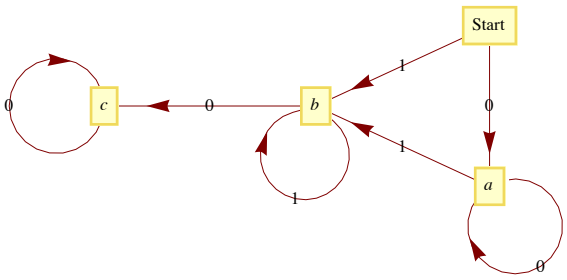
CHAPTER 9

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 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^1 defined by $vr^1 w$ if there is a path of length l from v to w? Yes, since vrw if and only if an edge, which is a path of length l, connects v to w.

Induction: Assume that $vr^k w$ if and only if there is a path of length k from v to w. We must show that $vr^{k+1} w$ if and only if there is a path of length $k + 1$ from v to w.

$vr^{k+1} w \Rightarrow vr^k y$ and yrw, 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, $vr^k y$ and $yrw \Rightarrow vr^{k+1} w$ ■

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 $n \geq 5$, 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 $e = e_1 + e_2 + 1$.

$$\begin{aligned} v + r - e + (v_1 + v_2) + (r_1 + r_2 - 1) - (e_1 + e_2 + 1) \\ &= (v_1 + r_1 - e_1) + (v_2 + r_2 - e_2) - 2 \\ &= 2 + 2 - 2 \\ &= 2 \qquad \blacksquare \end{aligned}$$

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 $n \geq 11$, 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

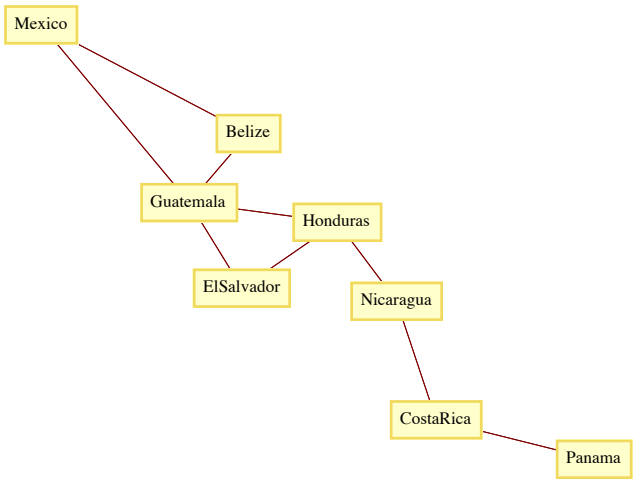
1. Graphs G_1 and G_2 are isomorphic. One isomorphism between them is $\{(a, e), (b, h), (c, f), (d, g)\}$. To see that G_3 is not isomorphic to the other two notice that k and j are not connected by an edge while in G_1 and G_2 every pair of vertices is connected.

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, $W \bigcup \{v\}$ 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)

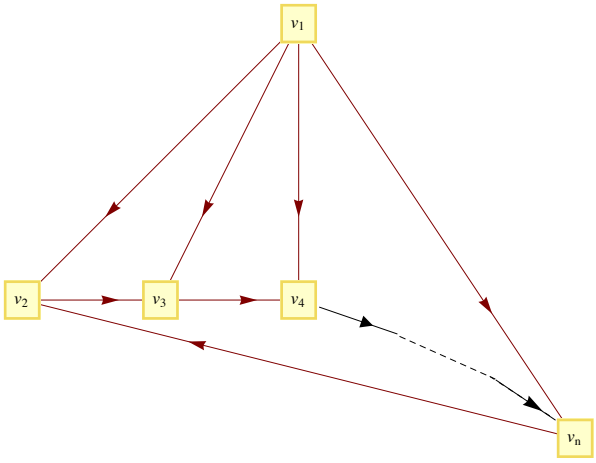
(c) This path could be a list of the countries that you would go through in your trip.

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* (source) $=$ *indeg* (sink) $= n - 1$

(c) Let $V = \{v_1, v_2, \ldots, v_n\}$. The following graph demonstrates that $p \bigwedge \neg q$ is possible. Similar graphs can be drawn for the other situations.



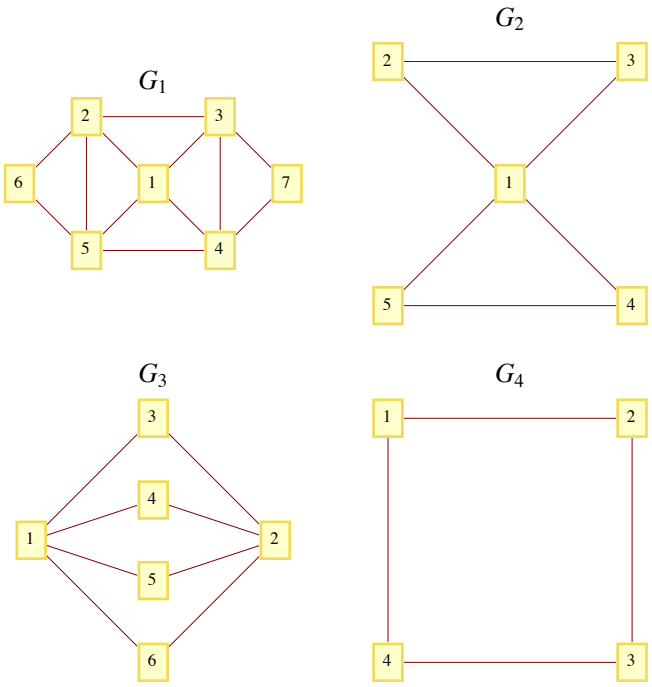
	k	1	2	3	4	5	6	7	8	9
	$V[k]$.name	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*
9.	$V[k]$.found	*T*	*T*	*T*	*T*	*T*	*T*	*T*	*T*	*T*
	$V[k]$.from	4	1	5	5	1	3	5	5	6
	depth set	3	1	2	2	1	3	2	2	4

11. G_1 is randomly Eulerian from no vertex, yet it is Eulerian.

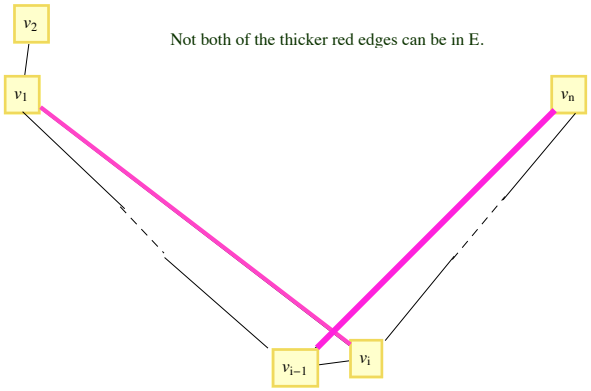
G_2 is randomly Eulerian from only vertex 1.

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 $(G, E \cup \{e\})$, there is a path in G that visits every vertex in the order $v_1, v_2, \ldots v_n$. Now for $2 \le i \le n$, 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.

