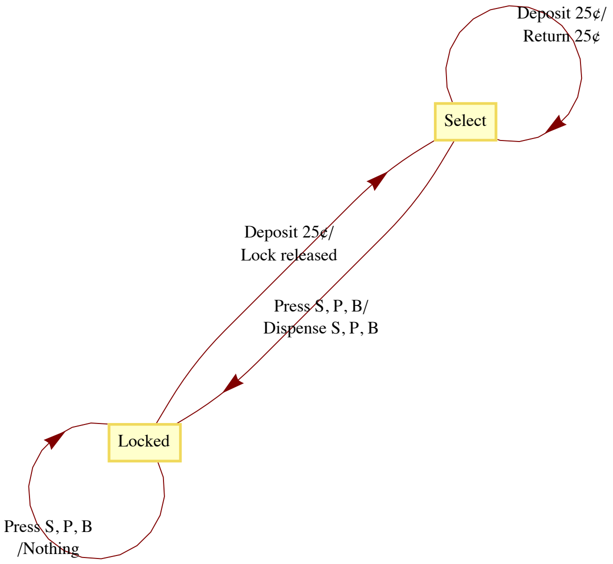


Then draw arrows as shown above and list the elements of the union in order established by this pattern: $x_{11}, x_{21}, x_{12}, x_{13}, x_{22}, x_{31}, x_{41}, x_{32}, x_{23}, x_{14}, x_{15}, \ldots$

(b) Each of the sets A^1 , A^2 , A^3 , … are countable and A^* is the union of these sets; hence A^* is countable.

Section 14.3

x	s	$Z(x, s)$	$t(x, s)$
Deposit 25 ¢	Locked	Nothing	Select
Deposit 25 ¢	Select	Return 25 ¢	Select
Press S	Locked	Nothing	Locked
Press S	Select	Dispense S	Locked
Press P	Locked	Nothing	Locked
Press P	Select	Dispense P	Locked
Press B	Locked	Nothing	Locked
Press B	Select	Dispense B	Locked



3. {000, 011, 101, 110, 111}

5. (a) Input:10110, Output: 11011 ⇒ 10110 is in position 27

Input: 00100, Output: 00111 ⇒ 00100 is in position 7

Input:11111, Output: 10101 ⇒ 11111 is in position 21

(b) Let $x = x_1\, x_2 \ldots x_n$ and recall that for $n \geq 1$, $G_{n+1} = \left(\begin{array}{c} 0\, G_n \\ 1\, {G_n}^r \end{array}\right)$, where ${G_n}^r$ is the reverse of G_n. To prove that the Gray Code Decoder always works, let $p\,(n)$ be the proposition "Starting in Copy state, x's output is the position of x in G_n; and starting in Complement state, x's output is the position of x in ${G_n}^r$." That p(1) is true is easy to verify for both possible values of x, 0 and 1. Now assume that for some $n \geq 1$, $p\,(n)$ is true and consider $x = x_1\, x_2 \ldots x_n\, x_{n+1}$.

If $x_1 = 0$,

$$\begin{aligned} x' s \text{ output} &= 0 \text{ followed by } (x_2 \ldots x_n\, x_{n+1})' s \text{ output starting in Copy} \\ &= 0 \text{ followed by } (x_2 \ldots x_n\, x_{n+1})' s \text{ position in } G_n \\ &= x' s \text{ position in } G_{n+1} \end{aligned}$$

If $x_1 = 1$,

$$\begin{aligned} x' s \text{ output} &= 1 \text{ followed by } (x_2 \ldots x_n\, x_{n+1})' s \text{ output starting in Complement} \\ &= 1 \text{ followed by } (x_2 \ldots x_n\, x_{n+1})' s \text{ position in } G_n{}^r \\ &= x' s \text{ position in } G_{n+1} \end{aligned}$$

Section 14.4

1.

Input String	a	b	c	aa	ab	ac
1	$(a, 1)$	$(a, 2)$	$(c, 3)$	$(a, 1)$	$(a, 2)$	$(c, 3)$
2	$(a, 2)$	$(a, 1)$	$(c, 3)$	$(a, 2)$	$(a, 1)$	$(c, 3)$
3	$(c, 3)$	$(c, 3)$	$(c, 3)$	$(c, 3)$	$(c, 3)$	$(c, 3)$

Input String	ba	bb	bc	ca	cb	cc
1	$(a, 2)$	$(a, 1)$	$(c, 3)$	$(c, 3)$	$(c, 3)$	$(c, 3)$
2	$(a, 1)$	$(a, 2)$	$(c, 3)$	$(c, 3)$	$(c, 3)$	$(c, 3)$
3	$(c, 3)$	$(c, 3)$	$(c, 3)$	$(c, 3)$	$(c, 3)$	$(c, 3)$

We can see that $T_a\, T_a = T_{aa} = T_a$, $T_a\, T_b = T_{ab} = T_b$, etc. Therefore, we have the following monoid:

	T_a	T_b	T_b
T_a	T_a	T_b	T_c
T_b	T_b	T_a	T_c
T_c	T_c	T_c	T_c

Notice that T_a is the identity of this monoid.

(b)

Input String	1	2	11	12	21	22
A	C	B	A	D	D	A
B	D	A	B	C	C	B
C	A	D	C	B	B	C
D	B	C	D	A	A	D

Input String	111	112	121	122	211	212	221	222
A	C	B	B	C	B	C	C	B
B	D	A	A	D	A	D	D	A
C	B	C	C	B	C	B	B	C
D	B	C	C	B	C	B	B	C

We have the following monoid:

	T_1	T_2	T_{11}	T_{12}
T_1	T_{11}	T_{12}	T_1	T_2
T_2	T_b	T_{11}	T_2	T_1
T_{11}	T_1	T_2	T_{11}	T_{12}
T_{12}	T_2	T_1	T_{12}	T_{11}

Notice that T_{11} is the identity of this monoid.

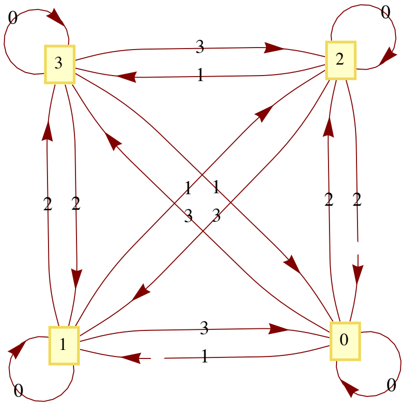
3. Yes, just consider the unit time delay machine of Figure 14.4.2. Its monoid is described by the table at the end of Section 14.4 where the T_λ row and T_λ column are omitted. Next consider the machine in Figure 14.5.3. The monoid of this machine is:

	T_λ	T_0	T_1	T_{00}	T_{01}	T_{10}	T_{11}
T_λ	T_λ	T_0	T_1	T_{00}	T_{01}	T_{10}	T_{11}
T_0	T_0	T_{00}	T_{01}	T_{00}	T_{01}	T_{10}	T_{11}
T_1	T_1	T_{10}	T_{11}	T_{00}	T_{01}	T_{10}	T_{11}
T_{00}	T_{00}	T_{00}	T_{01}	T_{00}	T_{01}	T_{10}	T_{11}
T_{01}	T_{01}	T_{10}	T_{11}	T_{00}	T_{01}	T_{10}	T_{11}
T_{10}	T_{10}	T_{00}	T_{01}	T_{00}	T_{01}	T_{10}	T_{11}
T_{11}	T_{11}	T_{10}	T_{11}	T_{00}	T_{01}	T_{10}	T_{11}

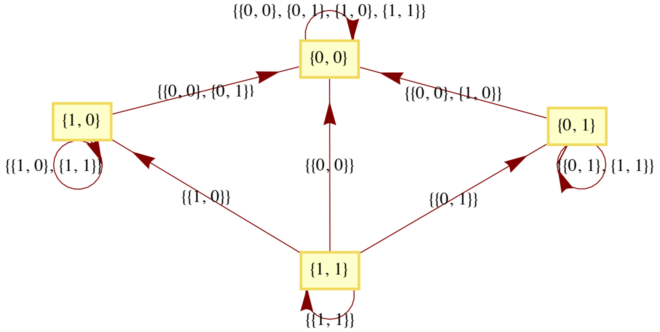
Hence both of these machines have the same monoid, however, their transition diagrams are nonisomorphic since the first has two vertices and the second has seven.

Section 14.5

1. (a)



(b)



Supplementary Exercises—Chapter 14

1. Let $f,\ g,\ h \in M$, and $a \in B$.

$$\begin{aligned}((f*g)*h)(a) &= (f*g)(a) \bigwedge h(a)\\ &= (f(a) \bigwedge g(a)) \bigwedge h(a)\\ &= f(a) \bigwedge (g(a) \bigwedge h(a))\\ &= f(a) \bigwedge (g*h)(a)\\ &= (f*(g*h))(a)\end{aligned}$$

Therefore $(f * g) * h = f * (g * h) \Rightarrow *$ is associative.

The identity for $*$ is the function $u \in M$ where $u(a) = 1$ = the "one" of B. If $a \in B$

$$(f*u)(a) = f(a) \bigwedge u(a) = f(a) \bigwedge 1 = f(a)$$

Therefore $f * u - f$. Similarly $u * f = f$.

There are $2^2 = 4$ functions in M for $B = B_2$. These four functions are named in the text (see Figure 14.1.1). The table for $*$ is

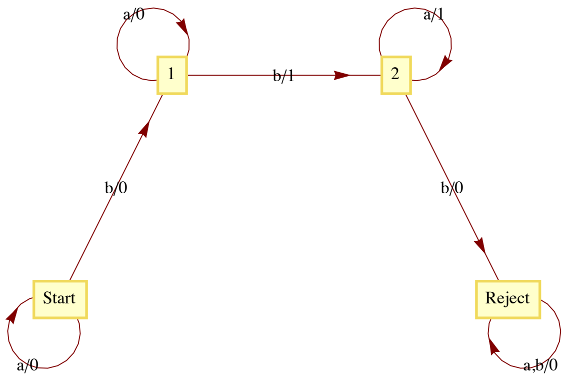
	z	i	t	u
z	z	z	z	z
i	z	i	z	i
t	z	z	t	t
u	z	u	t	u

3. $\{a,\ bb,\ bbb,\ bbbb,\ \ldots\}$

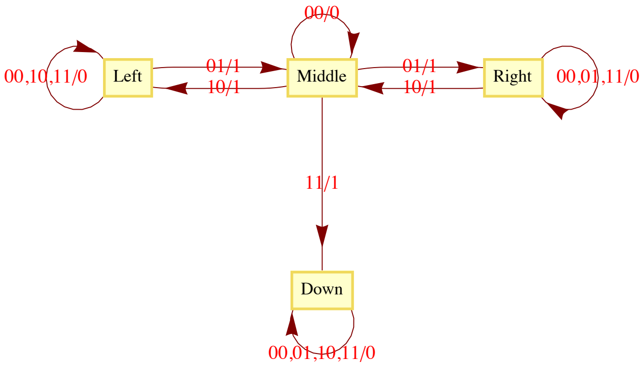
5. S = start symbol. Nonterminals = $\{S,\ B_0\ ,\ B_1,\ B_2\}$

$$
\begin{array}{llll}
S \to B_0 & B_0 -> a\,B_0 & B_0 \to b\,B_1 & \\
 & B_1 \to a\,B_1 & B_1 \to b\,B_2 & B_1 \to b \\
 & B_2 \ \to a\,B_2 & B_2 \to a &
\end{array}
$$

7.

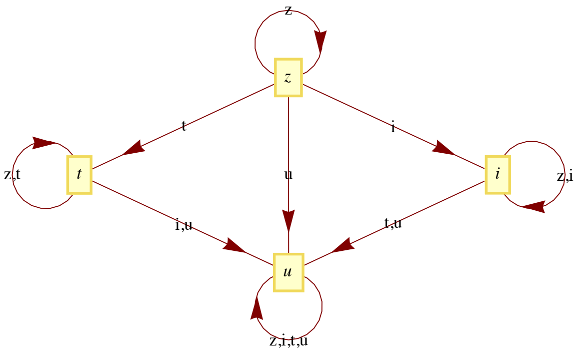


9. (a)



(b) The possible output sequences are 100, 010, 001, and 111. Note: Output for $t\ =\ 3$ is determined by the next state, $s(4)$). If $s\,(4)\ =\ s\,(3)$, output at $t\ =\ 3$ is 0, while if $s(4)\ \neq\ s(3)$, output at $t = 3$ is 1.

11.



CHAPTER 15

Section 15.1

1. The only other generator is -1.

3. If $|G| = m$, $m > 2$, and $G = \langle a \rangle$, then $a, a^2, \ldots, a^{m-1}$, $a^m = e$ are distinct elements of G. Furthermore, $a^{-1} = a^{m-1} \neq a$, If $1 \leq k \leq m$, a^{-1} generates a^k:

$$\begin{aligned}(a^{-1})^{m-k} &= (a^{m-1})^{m-k} = a^{m^2-m-m\,k+k} \\ &= (a^m)^{m-k-1} * a^k = e * a^k = a^k\end{aligned}$$

Similarly, if G is infinite and $G = \langle a \rangle$, then a^{-1} generates G.

5. (a) No. Assume that $q \in \mathbb{Q}$ generates $\mathbb{Q}$. Then $\langle q \rangle = \{n\,q : n \in \mathbb{Z}\}$. But this gives us at most integer multiples of q, not every element in $\mathbb{Q}$.

(b) No. Similar reasoning to part a.

(c) Yes. 6 is a generator of $6\,\mathbb{Z}$.

(d) No.

(e) Yes, $(1, 1, 1)$ is a generator of the group.