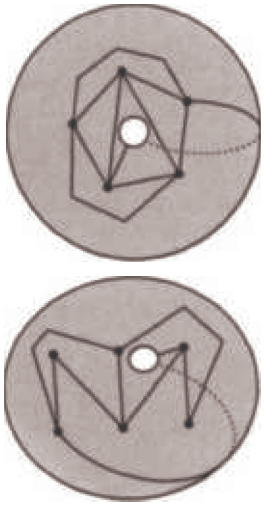
17.(a) (A, D, F, E, C, B, A)

(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

$$(n-2) + (n-3) + \cdots + 2 + 1 + 0 = \frac{1}{2\,(n-2)\,(n-1)} \text{ seconds}$$

$$\approx \frac{1}{2\,n^2} \text{ seconds, when } n \text{ is large.}$$

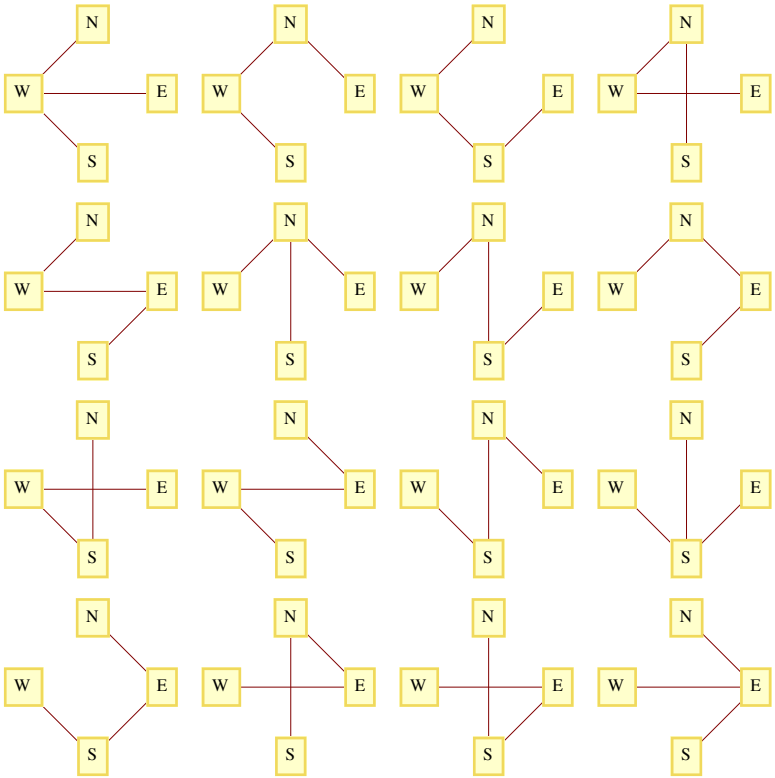
19.



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.

$2|E| = \sum_{v \in V} deg(v) \geq 2|V| - 1$

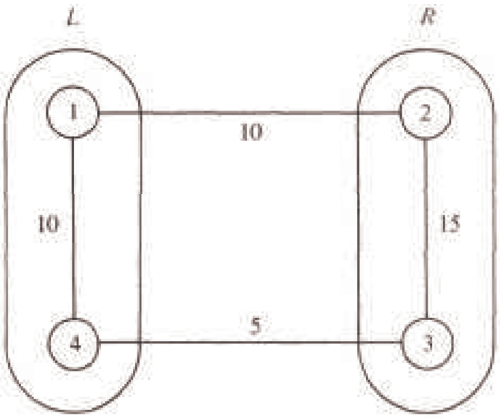
or $|E| \geq |V| - \frac{1}{2} \Rightarrow |E| \geq |V| \Rightarrow (V, E)$ is not a tree.

(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.



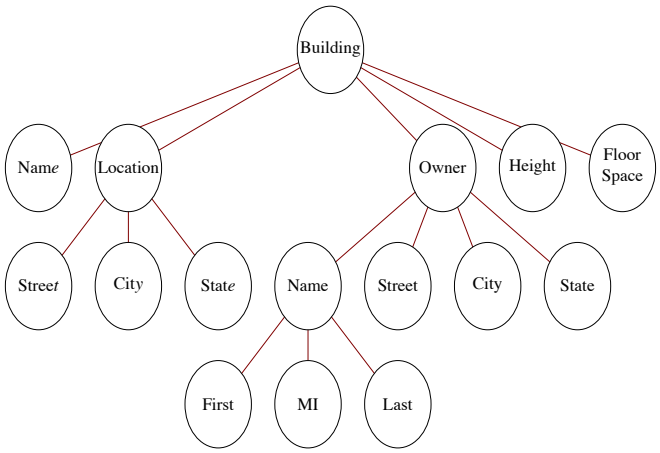
5, (a) Edges in one solution are:
{8, 7}, {8, 9}, {8, 13}, {7, 6}, {9, 4}, {13, 12}, {13, 14}, {6, 11}, {6, 1}, {1, 2}, {4, 3}, {4, 5} {14, 15}, and {5, 10}

(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.

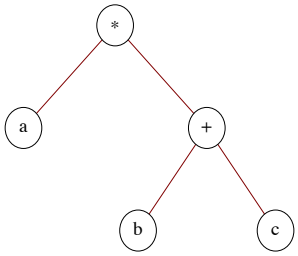
3.



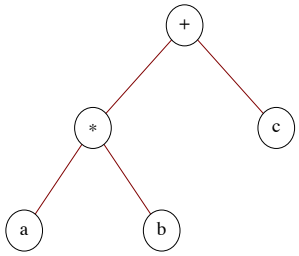
Section 10.4

1.

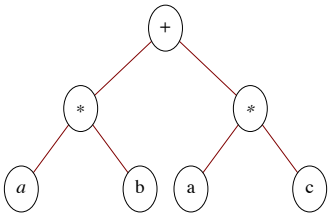
(a)



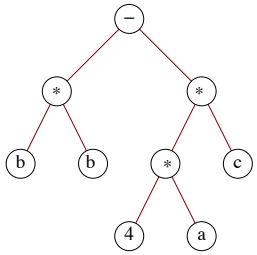
(b)



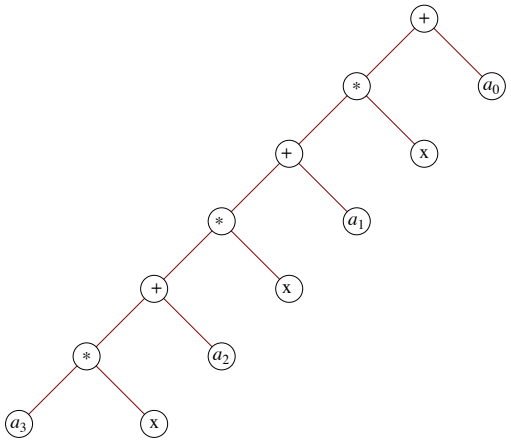
(c)



(d)



(e)

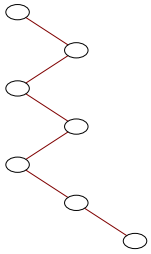


3.

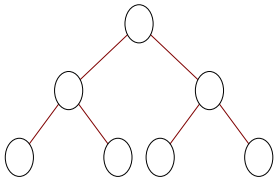
	Preorder	Inorder	Postorder
(a)	$\cdot a + bc$	$a \cdot b + c$	$abc + \cdot$
(b)	$+ \cdot abc$	$a \cdot b + c$	$ab \cdot c +$
(c)	$+ \cdot ab \cdot ac$	$a \cdot b + a \cdot c$	$ab \cdot ac \cdot +$

5.

(a)



(b)



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.