7. Theorem 15.1.4 implies that a generates $\mathbb{Z}_n$ if and only if the greatest common divisor of n and a is 1 (i. e., n and a are relatively prime). Therefore the list of generators of $\mathbb{Z}_n$ are the integers in $\mathbb{Z}_n$ that are relatively prime to n. The generators of $\mathbb{Z}_{25}$ are all of the nonzero elements except 5, 10, 15, and 20. The generators of $\mathbb{Z}_{256}$ are the odd integers in $\mathbb{Z}_{256}$ since 256 is 2^8. *Mathematica* expression to generate these sets are

```
Select[Range[0, 24], Function[a, GCD[25, a] == 1]]
```

```
{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24}
```

```
Select[Range[0, 255], Function[a, GCD[256, a] == 1]]
```

```
{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65,
  67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, 91, 93, 95, 97, 99, 101, 103, 105, 107, 109, 111, 113, 115, 117, 119,
  121, 123, 125, 127, 129, 131, 133, 135, 137, 139, 141, 143, 145, 147, 149, 151, 153, 155, 157, 159, 161, 163, 165,
  167, 169, 171, 173, 175, 177, 179, 181, 183, 185, 187, 189, 191, 193, 195, 197, 199, 201, 203, 205, 207, 209, 211,
  213, 215, 217, 219, 221, 223, 225, 227, 229, 231, 233, 235, 237, 239, 241, 243, 245, 247, 249, 251, 253, 255}
```

9. (a) $\theta : \mathbb{Z}_{77} \to \mathbb{Z}_7 \times \mathbb{Z}_{11}$

$$\begin{array}{ccc} 21 & \rightarrow & (0, 10) \\ 5 & \rightarrow & (5, 5) \\ 7 & \rightarrow & (0, 7) \\ 15 & \rightarrow & \underline{(1, 4)} \\ \text{sum} = 48 & \leftarrow & (6, 4) = \text{sum} \end{array}$$

The final sum, 48, is obtained by using the facts that $\theta^{-1}(1, 0) = 22$ and $\theta^{-1}(0, 1) = 56$

$$\begin{aligned}\theta^{-1}(6, 4) &= 6 \times_{77} \theta^{-1}(1, 0) + 4 \times_{77} \theta^{-1}(0, 1) \\ &= 6 \times_{77} 22 +_{77} 4 \times_{77} 56 \\ &= 55 +_{77} 70 \\ &= 48\end{aligned}$$

(b) Using the same isomorphism:

$$\begin{array}{ccc} 25 & \rightarrow & (4, 3) \\ 26 & \rightarrow & (5, 4) \\ 40 & \rightarrow & (5, 7) \\ & & \text{sum} = (0, 3) \end{array}$$

$$\begin{aligned}\theta^{-1}(0, 3) &= 3 \times_{77} \theta^{-1}(0, 1) \\ &= 3 \times_{77} 56 \\ &= 14\end{aligned}$$

The actual sum is 91. Our result is incorrect, since 91 is not in $\mathbb{Z}_{77}$. Notice that 91 and 14 differ by 77. Any error that we get using this technique will be a multiple of 77.

Section 15.2

1. Call the subsets A and B respectively. If we choose $0 \in A$ and $5 \in B$ we get $0 +_{10} 5 = 5 \in B$. On the other hand, if we choose $3 \in A$ and $8 \in B$, we get $3 +_{10} 8 = 1 \in A$. Therefore, the induced operation is not well defined on $\{A, B\}$.

3. (a) The four distinct cosets in G/H are

$$H = \{(0, 0), (2, 0)\}$$

$$(1, 0) + H = \{(1, 0), (3, 0)\}$$

$$(0, 1) + H = \{(0, 1), (2, 1)\},$$

and $(1, 1) + H = \{(1, 1), (3, 1)\}$

None of these cosets generates G/H; therefore G/H is not cyclic. Hence G/H must be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(b) The factor group is isomorphic to $[\mathbb{R}; +]$. Each coset of $\mathbb{R}$ is a line in the complex plane that is parallel to the x-axis: $\tau : \mathbb{C}/\mathbb{R} \to \mathbb{R}$, where $T(\{a + b i \mid a \in \mathbb{R}\}) = b$ is an isomorphism.

(c) $\langle 8 \rangle = \{0, 4, 8, 12, 16\} \Rightarrow |\mathbb{Z}_{20}/\langle 8 \rangle| = 4$.

The four cosets are: $\overline{0}, \overline{1}, \overline{2}$, and $\overline{3}$. 1 generates all four cosets. The factor group is isomorphic to $[\mathbb{Z}_4, +_4]$ because $\overline{1}$ generates it.

5.
$$\begin{aligned} a \in bH &\Leftrightarrow a = b * h \text{ for some } h \in H \\ &\Leftrightarrow b^{-1} * a = h \text{ for some } h \in H \\ &\Leftrightarrow b^{-1} * a \in H \end{aligned}$$

Section 15.3

1. (a) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$

(e) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$ (f) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$

(g) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

3. Yes and no, respectively

5. $D_4 = \{i, r, r^2, r^3, f_1 f_2, f_3, f_4\}$

Where i is the identity function, $r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, and

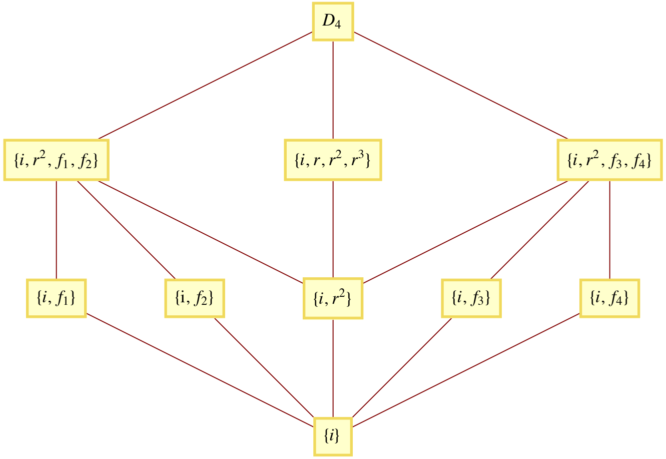
$$f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \; f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \; f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

The operation table for the group is

$\circ$	i	r	r^2	r^3	f_1	f_2	f_3	f_4
i	i	r	r^2	r^3	f_1	f_2	f_3	f_4
r	r	r^2	r^3	i	f_4	f_3	f_1	f_2
r^2	r^2	r^3	i	r	f_2	f_1	f_4	f_3
r^3	r^3	i	r	r^2	f_3	f_4	f_2	f_1
f_1	f_1	f_3	f_2	f_4	i	r^2	□	r^3
f_2	f_2	f_4	f_1	f_3	r^2	i	r^3	r
f_3	f_3	f_2	f_4	f_1	r^3	r	i	r^2
f_4	f_4	f_1	f_3	f_2	r	r^3	r^2	i

A lattice diagram of its subgroups is



All proper subgroups are cyclic except $\{i, r^2, f_1, f_2\}$ and $\{i, r^2, f_3, f_4\}$. Each 2-element subgroup is isomorphic to $\mathbb{Z}_2$; $\{i, r, r^2, r^3\}$ is isomorphic to $\mathbb{Z}_4$; and $\{i, r^2, f_1, f_2\}$ and $\{i, r^2, f_3, f_4\}$ are isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

7. One solution is to cite Exercise 3 at the end of Section 11.3. It can be directly applied to this problem. An induction proof of the problem at hand would be almost identical to the proof of the more general statement.

$$\begin{aligned}(t_1 t_2 \cdots t_r)^{-1} &= t_r^{-1} \cdots t_2^{-1} t_1^{-1} && \text{by Exercies 3 of Section 11.3}\\ &= t_r \cdots t_2 t_1 && \text{since each transposition inverts itself. } \blacksquare\end{aligned}$$

9. Part I: That $|S_k| = k!$ follows from Exercise 3 of Section 7.3.

Part II: Let f be the function defined on $\{1, 2, ..., n\}$ by $f(1) = 2$, $f(2) = 3$, $f(3) = 1$, and $f(j) = j$ for $4 \leq j \leq n$; and let g be defined by $g(1) = 1$, $g(2) = 3$, $g(3) = 2$, and $g(j) = j$ for $4 \leq j \leq n$. Note that f and g are elements of S_n. Next, $(f \circ g)(1) = f(g(1)) = f(1) = 2$, while $(g \circ f)(1) = g(f(1)) = g(2) = 3$, hence $f \circ g \neq g \circ f$ and S_n is non-abelian for any $n \geq 3$.