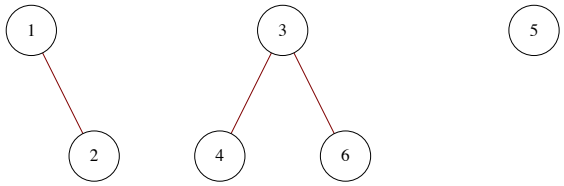
Supplementary Exercises—Chapter 10

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 : $v_1 = 2,\ v_2 = 1,\ v_3 = 3,\ v_4 = 4$

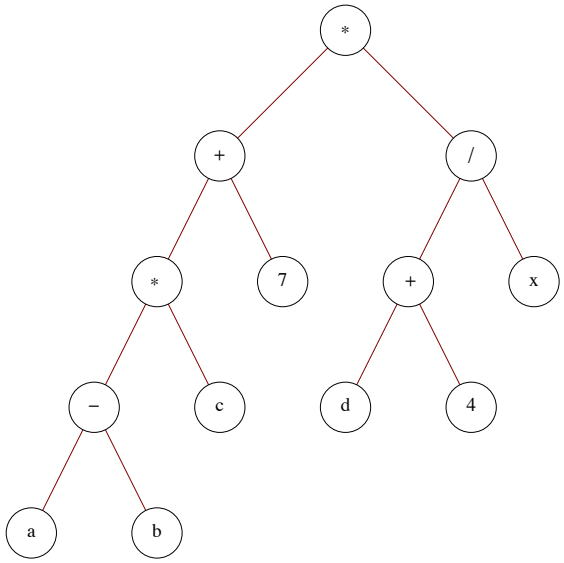
(b) Starting at either end of the chain label the first vertex $S(1) = 1$ and the $(k + 1)$ st vertex, $k \geq 1$, $S(k + 1) = S(k) + k$. The edge connecting the kth and $(k + 1)$ st vertex is the kth edge and since $(S(k + 1) - s(k)) = k$, the chain is graceful. The closed form expression for $S(k)$ 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.

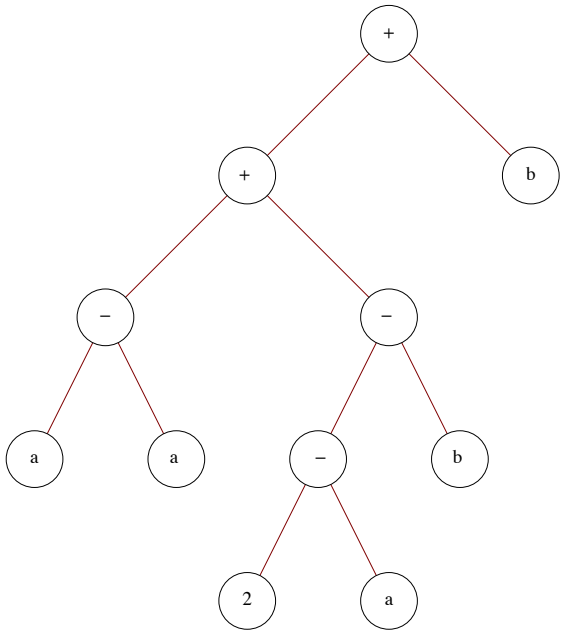


Vertices 4 and 6 have the same root in this tree; hence {4, 6} is rejected. {1, 5} and {2, 3} are the final edges that complete the minimal spanning tree. Notice that {4, 6} could have been the second edge selected. In that case, {3, 4} would be rejected.

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. $a, b \in A \cap B \Rightarrow a, b \in A$ by the definition of intersection
$\Rightarrow a * b \in A$ by the closure of A with respect to $*$

Similarly, $a, b \in A \cap B \Rightarrow a * b \in B$. Therefore, $a * b \in A \cap B$.

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 $M_{2\times2}(\mathbb{R})$, 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: $f(x) = f(y) \Rightarrow a * x = a * y$
$\Rightarrow x = y$ (by left cancellation)

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:

$$\begin{aligned}(a_1 * a_2 * \cdots * a_n * a_{n+1})^{-1} &= ((a_1 * a_2 * \cdots * a_n) * a_{n+1})^{-1} \text{ by the associative law}\\ &= {a_{n+1}}^{-1} * (a_1 * a_2 * \cdots * a_n)^{-1} \text{ by the basis}\\ &= {a_{n+1}}^{-1} * ({a_n}^{-1} * \cdots * {a_2}^{-1} * {a_1}^{-1}) \text{ by the induction hypothesis}\\ &= {a_{n+1}}^{-1} * {a_n}^{-1} * \cdots * {a_2}^{-1} * {a_1}^{-1} \text{ by the associative law } \blacksquare\end{aligned}$$

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.

$$\begin{aligned}(a^{n+1})^{-1} &= (a^n * a)^{-1} \text{ by the definition of exponentiation}\\ &= a^{-1} * (a^n)^{-1} \text{ by Theorem } 11.3\cdot 4\\ &= a^{-1} * (a^{-1})^n \text{ by the induction hypothesis}\\ &= (a^{-1})^{n+1} \text{ by the lemma}\end{aligned}$$

If n is negative, then $-n$ is positive and

$$\begin{aligned}a^{-n} &= \left(\left((a^{-1})^{-1}\right)^{-n}\right)\\ &= (a^{-1})^{-(-n)} \text{ since the property is true for positive numbers}\\ &= (a^{-1})^n\end{aligned}$$

(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

$$\begin{aligned}a^{n+(m+1)} &= a^{(n+m)+1} \text{ by the associativity of integer addition}\\ &= a^{n+m} * a^1 \text{ by the definition of exponentiation}\\ &= (a^n * a^m) * a^1 \text{ by the induction hypothesis}\\ &= a^n * (a^m * a^1) \text{ by associativity}\\ &= a^n * a^{m+1} \text{ by the definition of exponentiation}\end{aligned}$$

(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 $m > 0$,

$$\begin{aligned}(a^n)^{m+1} &= (a^n)^m * a^n \text{ definition of exponentiation}\\ &= a^{n\,m} * a^n \text{ by the induction hypothesis}\\ &= a^{n\,m+n} \text{ by part } (a) \text{ of this problem}\\ &= a^{n(m+1)}\end{aligned}$$

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 $m = 11q + r, 0 \le r < 11$.

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) $\langle 1\rangle = \langle 5\rangle = \langle 7\rangle = \langle 11\rangle = \mathbb{Z}_{12}$

   $\langle 2\rangle = \langle 10\rangle = \{2, 4, 6, 8, 10, 0\}$

   $\langle 3\rangle = \langle 9\rangle = \{3, 6, 9, 0\}$

   $\langle 4\rangle = \langle 8\rangle = \{4, 8, 0\}$

   $\langle 6\rangle = \{6, 0\}$

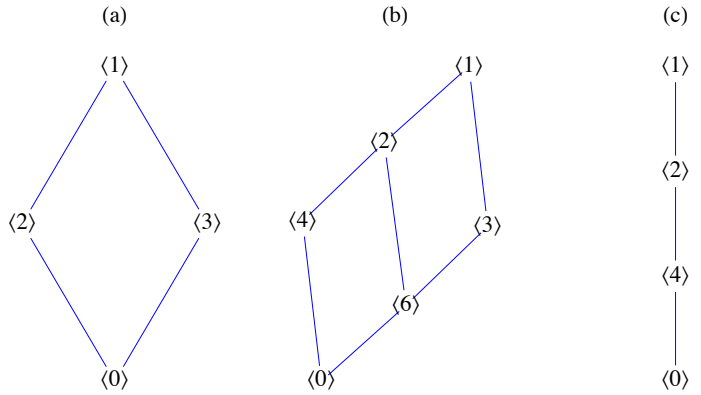
   $\langle 0\rangle = \{0\}$

   (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 $T : G \to \mathbb{Z}$ 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 $f \in S$,

$$f \circ f^{-1} = f^{-1} \circ f = i \quad \Rightarrow \quad f \text{ inverts } f^{-1}, \quad \text{or} \quad (f^{-1})^{-1} = f .$$