11. (a) Both groups are non-abelian and of order 6; so they must be isomorphic, since only one such group exists up to isomorphism. The function $\theta : S_3 \to R_3$ defined by

$$\begin{array}{ll}\theta(i) = I & \theta(f_1) = F_1\\ \theta(r_1) = R_1 & \theta(f_2) = F_2\\ \theta(r_2) = R_2 & \theta(f_3) = F_3\end{array}$$

is an isomorphism,

(b) Recall that since every function is a relation, it is natural to translate functions to Boolean matrices. Suppose that $f \in S_n$. We will define its image, $\theta(f)$, by

$$\theta(f)_{kj} = 1 \quad \Leftrightarrow \quad f(j) = k$$

That θ is a bijection follows from the existence of θ^{-1}. If A is a rook matrix,

$$\begin{aligned}\theta^{-1}(A)(j) = k &\Leftrightarrow \text{The 1 in column } j \text{ of } A \text{ appears in row } k\\ &\Leftrightarrow A_{kj} = 1\end{aligned}$$

For $f, g \in S_n$,

$$\begin{aligned}\theta(f \circ g)_{kj} = 1 &\Leftrightarrow (f \circ g)(j) = k\\ &\Leftrightarrow \exists\, l \text{ such that } g(j) = l \text{ and } f(l) = k\\ &\Leftrightarrow \exists\, l \text{ such that } \theta(g)_{lj} = 1 \text{ and } \theta(f)_{kl} = 1\\ &\Leftrightarrow (\theta(f)\,\theta(g))_{kj} = 1\end{aligned}$$

Therefore, θ is an isomorphism. $\blacksquare$

Section 15.4

1. (a) Yes, the kernel is $\{1, -1\}$

(b) No, since $\theta_2(2 +_5 4) = \theta_2(1) = 1$, but $\theta_2(2) +_2 \theta_2(4) = 0 +_2 0 = 0$

(c) Yes, the kernel is $\{(a, -a) \mid a \in \mathbb{R}\}$

(d) No

3. $\langle r\rangle = \{i, r, r^2, r^3\}$ is a normal subgroup of D_4. To see you could use the table given in the solution of Exercise 5 of Section 15.3 and verify that $a^{-1}\, h\, a \in \langle r\rangle$ for all $a \in D_4$ and $h \in \langle r\rangle$. A more efficient approach is to prove the general theorem that if H is a subgroup G with exactly two distinct left cosets, than H is normal.

$\langle f_1\rangle$ is not a normal subgroup of D_4. $\langle f_1\rangle = \{i, f_1\}$ and if we choose $a = r$ and $h = f_1$ then $a^{-1}\, h\, a = r^3\, f_1\, r = f_2 \notin \langle f_1\rangle$

5. $(\beta \circ \alpha)\,(a_1, a_2, a_3) = 0$ and so $\beta \circ \alpha$ is the trivial homomorphism, but a homomorphism nevertheless.

7. Let $x,\ y \in G$.

$$\begin{aligned} q(x * y) &= (x * y)^2 \\ &= x * y * x * y \\ &= x * x * y * y \quad \text{since } G \text{ is abelian} \\ &= x^2 * y^2 \\ &= q(x) * q(y) \end{aligned}$$

Hence, q is a homomorphism.

In order for q to be an isomorphism, it must be the case that no element other than the identity is its own inverse.

$$\begin{aligned} x \in \text{Ker}\,(q) &\Leftrightarrow q\,(x) = e \\ &\Leftrightarrow x * x = e \\ &\Leftrightarrow x^{-1} = x \end{aligned}$$

9. Proof: Recall: The inverse image of H' under θ is

$$\theta^{-1}(H') = \{g \in G \mid \theta(g) \in H'\}$$

Closure: Let $g_1\ g_2 \in \theta^{-1}(H')$, then $\theta(g_1),\ \theta(g_2) \in H'$. Since H' is a subgroup of G',

$$\theta(g_1) \diamond \theta(g_2) = \theta(g_1 * g_2) \Rightarrow g_1 * g_2 \in \theta^{-1}(H')$$

Identity: By Theorem 15.4.2(a), $e \in \theta^{-1}(H')$.

Inverse: Let $a \in \theta^{-1}(H')$. Then $\theta(a) \in H'$ and by Theorem 15.4.2(b), $\theta(a)^{-1} = \theta(a^{-1}) \in H'$ and so $a^{-1} \in \theta^{-1}(H')$.

Section 15.5

1. (a) Error detected, since an odd number of Is was received; ask for retransmission.

(b) No error detected; accept this block.

(c) No error detected; accept this block.

3. (a) Syndrome = $(1,\ 0,\ 1)$. Corrected message = $(1,\ 1,\ 0)$.

(b) Syndrome = $(1,\ 1,\ 0)$. Corrected message = $(0,\ 0,\ 1)$.

(c) Syndrome $(0, 0, 0)$. Corrected message = received message.
= $(0,\ 1,\ 1)$

(d) Syndrome = $(1,\ 1,\ 0)$. Corrected message = $(1,\ 0,\ 0)$.

(e) Syndrome = $(1,\ 1,\ 1)$. This syndrome occurs only if two bits have been switched. No reliable correction is possible.

5. Let G be the 9×10 matrix obtained by augmenting the 9×9 identity matrix with a column of ones. The function $e : \mathbb{Z}_2{}^9 \to \mathbb{Z}_2{}^{10}$ defined by $e\,(a) = a\,G$ will allow us to detect single errors, since $e\,(a)$ will always have an even number of ones.

Supplementary Exercises—Chapter 15

1. Theorem 15.1.3 guarantees that all subgroups of any cyclic group can be determined by finding all cyclic subgroups. We can find all cyclic subgroups of noncyclic groups but there may be other subgroups.

3. First, write 120 as a product of powers of distinct primes: $120 = 2^3 \cdot 3 \cdot 5$. The Chinese Remainder Theorem states that $\theta : \mathbb{Z}_{120} \to \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ defined by $\theta(k) = (k \bmod 8,\ k \bmod 3,\ k \bmod 5)$ is an isomorphism. In particular, $\theta(74) = (2, 2, 4)$ and $\theta(85) = (5, 1, 0)$. Therefore,

$$\begin{aligned}\theta(74 +_{120} 85) &= \theta(74) + \theta(85)\\ &= (2, 2, 4) + (5, 1, 0)\\ &= (7, 0, 4)\end{aligned}$$

Since $\theta(105) = (1, 0, 0)$, and $\theta(96) = (0, 0, 1)$, we can compute

$$\begin{aligned}\theta^{-1}(7, 0, 4) &= 7 \times_{120} 105 +_{120} 4 \times_{120} 96 .\\ &= 39\end{aligned}$$

5. $H = 0 + H = \{0, 4, 8\} = 4 + H = 8 + H$

$1 + H = \{1, 5, 9\} = 5 + H = 9 + H$

$2 + H = \{2, 6, 10\} = 6 + H = 10 + H$

$3 + H = \{3, 7, 11\} = 7 + H = 11 + H$

The operation table for this factor group is the same as that of $[\mathbb{Z}_4, +_4]$ with k replaced with $k + H$.

7. (a) $|\mathbb{Z}_8| = 8$ and $|\langle 2\rangle| = 4$, therefore there are 2 distinct left cosets, and they are:

$0 + \langle 2\rangle = \{0, 2, 4, 6\} = 2 + \langle 2\rangle = 4 + \langle 2\rangle = 6 + \langle 2\rangle$

$1 + \langle 2\rangle = \{1, 3, 5, 7\} = 3 + \langle 2\rangle = 5 + \langle 2\rangle = 7 + \langle 2\rangle$

(b) $|\mathbb{Z}_{12}| = 12$ and $|\langle 2\rangle| = 6$, therefore there are 2 distinct left cosets and they are:

$0 + \langle 2\rangle = \{(), 2, 4, 6, 8, 10\} = 2 + \langle 2\rangle = 4 + \langle 2\rangle - 6 + \langle 2\rangle = 8 + \langle 2\rangle = 10 + \langle 2\rangle$

and $1 + \langle 2\rangle = \{1, 3, 5, 7, 9, 11\} = 3 + \langle 2\rangle = 5 + \langle 2\rangle = 7 + \langle 2\rangle = 9 + \langle 2\rangle = 11 + \langle 2\rangle$

(c) Since both groups are of order 2 and there is only one group of order 2 up to isomorphism, they are isomorphic. A simpler group is $\mathbb{Z}_2$.

7. Assume f is even, $f = t_1 \circ t_2 \circ \cdots \circ t_{2r}$ for some r, where each t_i is a transposition. Hence

$f^{-1} = (t_1 \circ t_2 \circ \cdots \circ t_{2r})^{-1} = t_{2r} \circ \cdots \circ t_2 \circ t_1$ by Exercise 11 of Section 15.3.

Since the alternative, that f is odd, leads to f^{-1} being odd, f is even if and only if f^{-1} is even.

11. (a) *This following is the "standard definition" of a Boolean algebra homomorphism.*
$f : B_1 \to B_2$ is a Boolean algebra homomorphism if and only if for all $a, b, \in B_1$.

(1) $f(a \bigwedge b) = f(a) \bigwedge f(b)$

(2) $f(a \bigvee b) = f(a) \bigvee f(b)$

(3) $f(\overline{a}) = \overline{f(a)}$

(b) (i) $$\begin{aligned}f(0) &= f(a \wedge \overline{a})\\ &= f(a) \bigwedge f(\bar{a})\\ &= f(a) \bigwedge \overline{f(a)}\\ &= 0\end{aligned}$$

and

$$\begin{aligned}f(1) &= f(a \vee \overline{a})\\ &= f(a) \bigvee f(\bar{a})\\ &= f(a) \bigvee \overline{f(a)}\\ &= 1\end{aligned}$$

Note : The 0 and 1 of B_1 may be different than those of B_2.

(ii) $a \leq b \Rightarrow a = a \bigwedge b$ by Supplementary Exercise 4 of Chapter 13
$\Rightarrow f(a) = f(a \bigwedge b) = f(a) \bigwedge f(b)$
$\Rightarrow f(a) \leq f(b)$ by the same exercise cited above.

(iii) See the solution to Exercise 15 of the Supplementary section of Chapter 13 for the definition of Boolean subalgebra. Part (i) of this exercise shows that $f(B_1)$ contains the 0 and 1 of B_2. The definition in part a shows that $f(a) \in f(B_1)$ has a complement, namely $f(\overline{a}) \in f(B_1)$, and also that $f(B_1)$ must be closed with respect to both $\wedge$ and $\vee$. For example, if $a, b \in B_1$, then $a \bigwedge b \in B_1$, and since $f(a) \bigwedge f(b) = f(a \bigwedge b)$, $f(a) \bigwedge f(h) \in f(B_1)$.

13 (a) $\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$

(b) $e(1111) = 1111111$ and $e(1001) = 1001001$

(c) (i) Syndrome = 101 => Error in second bit, since 101 is the second row of P.

Corrected message = 0000.

(ii) Syndrome = 000 => No error in transmission. Correct message is 1010.

(iii) Syndrome = 001 => Error in seventh bit, since 001 is the seventh row of P.

Corrected message = 1011. (Since the error was in a parity bit, the actual message is not corrected.)

(d) The most direct way of proving that all single errors can be corrected is to compute the syndromes of each of the seven possible one-bit errors. Since each of them produces a distinct syndrome (the rows of P), single errors can always be corrected.

CHAPTER 16

Section 16.1

1. All but rings c and e are commutative. All of the rings have a unity element. The number 1 is the unity for all of the rings except c and e. The unity for $M_{2\times 2}(\mathbb{R})$ is the two by two identity matrix; the unity for $M_{n\times n}(\mathbb{R})$ is the n by n identity matrix. The units are as follows:

(a) $\{1, -1\}$

(b) $\mathbb{C}^*$

(c) $\{A \mid |A| = \pm 1\}$

(d) $\mathbb{Q}^*$

(e) $\{A \mid A_{11} A_{22} - A_{12} A_{21} \neq 0\}$

(f) $\{1\}$

3. Hints: (a) Consider commutativity

(b) Solve $x^2 = 3x$ in both rings.

5. (a) We already know that $3\mathbb{Z}$ is a subgroup of the group $\mathbb{Z}$; so part 1 of Theorem 16.1.1 is satisfied. We need only show that part 2 of the theorem holds: Let $3m,\ 3n \in 3\mathbb{Z}$.

$(3m)(3n) = 3(3mn) \in 3\mathbb{Z}$, since $3mn \in \mathbb{Z}$. ■

(b) The proper subrings are $\{0, 2, 4, 6\}$ and $\{0, 4\}$; while $\{0\}$ and $\mathbb{Z}_8$ are improper subrings.

(c) The proper subrings are $\{00, 01\}$, $\{00, 10\}$, and $\{00, 11\}$: while $\{00\}$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are improper subrings.

7. (a) The left-hand side of the equation factors into the product $(x-2)(x-3)$. Since $\mathbb{Z}$ is an integral domain, $x = 2$ and $x = 3$ are the only possible solutions.

(b) Over $\mathbb{Z}_{12}$, 2, 3, 6, and 11 are solutions. Although the equation factors into $(x-2)(x-3)$, this product can be zero without making x either 2 or 3. For example. If $x = 6$ we get $(6-2) \times_{12} (6-3) = 4 \times_{12} 3 = 0$. Notice that 4 and 3 are divisors of zero.

9. Let R_1, R_2, and R_3 be any rings, then

(a) R_1 is isomorphic to R_1 and so "is isomorphic to" is a reflexive relation on rings,

(b) R_1 is isomorphic to R_2 $\Rightarrow R_2$ is isomorphic to R_1, and so "is isomorphic to" is a symmetric relation on rings,

(c) R_1 is isomorphic to R_2, and R_2 is isomorphic to R_3 implies that R_1 is isomorphic to R_3, and so "is isomorphic to" is a transitive relation on rings.