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 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 $A \in$ GL (2, $\mathbb{R}$), it has an inverse by the definition of GL (2, $\mathbb{R}$). The inverse of A is in 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:

$$a * e = a \quad \Rightarrow \quad a + e + 5 = a \quad \Rightarrow \quad e = -5.$$

If a is a real number, the inverse of a is determined by solving the equation $a * x = -5$;

$$a * x = -5 \quad \Rightarrow \quad a + x + 5 = -5 \quad \Rightarrow \quad x = -a - 10$$

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, $\mathbb{R}$).

$$\begin{aligned} AXB = C &\Rightarrow XB = A^{-1}C \quad \text{(multiply on the left by } A^{-1}\text{)} \\ &\Rightarrow X = A^{-1}CB^{-1} \text{ (multiply on the right by } B^{-1}\text{)} \end{aligned}$$

$$X = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{3} \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{4} & 0 \\ -\frac{1}{6} & \frac{1}{3} \end{pmatrix}$$

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) $A, B \in \text{SL}(2, \mathbb{R}) \Rightarrow |A| = |B| = 1$.

$$\begin{aligned} |AB| = |A|\cdot|B| = 1\cdot 1 = 1 &\Rightarrow AB \in \text{SL}(2, \mathbb{R}) \\ &\Rightarrow \text{SL}(2, \mathbb{R}) \text{ is closed with respect to matrix multiplication} \end{aligned}$$

(b) $|I| = 1 \Rightarrow I \in \text{SL}(2, \mathbb{R})$

(c) $A \in \text{SL}(2, \mathbb{R}) \Rightarrow |A| = 1$

$$|A^{-1}| = |A|^{-1} = 1 \Rightarrow A^{-1} \in \text{SL}(2, \mathbb{R})$$

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,

$$\begin{aligned} (A + B)_{ij} &= A_{ij} + B_{ij} \quad \text{definition of matrix addition} \\ &= A_{ji} + B_{ji} \quad \text{since both } A \text{ and } B \text{ are symmetirc} \\ &= (A + B)_{ji} \quad \text{definition of matrix addition} \end{aligned}$$

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 $(p \bigwedge \neg q) \Leftrightarrow 0$, and $(p \bigwedge q) \Leftrightarrow 0$, 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 $T: \mathbb{C} \to \mathbb{R}^2$ where $T(a + bi) = (a, b)$. For any two complex numbers $a + bi$ and $c + di$,

$$\begin{aligned} T((a + bi) + (c + di)) &= T((a + c) + (b + d)i) \quad \text{definition of } + \text{ in } \mathbb{C} \\ &= \{a + c, b + d) \quad \text{definition of } T \\ &= (a, b) + (c, d) \quad \text{definition of } + \text{ in } \mathbb{R}^2 \\ &= T(a + bi) + T(c + di) \quad \text{definition of } T \end{aligned}$$

Since T has an inverse ($T^{-1}(a, b) = a + bi$), 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 $U(a + bi) = (b, a)$ 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 isomosphism 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) $\{(-3 - 0.5x_3,\ 11 - 4x_3,\ x_3) \mid x_3\}$

(c) $\{(-5,\ 14/5,\ 8/5)\}$

(d) $\{(6.25 - 2.5x_3,\ -0.75 + 0.5x_3,\ x_3) \mid x_3 \in \mathbb{R}\}$

3. (a) $\{(1.2, 2.6, 4.5)\}$

(b) $\{(-6x_3 + 5,\ 2x_3 + 1,\ x_3) \mid x_3 \in \mathbb{R}\}$

(c) $\{(-9x_3 + 3,\ 4,\ x_3) \mid x_3 \in \mathbb{R}\}$

(d) $\{(3x_4 + 1,\ -2x_4 + 2,\ x_4 + 1,\ x_4) \mid x_4 \in \mathbb{R}\}$

5. (a) $\{(3, 0)\}$

(b)
$$\begin{pmatrix} 1 & 1 & 2 & 1 \\ 1 & 2 & 4 & 4 \\ 1 & 3 & 3 & 0 \end{pmatrix} \quad \begin{matrix} -R_1 + R_2 \\ -R_1 + R_3 \end{matrix} \rightarrow \begin{pmatrix} 1 & 1 & 2 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 1 & -1 \end{pmatrix}$$

$$\begin{matrix} -R_2 + R_1 \\ -2R_2 + R_3 \end{matrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & -2 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & -3 & -7 \end{pmatrix}$$

$$\tfrac{-1}{3}R_3 \rightarrow \begin{pmatrix} 1 & 0 & 0 & -2 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & \frac{7}{3} \end{pmatrix}$$

$$\tfrac{-1}{2}R_3 + R_2 \rightarrow \begin{pmatrix} 1 & 0 & 0 & -2 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & \frac{7}{3} \end{pmatrix}$$

The row reduction can be done with *Mathematica*:

```
RowReduce[{{1, 1, 2, 1}, {1, 2, 4, 4}, {1, 3, 3, 0}}]
```

$$\begin{pmatrix} 1 & 0 & 0 & -2 \\ 0 & 1 & 0 & -\frac{5}{3} \\ 0 & 0 & 1 & \frac{7}{3} \end{pmatrix}$$

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 $AX = 0$. If X_1 and X_2 be in S. Then

$$A(X_1 + X_2) = AX_1 + AX_2 = \mathbf{0} + \mathbf{0} = \mathbf{0}$$

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

$$A(-X) = -(AX) = -\mathbf{0} = \mathbf{0},$$

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 lc of Section 12.1.

$$\begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & -1 \\ 1 & 3 & 1 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ 5 \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & -1 \\ 1 & 3 & 1 \end{pmatrix}^{-1} = \frac{1}{5}\begin{pmatrix} 5 & 5 & -5 \\ -2 & -1 & 3 \\ 1 & -2 & 1 \end{pmatrix}$$

and $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = A^{-1}\begin{pmatrix} 1 \\ -1 \\ 5 \end{pmatrix} = \begin{pmatrix} -5 \\ \frac{14}{5} \\ \frac{8}{5} \end{pmatrix}$

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

$$y = (-b_1 + 2b_2)x_1 + (2b_1 - 3b_2)x_2.$$

The second linear combination can be computed using *Mathematica* as follows.

```
Solve[c1 {3, 2} + c2 {2, 1} == {b1, b2}, {c1, c2}]
```

$\{\{c_1 \to 2b_2 - b_1, c_2 \to 2b_1 - 3b_2\}\}$

(b) If $y = (b_1, b_2)$ is any vector in $\mathbb{R}^2$, then

$$y = (-3b_1 + 4b_2)x_1 + (-b_1 + b_2)x_2 + (0)x_3$$

(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

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} = xA_1z + yA_2 + zA_3 + wA_4$$

(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 AP is

$$\begin{pmatrix} A_{(1)} P^{(j)} \\ A_{(2)} P^{(j)} \\ \vdots \\ A_{(n)} P^{(j)} \end{pmatrix}$$

Hence, $(AP)^{(j)} = A\left(P^{(j)}\right)$ for $j = 1, 2, \ldots, n$. Thus, each column of AP 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 $AB = BA$. For example, in the last step, $(A+B)^2$ expands to $A^2 + AB + BA + B^2$, not $A^2 + 2AB + B^2$, if we can't assume commutativity.

$$e^A e^B = \left(\sum_{k=0}^{\infty} \frac{A^k}{k!}\right)\left(\sum_{k=0}^{\infty} \frac{B^k}{k!}\right)$$

$$= \left(I + A + \frac{A^2}{2} + \frac{A^3}{6} + \cdots\right)\left(I + B + \frac{B^2}{2} + \frac{B^3}{6} + \cdots\right)$$

$$= I + A + B + \frac{A^2}{2} + AB + \frac{B^2}{2} + \frac{A^3}{6} + \frac{A^2B}{2} + \frac{AB^2}{2} + \frac{B^3}{6} + \cdots$$

$$= I + (A+B) + \frac{1}{2}(A^2 + 2AB + B^2) + \frac{1}{6}(A^3 + 3A^2B + 3AB^2 + B^3) + \cdots$$

$$= I + (A+B) + \frac{1}{2}(A+B)^2 + \frac{1}{6}(A+B)^3 + \cdots$$

$$= e^{A+B}$$

$(A+B)^2$ 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;

$$e^A e^{-A} = e^{A+(-A)}$$
$$= e^{\mathbf{0}}$$
$$= I \qquad \text{by part } b \text{ of this problem.}$$

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

$$\begin{aligned} A(\alpha_1\,x_1 + \alpha_2\,x_2) = \mathbf{0} \quad &\Rightarrow\ \alpha_1\,x_1 + \alpha_2\,x_2 = \mathbf{0} \quad \text{since } A^{-1} \text{ exists} \\ &\Rightarrow\ \alpha_1 = \alpha_2 = 0 \quad \text{since } \{x_1,\, x_2\} \text{ is a basis} \\ &\Rightarrow\ \{A\,x_1,\, A\,x_2\} \text{ is linearly independent} \end{aligned}$$

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. $A = P^{-1}\,D\,P \quad \Rightarrow\ A^{100} = P^{-1}\,D^{100}\,P$

$$\begin{pmatrix} 0.6 & 0.2 \\ 0.4 & 0.8 \end{pmatrix} = \tfrac{1}{3}\begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}\begin{pmatrix} 1^{100} & 0 \\ 0 & 0.4^{100} \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix} \approx \begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{2}{3} & \frac{2}{3} \end{pmatrix}$$

Note: $0.4^{100} = 1.60694 \times 10^{-40} \approx 0$.

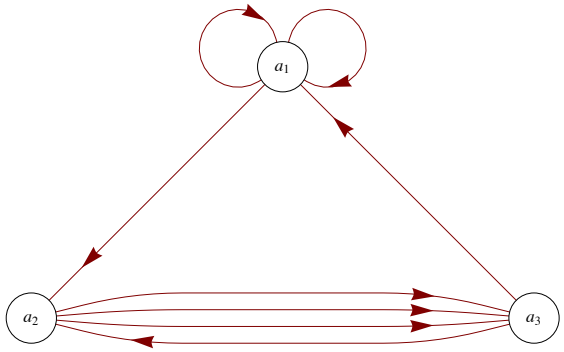
11. (a) $\lambda = 0,\ \pm\sqrt{2}$

(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

$$\begin{array}{c} \\ a_1 \\ a_2 \\ a_3 \end{array}\begin{array}{c} \begin{array}{ccc} a_1 & a_2 & a_3 \end{array} \\ \begin{pmatrix} 2 & 1 & 0 \\ 1 & 0 & 3 \\ 1 & 1 & 0 \end{pmatrix} \end{array}$$

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, $(A^2)_{ij}$ 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) ßdo not exist.

(b) No greatest element exists, but a_1 is the least element.

5. If 0 and 0' are distinct least elements, then

$$\left.\begin{array}{l} 0 \le 0' \quad \text{since 0 is a least element} \\ 0' \le 0 \quad \text{since 0' is a least element} \end{array}\right\} \Rightarrow 0 = 0' \text{ by antisymmetry, a contradiction. } \blacksquare$$

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 $g \ge h$ since g is a greatest lower bound and $h \ge g$ 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 $[L, \vee, \wedge]$ be a lattice, $a, b \in L$. We must prove that $a \vee b = b \vee a$.

Proof: By the definition of least upper bound, $a \vee b \ge b$ and $a \vee b \ge a$ therefore, by Exercise 4, part c, $a \vee b \ge b \vee a$. Similarly, $b \vee a \ge a \vee b$, and by antisymmetry $a \vee b = b \vee a$. $\blacksquare$

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
ϕ	A
$\{a\}$	$\{b, c\}$
$\{b\}$	$\{a, c\}$
$\{c\}$	$\{a, b\}$
$\{a, b\}$	$\{c\}$
$\{a, c\}$	$\{b\}$
$\{b, c\}$	$\{a\}$
A	ϕ

This lattice is a Boolean algebra since it is a distributive complemented lattice.

3. a and g.

5. (a) $S^*: a \vee b = a$ if $a \geq b$

(b) $S: A \cap B = A$ if $A \subseteq B$

$S^*: A \cup B = A$ if $A \supseteq B$

(c) Yes

(d) $S: p \wedge q \Leftrightarrow p$ if $p \Rightarrow q$

$S^*: p \vee q \Leftrightarrow p$ if $q \Rightarrow p$

(e) Yes

7. **Definition: Boolean Algebra Isomorphism.** $[B, \wedge, \vee, -]$ is isomorphic to $[B', \wedge, \vee, \sim]$ if and only if there exists a function $T: B \to B'$ such that

(a) T is a bijection;

(b) $T(a \wedge b) = T(a) \wedge T(b)$ for all $a, b \in B$

(c) $T(a \vee b) = T(a) \vee T(b)$ 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: $x \wedge 3 = 3$ or $x \wedge 3 = 1$. We do this through the following table:

x	verification
1	$1 \wedge 3 = 1$
2	$2 \wedge 3 = 1$
3	$3 \wedge 3 = 3$
5	$5 \wedge 3 = 1$
6	$6 \wedge 3 = 3$
10	$20 \wedge 3 = 1$
15	$15 \wedge 3 = 3$
30	$30 \wedge 3 = 3$

For $a = 5$, a similar verification can be performed.

(b) $6 = 2 \vee 3, 10 = 2 \vee 5, 15 = 3 \vee 5$, and $30 = 2 \vee 3 \vee 5$.

3. If $B = D_{30}$ 30 then $A = \{2, 3, 5\}$ and D_{30} is isomorphic to $\mathcal{P}(A)$, where

$1 \leftrightarrow \emptyset$ $\quad 5 \leftrightarrow \{5\}$
$2 \leftrightarrow \{2\}$ $\quad 10 \leftrightarrow \{2, 5\}$
$3 \leftrightarrow \{3\}$ $\quad 15 \leftrightarrow \{3, 5\}$
$6 \leftrightarrow \{2, 3\}$ $\quad 30 \leftrightarrow \{2, 3, 5$

and

Join $\leftrightarrow$ Union
Meet $\leftrightarrow$ Intersection
Complement $\leftrightarrow$ Set Complement

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)