We haven't proven these properties here, just stated them. The combination of these observations implies that "is isomorphic to" is an equivalence relation on rings,

11. (a) Commutativity is clear from examination of a multiplication table for $\mathbb{Z}_2 \times \mathbb{Z}_3$. More generally, we could prove a theorem that the direct product of two or more commutative rings is commutative. $(1, 1)$ is the unity of $\mathbb{Z}_2 \times \mathbb{Z}_3$.

(b) $\{(m, n) \mid m = 0 \text{ or } n = 0,\ (m, n) \neq (0, 0)\}$

(c) Another example is $\mathbb{Z} \times \mathbb{Z}$. No, since by definition an integral domain D must contain the additive identity so we always have $(m, 0) \cdot (0, n) = (0, 0)$ in $D \times D$.

13. (a) $$\begin{aligned}(a+b)(c+d) &= (a+b)c+(a+b)d\\ &= ac+bc+ad+bd\end{aligned}$$

(b) $$\begin{aligned}(a+b)(a+b) &= aa+ba+ab+bb && \text{by part } a\\ &= aa+ab+ab+bb && \text{since } R \text{ is commutative}\\ &= a^2+2ab+b^2\end{aligned}$$

15. Hint: The set of units of a ring is a group under multiplication. Apply a theorem from a group theory.

17. Proof of Corollary to Theorem 6.1.4: Since p is a prime, all nonzero elements of $\mathbb{Z}_p$ are relatively prime to p. By Theorem 16.1.4 we are done.

Section 16.2

3. No, since $2^{-1} = 2$ in $\mathbb{Z}_3$, but $a^{-1} \neq a$ and $b^{-1} \neq b$ in F.

5. (a) 0 (over $\mathbb{Z}_2$), 1 (over $\mathbb{Z}_3$), 3 (over $\mathbb{Z}_5$)

(b) 2 (over $\mathbb{Z}_3$), 3 (over $\mathbb{Z}_5$)

(c) 2

7. (a) 0 and 1 (b) 1 (c) 1 (d) none

9. (c) The roots of $x^2 - 2 = 0$ are $\sqrt{2}$ and $-\sqrt{2}$. Both numbers can be expressed in the form $a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$: $\sqrt{2} = 0 + 1 \cdot \sqrt{1}$ and $-\sqrt{2} = 0 + -1 \cdot \sqrt{2}$.

(d) No, since $\pm\sqrt{3}$ cannot be expressed in the form $a + b\sqrt{2}$,$a, b \in \mathbb{Q}$. If there exist rational numbers a and b such that $\sqrt{3} = a + b\sqrt{2}$, then clearly $b \neq 0$ since $\sqrt{3}$ is irrational and $a \neq 0$ for that would imply that $\sqrt{3/2}$ is rational, which is false. If we square both sides, of the equation we will get a rational expression for $\sqrt{2}$ which is also false.

Section 16.3

1. (i) $f(x) + g(x) = 2 + 2x + x^2$, $f(x)g(x) = 1 + 2x + 2x^2 + x^3$

(ii) $f(x) + g(x) = x^2$, $f(x)g(x) = 1 + x^3$

(iii) $1 + 3x + 4x^2 + 3x^3 + x^4$

(iv) $1 + x + x^3 + x^4$

(v) $x^2 + x^3$

3. (a) If $a, b \in \mathbb{R}$, $a - b$ and ab are in $\mathbb{R}$ since $\mathbb{R}$ is a ring in its own right. Therefore, $\mathbb{R}$ is a subring of $\mathbb{R}[x]$. The proofs of parts b and c are similar.

5. (a) Reducible, $(x + 1)(x^2 + x + 1)$

(b) Reducible, $x(x^2 + x + 1)$

(c) Irreducible. If you could factor this polynomial, one factor would be either x or $x + 1$, which would give you a root of 0 or 1, respectively. By substitution of 0 and 1 into this polynomial, it clearly has no roots.

(d) Reducible, $(x + 1)^4$

7. We illustrate this property of polynomials by showing that it is not true for a nonprime polynomial in $\mathbb{Z}_2[x]$. Suppose that $p(x) = x^2 + 1$, which can be reduced to $(x + 1)^2$, $a(x) = x^2 + x$, and $b(x) = x^3 + x^2$. Since $a(x)b(x) = x^5 + x^3 = x^3(x^2 + 1)$, $p(x) \mid a(x)b(x)$. However, $p(x)$ is not a factor of either $a(x)$ or $b(x)$.

9. The only possible proper factors of $x^2 - 3$ are $\left(x - \sqrt{3}\right)$ and $\left(x + \sqrt{3}\right)$, which are not in $\mathbb{Q}[x]$ but are in $\mathbb{R}[x]$.

11. For $n \geq 0$, let $S(n)$ be the proposition: For all $g(x) \neq 0$ and $f(x)$ with $\deg f(x) = n$, there exist unique polynomials $q(x)$ and $r(x)$ such that $f(x) = g(x)q(x) + r(x)$, and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Basis: $S(0)$ is true, for if $f(x)$ has degree 0, it is a nonzero constant, $f(x) = c \neq 0$, and so either $f(x) = g(x) \cdot 0 + c$ if $g(x)$ is not a constant, or $f(x) = g(x)g(x)^{-1} + 0$ if $g(x)$ is also a constant.

Induction: Assume that for some $n \geq 0$, $S(k)$ is true for all $k \leq n$, If $f(x)$ has degree $n + 1$, then there are two cases to consider. If $\deg g(x) > n + 1$, $f(x) = g(x) \cdot 0 + f(x)$, and we are done. Otherwise, if $\deg g(x) = m \leq n + 1$, we perform long division as follows, where LDT's = various terms of lower degree than $n + 1$.

$$\begin{array}{r l}
 & \quad f_{n+1}\cdot g_m{}^{-1}\,x^{n+1-m} \\ \cline{2-2}
g_m\,x^m + \text{LDT's} & \big)\, f_{n+1}\,x^{n+1} + \text{LDT's} \\
 & \quad \underline{f_{n+1}\,x^{n+1} + \text{LDT's}} \\
 & \qquad\qquad h(x)
\end{array}$$

Therefore,

$$\begin{aligned} h(x) &= f(x) - (f_{n+1}\cdot g_m{}^{-1}\,x^{n+1-m})\,g(x) \;\Rightarrow \\ f(x) &= (f_{n+1}\cdot g_m{}^{-1}\,x^{n+1-m})\,g(x) + h(x) \end{aligned}$$

Since $\deg h(x)$ is less than $n+1$, we can apply the induction hypothesis:

$$h(x) = g(x)\,q(x) + r(x) \text{ with } \deg r(x) < \deg g(x).$$

Therefore,

$$f(x) = g(x)\,(f_{n+1}\cdot g_m{}^{-1}\,x^{n+1-m} + q(x)) + r(x) \text{ with } \deg r(x) < \deg g(x).$$

This establishes the existence of a quotient and remainder. The uniqueness of $q(x)$ and $r(x)$ as stated in the theorem is proven as follows: if $f(x)$ is also equal to $g(x)\,\overline{q}(x) + \overline{r}(x)$ with $\deg \overline{r}(x) < \deg g(x)$, then

$$g(x)\,q(x) + r(x) = g(x)\,\overline{q}(x) + \overline{r}(x) \Rightarrow g(x)\,(\overline{q}(x) - q(x)) = r(x) - \overline{r}(x)$$