$M_1(x_1, x_2) = 0$
$M_2(x_1, x_2) = (\overline{x_1} \wedge \overline{x_2})$
$M_3(x_1, x_2) = (\overline{x_1} \wedge x_2)$
$M_4(x_1, x_2) = (x_1 \wedge \overline{x_2})$
$M_5(x_1, x_2) = (x_1 \wedge x_2)$
$M_6(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \vee (\overline{x_1} \wedge x_2)) = \overline{x_1}$
$M_7(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \vee (x_1 \wedge \overline{x_2})) = \overline{x_2}$
$M_8(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \vee (x_1 \wedge x_2)) = ((x_1 \wedge x_2) \vee (\overline{x_1} \wedge \overline{x_2}))$
$M_9(x_1, x_2) = ((\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2})) = ((x_1 \wedge \overline{x_2}) \vee (\overline{x_1} \wedge x_2))$
$M_{10}(x_1, x_2) = ((\overline{x_1} \wedge x_2) \vee (x_1 \wedge x_2)) = x_2$
$M_{11}(x_1, x_2) = ((x_1 \wedge \overline{x_2}) \vee (x_1 \wedge x_2)) = x_1$
$M_{12}(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \vee (\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2})) = (\overline{x_1} \vee \overline{x_2})$
$M_{13}(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \vee (\overline{x_1} \wedge x_2) \vee (x_1 \wedge x_2)) = (\overline{x_1} \vee x_2)$
$M_{14}(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \vee (x_1 \wedge \overline{x_2}) \vee (x_1 \wedge x_2)) = (x_1 \vee \overline{x_2})$
$M_{15}(x_1, x_2) = ((\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2}) \vee (x_1 \wedge x_2)) = (x_1 \vee x_2)$
$M_{16}(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \vee (\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2}) \vee (x_1 \wedge x_2)) = 1$

(b) The truth talbe for the funcitons 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. Withthree 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:

$M(x_1, x_2) = (c_1 \wedge \overline{x_1} \wedge \overline{x_2}) \bigvee (c_2 \wedge \overline{x_1} \wedge x_2) \bigvee (c_3 \wedge x_1 \wedge \overline{x_2}) \bigvee (c_4 \wedge x_1 \wedge x_2)$

$f(0, 0) = 0 \Rightarrow M(0, 0) = 0 \Rightarrow c_1 = 0$
$f(0, 1) = 1 \Rightarrow M(0, 0) = 1 \Rightarrow c_1 = 1$
$f(1, 0) = a \Rightarrow M(0, 0) = a \Rightarrow c_1 = a$
$f(1, 1) = a \Rightarrow M(0, 0) = a \Rightarrow c_1 = a$

Therefore,

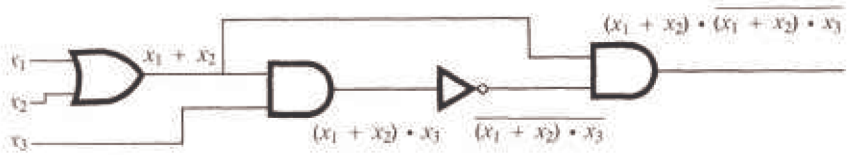
$M(x_1, x_2) = (\overline{x_1} \wedge x_2) \bigvee (a \wedge x_1 \wedge \overline{x_2}) \bigvee (a \wedge x_1 \wedge x_2)$

$M(0, a) = \left(\overline{0} \wedge a\right) \bigvee (a \bigwedge 0 \bigwedge \overline{a}) \bigvee (a \bigwedge 0 \bigwedge a) = a$

This contradicts $f(0, a) = b$, and so f is not a Boolean function.

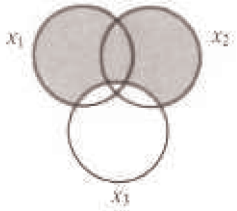
Section 13,7

1. (a)



(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:



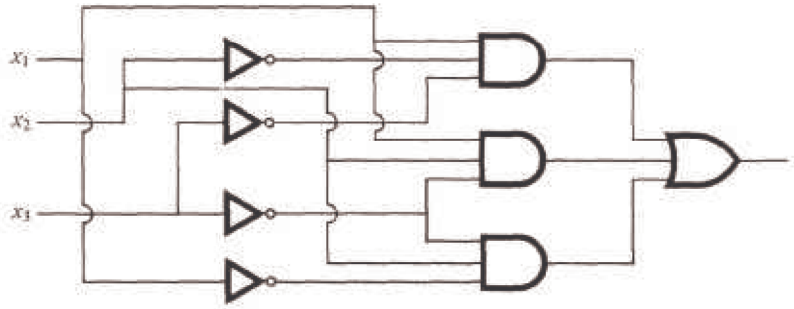
We can read off the minterm normal form from this diagram:

$$f(x_1, x_2, x_3) = x_1\cdot\overline{x_2}\cdot\overline{x_3} + x_1\cdot x_2\cdot\overline{x_3} + \overline{x_1}\cdot x_2\cdot\overline{x_3}$$

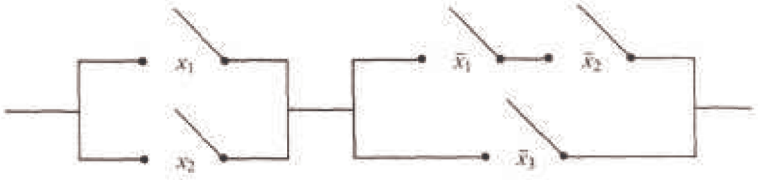
(d)

Simplified form:

Minterm form:



(e)

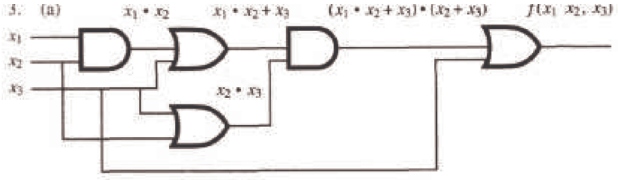


(f)

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.

5. (a)



(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 $\cdot$

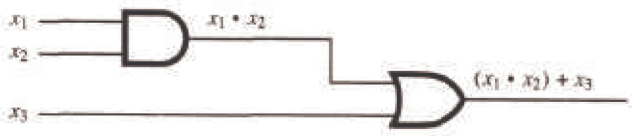
$= (x_1 \cdot (x_2 \cdot x_2)) + (x_3 + x_3)$

by the associative laws of $\cdot$ and $+$

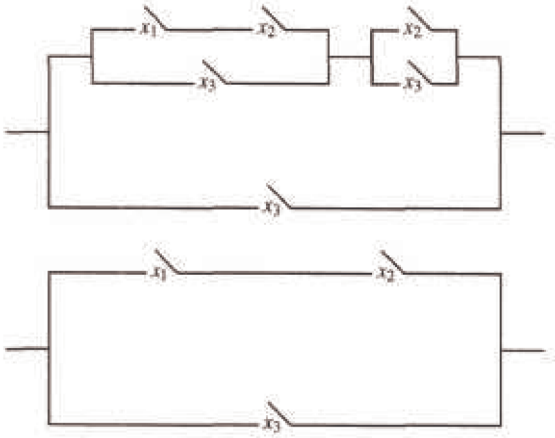
$= (x_1 \cdot x_2) + x_3$

by the idempotent laws of $\cdot$ and $+$

(c)



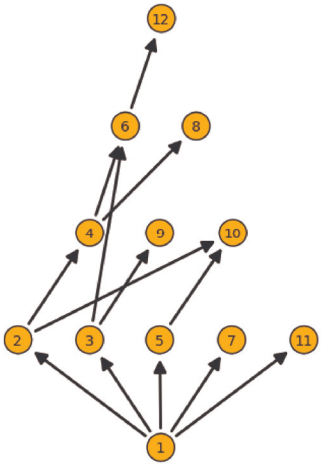
(d)