Since $\deg r(x) - \overline{r}(x) < \deg g(x)$, the degree of both sides of the last equation is less than $\deg g(x)$. Therefore, it must be that $\overline{q}(x) - q(x) = 0$, or $q(x) = \overline{q}(x)$ And so $r(x) = \overline{r}(x)$. ■

Section 16.4

1. If $a_0 + a_1\sqrt{2} \in \mathbb{Q}\left[\sqrt{2}\right]$ is nonzero, then it has a multiplicative inverse:

$$\begin{aligned} \frac{1}{a_0 + a_1\sqrt{2}} &= \frac{1}{a_0 + a_1\sqrt{2}}\,\frac{a_0 - a_1\sqrt{2}}{a_0 - a_1\sqrt{2}} \\ &= \frac{a_0 - a_1\sqrt{2}}{a_0{}^2 - 2\,a_1{}^2} \\ &= \frac{a_0}{a_0{}^2 - 2\,a_1{}^2} - \frac{a_1}{a_0{}^2 - 2\,a_1{}^2}\sqrt{2} \end{aligned}$$

The denominator, $a_0{}^2 - 2\,a_1{}^2$, is nonzero since $\sqrt{2}$ is irrational. Since $\frac{a_0}{a_0{}^2 - 2\,a_1{}^2}$ and $\frac{-a_1}{a_0{}^2 - 2\,a_1{}^2}$ are both rational numbers, $a_0 + a_1\sqrt{2}$ is a unit of $\mathbb{Q}\left[\sqrt{2}\right]$. The field containing $\mathbb{Q}\left[\sqrt{2}\right]$ is denoted $\mathbb{Q}\left(\sqrt{2}\right)$ and so $\mathbb{Q}\left(\sqrt{2}\right) = \mathbb{Q}\left[\sqrt{2}\right]$

3. $x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$ has zeros $\pm\sqrt{2}$ and $\pm\sqrt{3}$. $\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$ contains the zeros $\pm\sqrt{2}$ but does not contain $\pm\sqrt{3}$, since neither are expressible in the form $a + b\sqrt{2}$. If we consider the set $\left\{c + d\sqrt{3} : c, d \in \mathbb{Q}\left(\sqrt{2}\right)\right\}$, then this field contains $\pm\sqrt{3}$ as well as $\pm\sqrt{2}$, an is denoted $\left(\mathbb{Q}\left(\sqrt{2}\right)\right)\left(\sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$. Taking into account the form of c and d in the description above, we can expand to

$$\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \left\{b_0 + b_1\sqrt{2} + b_2\sqrt{3} + b_3\sqrt{6} \;\middle|\; b_i \in \mathbb{Q}\right\}.$$

5. (a) $f(x) = x^3 + x + 1$ is reducible if and only if it has a factor of the form $x - a$. By Theorem 16.3.3, $x - a$ is a factor if and only if a is a zero. Neither 0 nor 1 is a zero of $f(x)$ over $\mathbb{Z}_2$.

(b) Since $f(x)$ is irreducible over $\mathbb{Z}_2$, all zeros of $f(x)$ must lie in an extension field of $\mathbb{Z}_2$. Let c be a zero of $f(x)$. $\mathbb{Z}_2(c)$ can be described several different ways. One way is to note that since $c \in \mathbb{Z}_2(c)$, $c^n \in \mathbb{Z}_2(c)$ for all n. Therefore, $\mathbb{Z}_2(c)$ includes $0, c, c^2, c^3, \ldots$. But $c^3 = c + 1$ since $f(c) = 0$. Furthermore, $c^4 = c^2 + c$, $c^5 = c^2 + c + 1$, $c^6 = c^2 + 1$, and $c^7 = 1$. Higher powers of c repeat preceding powers. Therefore,

$$\begin{aligned} \mathbb{Z}_2(c) &= \{0,\ 1,\ c,\ c^2,\ c+1,\ c^2+1,\ c^2+c+1,\ c^2+c\}. \\ &= \{a_0 + a_1 c + a_2 c^2 \mid a_i \in \mathbb{Z}_2\} \end{aligned}$$

The three zeros of $f(x)$ are c, c^2 and $c^2 + c$.

$$f(x) = (x + c)(x + c^2)(x + c^2 + c).$$

(c) Cite Theorem 16.2.4, part 3.

Section 16.5

3. Theorem 16.5.2 proves that not all nonzero elements in $F[[x]]$ are units.

7. (a) $b_0 = 1$

$b_1 = (-1)(2 \cdot 1) = -2$

$b_2 = (-1)(2 \cdot (-2) + 4 \cdot 1) = 0$

$b_3 = (-1)(2 \cdot 0 + 4 \cdot (-2) + 8 \cdot 1) = 0$

… (all others are zero)

Hence, $f(x)^{-1} = 1 - 2x$

(b) $$\begin{aligned} f(x) &= 1 + 2x + 2^2 x^2 + 2^3 x^3 + \cdots \\ &= (2x)^0 + (2x)^1 + (2x)^2 + (2x)^3 + \cdots \\ &= \frac{1}{1-2x} \end{aligned}$$

The last step follows from the formula for the sum of a geometric series.

9. (a) $$\begin{aligned} (x^4 - 2x^3 + x^2)^{-1} &= (x^2(x^2 - 2x + 1))^{-1} \\ &= x^{-2}(1 - 2x + x^2)^{-1} \\ &= x^{-2}\left(\sum_{k=0}^{\infty} (k+1) x^k\right) \text{ by Example 2 of 16.5} \\ &= \sum_{k=-2}^{\infty} (k+2) x^k \end{aligned}$$

Supplementary Exercises—Chapter 16

1. (a) This ring is not commutative.

$$\begin{aligned} (A+B)^2 &= (A+B) \cdot (A+B) \\ &= (A+B) \cdot A + (A+B) \cdot B \\ &= A \cdot A + B \cdot A + A \cdot B + B \cdot B \\ &= A^2 + B \cdot A + A \cdot B + B^2 \end{aligned}$$

(b) Yes

3. (a) By Theorem 16.1.1 show:

(1) $[D \ +]$ is a subgroup of the group $[M_{2\times 2}(\mathbb{R});\ +]$. We leave this to the reader.

(2) D is closed under multiplication. To prove this, let $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \in D$. Then,

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix} \in D$$

since $a\,c$ and $b\,d$ are real numbers and the product is in the form of a typical matrix in D.

(b) Since

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix} = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix},$$

D is commutative. The unity for D is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(c) The product of two nonzero matrices can be equal to zero. For example, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Therefore, D has divisors of zero and by Theorem 16.1.2 the cancellation law is not true in D.

5. (a) $2^4 = 16$

(b) The product cited in the solution to 3(c) above shows that $M_{2\times 2}(\mathbb{R})$ has divisors of zero. Therefore, the matrix polynomial $(x - I)(x + I)$ may have solutions other then $\pm I$. If fact you can verify that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ satisfy the given equation.

7. Use $T : A \to \mathbb{R}$ defined by $T\left(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\right) = a$

9. By substitution and the operation tables of Example 16.2.2,

$$\begin{aligned} a^2 + a + 1 &= b + a + 1 \\ &= 1 + 1 = 0 \end{aligned}$$

Therefore, a is a root. A similar calculation shows that b is a root. Substitution of 0 and 1 for x shows that they are not root.

11. By Theorem 16.3.3, $a \in \mathbb{Q}$ is a zero of $f(x)$ iff $(x - a)$ is a factor of $f(x)$, which also implies a must be a factor of 9. Hence, the only possible rational roots are: ±1, ±3, and ±9. We can verify that $(x - 3)$ is a divisor of $f(x)$ or that $x = 3$ is a zero of $f(x)$. Dividing $f(x)$ by $(x - 3)$ produces $q(x) = x^3 - 3x^2 + x - 3$, which has $x = 3$ as a rational root. Dividing $q(x)$ by $x - 3$ produces $x^2 + 1$. Hence, the complete factorization of $f(x)$ in $\mathbb{Q}[x]$ is $(x - 3)^2 (x^2 + 1)$.

13. $g(0) = 0, g(1) = 1,$

$$g(a) = a^3 + a^2 + a = 1 + b + a = 1 + 1 = 0, \text{and}$$

$$g(b) = b^3 + b^2 + b = 1 + a + b = 1 + 1 = 0.$$

Hence, 0, a, and b are zeros of $g(x)$ and the $g(x) = x(x - a)(x - b) = x(x + a)(x + b)$.

15. (a) Sum = (1, 0, 1), Product = (0, 1, 1, 1)

(b) Sum = (1, 0, 0, 0), Product = (0, 1, 1, 1, 0, 0, 1)

(c) Sum = (1, 1, 1, 0, 0), Product = (0, 0, 0, 0, 1, 1, 1, 0, 1)

(d) Sum = 010, Product = 11011

16. The encoding of a string of bits is based on polynomial division. Given a four bit message, we make the bits coefficients of a sixth degree polynomial, $b_3 x^3 + b_4 x^4 + b_5 x^5 + b_6 x^6$ which we can also express in $\mathbb{Z}_2{}^6$ as $(0, 0, 0, b_3, b_4, b_5, b_6)$, we divide this polynomial by $p(x) = 1 + x + x^3$ and add the remainder to the "message polynomial. The quotient is in the division is discarded. Thus, if the remainder, which must be a polynomial of degree less than 2, is $b_0 + b_1 x + b_2 x^2$, the encoded message is the string of bits $(b_0, b_1, b_2, b_3, b_4, b_5, b_6)$.

(a) Encode the following elements of $\mathbb{Z}_2{}^6$as described above.

(a) (0, 0, 0, 1, 1, 0, 1)

(b) (0, 0, 0, 1, 1, 1, 1)

(c) (0, 0, 0, 0, 0, 1, 0)

(b) Prove that the encoded message will always represent a polynomial with is evenly divisible by the polynomial $p(x)$ that is used to encode the message.

17. If the message polynomial is $m(x) = b_3 x^3 + b_4 x^4 + b_5 x^5 + b_6 x^6$ we divide by $p(x) = 1 + x + x^3$ and get a quotient and remainder: $m(x) = p(x) q(x) + r(x)$, where the degree of $r(x)$ is less than 3. We transmit $t(x) = m(x) + r(x) = m(x) + (m(x) - p(x) q(x)) = p(x) q(x)$ since $m(x) + m(x) = 0$. Now assume that the error x^k is added and we receive $p(x) q(x) + x^k$. Since x^k, $0 \leq k \leq 6$, is not a multiple of $p(x)$, the received polynomial is also not a multiple of $p(x)$. The following *Mathematica* calculation verifies this last claim.

```
({x^#, PolynomialRemainder[x^#, x^3 + x + 1, x, Modulus → 2]} & /@ Range[0, 6]) //
 Prepend[#, {"Monomial", "Remainder"}] &
```

$$\begin{pmatrix} \text{Monomial} & \text{Remainder} \\ 1 & 1 \\ x & x \\ x^2 & x^2 \\ x^3 & x + 1 \\ x^4 & x^2 + x \\ x^5 & x^2 + x + 1 \\ x^6 & x^2 + 1 \end{pmatrix}$$

19. (a) $b(x) = x^5 + x^4 + 1 = g(x)(x^2 + x + 1) + 0 \Rightarrow a = 111$

(b) $b(x) = x^5 + x^3 + x^2 + 1 = g(x) x^2 + 1$

$\Rightarrow$ error in the first bit of b

$\Rightarrow e(a) = 001\,101$

$\Rightarrow a = 001$

Getting a from $e(a)$ involves doing this calculation:

```
PolynomialQuotient[x^5 + x^3 + x^2, x^3 + x + 1, x, Modulus → 2]
```

x^2

(c) $b(x) = x^5 + x + 1 = g(x)(x^2+1) + x^2$
$\Rightarrow$ error in the third bit of b
$\Rightarrow e(a) = 111\,001$
$\Rightarrow a = 101$

```
PolynomialQuotient[x^5 + x^2 + x + 1, x^3 + x + 1, x, Modulus → 2]
```

$x^2 + 1$

(d) $b(x) = x^4 + x^3 + x + 1 = g(x)(x+1) + x^2 + x$
$\Rightarrow$ error in the fifth bit of b
$\Rightarrow e(a) = 110\,100$ (the string representation of $g(x)$)
$\Rightarrow a = 100$

21. (a) $g(x)$ is irreducible over $\mathbb{Z}_2$ since $g(0) = g(1) = 1$. Hence, g(x) does not split in $\mathbb{Z}_2$. Let β be a zero of $g(x)$, so that $\mathbb{Z}_2[\beta] = \{a + b\beta + c\beta^2 \mid a, b, c \in \mathbb{Z}_2\}$. This is a field of $2^3 = 8$ elements which, by Theorem 16.2.4, is isomorphic to GF(8).

23. $1/g(x) = f(x)$ of Example 16.5.2.

$$
\begin{array}{r l}
 & 1 + 2x + 3x^2 + 4x^3 + \cdots \\ \cline{2-2}
1 - 2x + x^2 & \big)\, 1 \\
 & 1 - 2x + 2x^2 \\
 & \quad \underline{2x - 4x^2 + 2x^3} \\
 & \qquad 3x^2 - 2x^3 \\
 & \qquad \underline{3x^2 - 6x^3 + 3x^4} \\
 & \qquad\qquad 4x^3 - 3x^4 \\
 & \qquad\qquad \underline{4x^3 - 8x^4 + 4x^5} \\
 & \qquad\qquad\qquad 5x^4 - 4x^5 \\
 & \qquad\qquad\qquad\qquad \ddots
\end{array}
$$

25. (a) $a_0 = a_1 = 1, a_2 = 2, a_3 = 3, a_4 = 5, \ldots.$, so

$$f(x) = 1 + x + 2x^2 + 3x^3 + 5x^4 + \cdots.$$

(b) $a_0 = a_1 = 1, a_2 = 0, a_3 = 1, a_4 = 1, a_5 = 0, \ldots.$

$$
\begin{aligned}
g(x) &= 1 + x + 0x^2 + x^3 + x^4 + 0x^5 + x^6 + x^7 + \cdots \\
&= (1+x) + x^3(1+x) + x^6(1+x) + \cdots \\
&= (1+x)(1 + x^3 + x^6 + \cdots) \\
&= \frac{(1+x)}{(1-x^3)}
\end{aligned}
$$