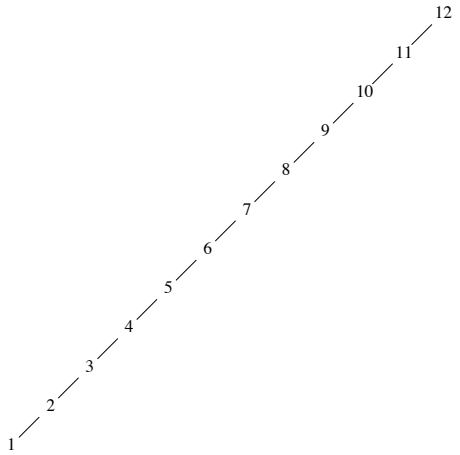
Supplementary Exercises—Chapter 13

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) $4 \vee 8 = 8, 3 \vee 15 = 15, 4 \wedge 8 = 4, 3 \wedge 15 = 3, 3 \wedge 5 - 15.$

(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.

$$a \wedge b = \gcd(a,\ b) = {p_1}^{m_1} {p_2}^{m_2} \cdots {p_n}^{m_n}$$

where $m_r = \min(i_r,\ j_r)$ and

$$a \vee b = \text{lcm}(a,\ b) = {p_1}^{M_1} {p_2}^{M_2} \cdots {p_n}^{M_n}$$

where $M_r = \max(i_r,\ j_r)$.

Based on this observation, we can compare $a \wedge (b \vee c)$ and $(a \wedge b) \vee (a \wedge c)$. The exponent of p, is $\min(i_r, \max(j_r,\ k_r))$ in $a \wedge (b \vee c)$ and $\max(\min(i_r,\ j_r),\ \min(i_r,\ k_r))$ in $(a \wedge b) \vee (a \wedge c)$. 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, $\Rightarrow$, since $0 \Rightarrow 0,\ 0 \Rightarrow 1, 1 \Rightarrow 1$ are all true statements.

(b) From the definitions of lub and gib and part (a) we have the tables

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	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, $(0,\ 1) \wedge (1,\ 0) = (0 \wedge 1,\ 1 \wedge 0) = (0,\ 0)$. 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,

$$(1,\ 0,\ 0) \vee (0,\ 1,\ 0) = (1 \vee 0, 0 \vee 1, 0 \vee 0) = (1,\ 1,\ 0)$$

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, $10 \vee 4$ does not exist in A.

(b) Yes. For all $a,\ b \in A, a \neq b$,

$a \vee b$ = the maximum of a and b,

$a \wedge b$ = 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.

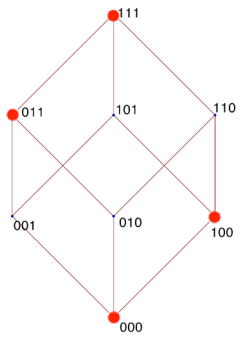
15. (a) First, by definition of subsystem in Section 11.5, a sub-Boolean algebra of a Boolean algebra B is a subset W of B which is a Boolean algebra under the same operations as B. Specifically, W must satisfy the conditions:

(i) The 0 and 1 of B must be in W,

(ii) $a \in W \Rightarrow \overline{a} \in W$

(iii) $a, b \in W \Rightarrow a \vee b \in W$ and $a \wedge b \in W$.

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.

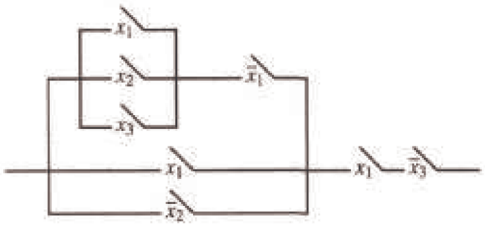
(c) A sub-Boolean algebra with 2^k elements must have k atoms; so the selection of k elements that will act as atoms can be considered in counting numbers of sub-Boolean algebras of a certain size. What is the number? We leave it to the reader in the general case.

17. $(\overline{x_1} \wedge x_2 \wedge x_3) \vee (\overline{x_1} \wedge \overline{x_2} \wedge x_3) \vee (x_1 \wedge x_2 \wedge x_3)$

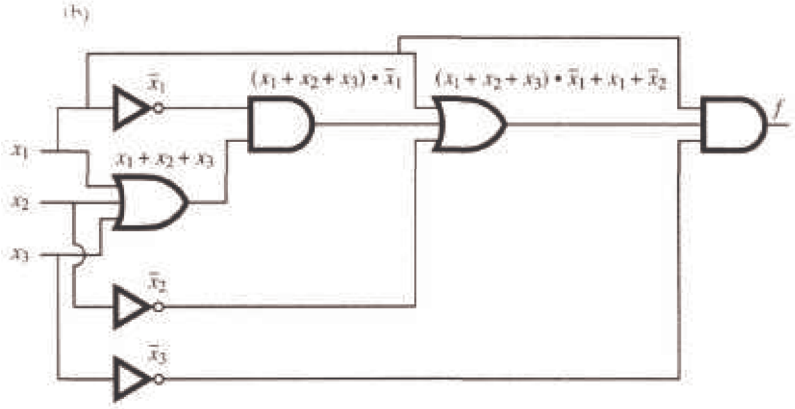
19. (a) Since each of the three variables can be any one of two values there are 2^3 rows, (See Table 13.6.3 for an example.) For n variables there are 2^n rows.

(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)



(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 $i : \mathbb{N} \to \mathbb{N}$ 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:

$$(f \circ g)(n) = f(g(n)) \leq g(n) \quad \text{since } f \text{ is in } S_1$$
$$\leq n \quad \text{since } g \text{ is in } S_1$$

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.

$$(AB)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

The sum of the j^{th} column is

$$\sum_{j=1}^{n} (AB)_{ij} = \sum_{k=1}^{n} a_{1k} b_{kj} + \sum_{k=1}^{n} a_{1k} b_{kj} + \cdots + \sum_{k=1}^{n} a_{nk} b_{kj}$$
$$= \sum_{k=1}^{n} \left(a_{1k} b_{kj} + a_{1k} b_{kj} + \cdots + a_{nk} b_{kj} \right)$$
$$= \sum_{k=1}^{n} b_{kj} (a_{1k} + a_{1k} + \cdots + a_{nk})$$
$$= \sum_{k=1}^{n} b_{kj} \qquad \text{since } A \text{ is stochastic}$$
$$= 1 \qquad \text{since } B \text{ is stochastic}$$

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: $S \to 00S,\ S \to 01S,\ S \to 10S,\ S \to 11S,\ S \to E,\ E \to 0,\ E \to 1$

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: $S \to 0A, S \to 1A, S \to \lambda, A \to 0B, A \to 1B, A \to \lambda, B \to 0C, B \to 1C, B \to A, C \to 0, C \to 1, C \to \lambda$

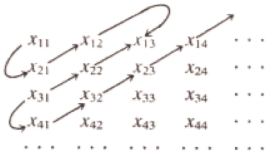
This is a regular grammar.

(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 $x_{i1}, x_{i2}, x_{i3}, \ldots$.

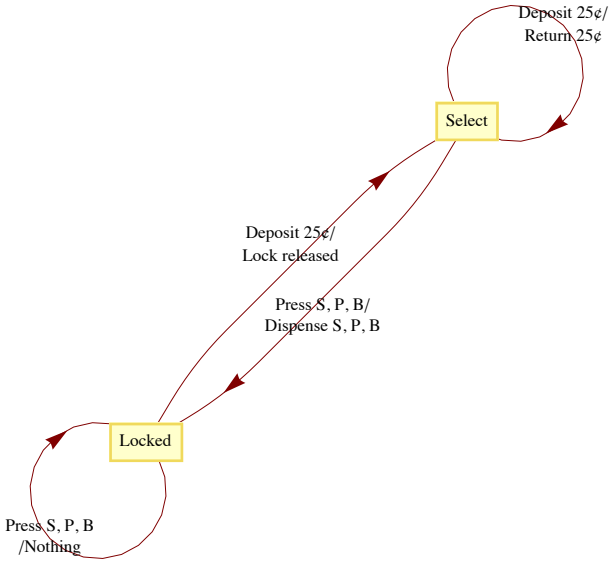


Then draw arrows as shown above and list the elements of the union in order established by this pattern: $x_{11}, x_{21}, x_{12}, x_{13}, x_{22}, x_{31}, x_{41}, x_{32}, x_{23}, x_{14}, x_{15}, \ldots$

(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 $n \geq 1$, $G_{n+1} = \begin{pmatrix} 0\, G_n \\ 1\, G_n{}^r \end{pmatrix}$, 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 $x_1 = 0$,

$$\begin{aligned} x\text{'s output} &= 0 \text{ followed by } (x_2 \ldots x_n\, x_{n+1})\text{'s output starting in Copy} \\ &= 0 \text{ followed by } (x_2 \ldots x_n\, x_{n+1})\text{'s position in } G_n \\ &= x\text{'s position in } G_{n+1} \end{aligned}$$

If $x_1 = 1$,

$$\begin{aligned} x\text{'s output} &= 1 \text{ followed by } (x_2 \ldots x_n\, x_{n+1})\text{'s output starting in Complement} \\ &= 1 \text{ followed by } (x_2 \ldots x_n\, x_{n+1})\text{'s position in } G_n{}^r \\ &= x\text{'s position in } G_{n+1} \end{aligned}$$

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.

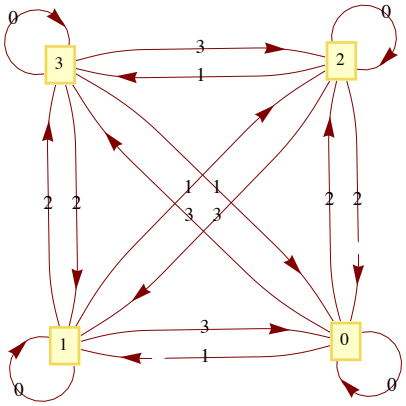
3. Yes, just consider the unit time delay machine of Figure 14.4.2. Its monoid is described by the table at the end of Section 14.4 where the T_λ row and T_λ column are omitted. Next consider the machine in Figure 14.5.3. The monoid of this machine is:

	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}

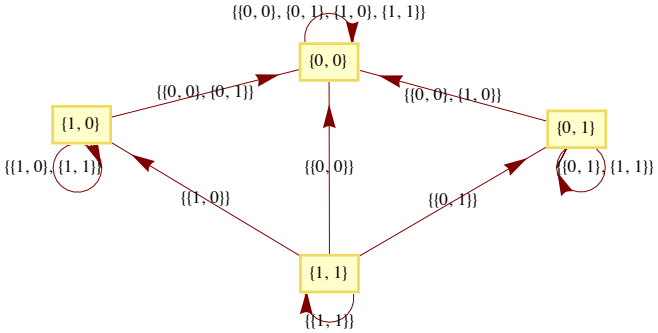
Hence both of these machines have the same monoid, however, their transition diagrams are nonisomorphic since the first has two vertices and the second has seven.

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

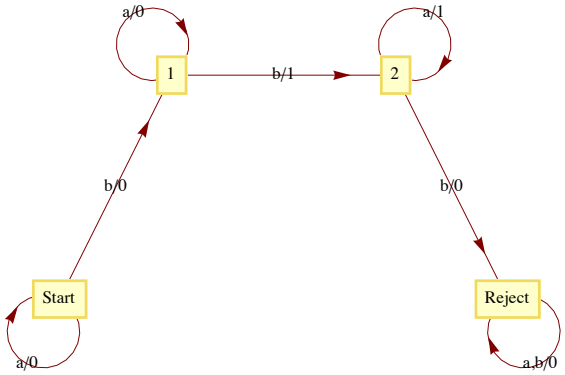
	z	i	t	u
z	z	z	z	z
i	z	i	z	i
t	z	z	t	t
u	z	u	t	u

3. $\{a,\ bb,\ bbb,\ bbbb,\ \ldots\}$

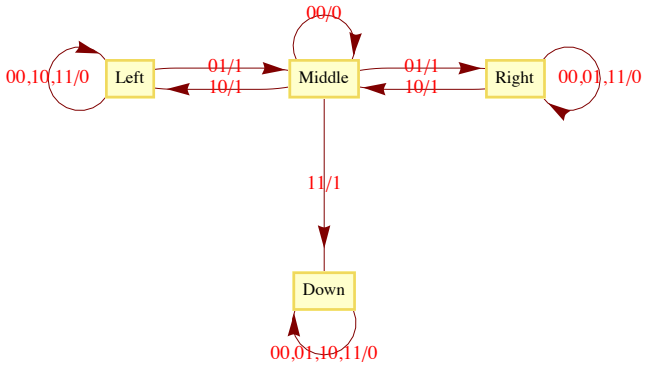
5. S = start symbol. Nonterminals = $\{S,\ B_0,\ B_1,\ B_2\}$

$S \to B_0 \quad B_0 \to a\,B_0 \quad B_0 \to b\,B_1$
$B_1 \to a\,B_1 \quad B_1 \to b\,B_2 \quad B_1 \to b$
$B_2 \to a\,B_2 \quad B_2 \to a$

7.

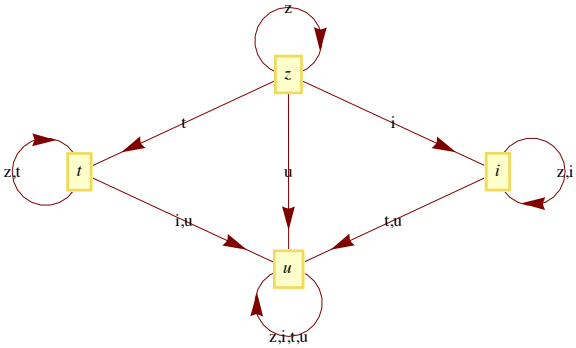


9. (a)



(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) $\theta : \mathbb{Z}_{77} \to \mathbb{Z}_7 \times \mathbb{Z}_{11}$

$$\begin{aligned}21 &\to (0, 10) \\ 5 &\to (5, 5) \\ 7 &\to (0, 7) \\ 15 &\to (1, 4) \\ \text{sum} = 48 &\leftarrow (6, 4) = \text{sum}\end{aligned}$$

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:

$$\begin{aligned}25 &\to (4, 3) \\ 26 &\to (5, 4) \\ 40 &\to (5, 7) \\ &\text{sum} = (0, 3)\end{aligned}$$

$$\begin{aligned}\theta^{-1}(0, 3) &= 3 \times_{77} \theta^{-1}(0, 1) \\ &= 3 \times_{77} 56 \\ &= 14\end{aligned}$$

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. $$\begin{aligned} a \in b\,H &\Leftrightarrow a = b * h \quad \text{for some } h \in H \\ &\Leftrightarrow b^{-1} * a = h \text{ for some } h \in H \\ &\Leftrightarrow b^{-1} * a \in H \end{aligned}$$

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

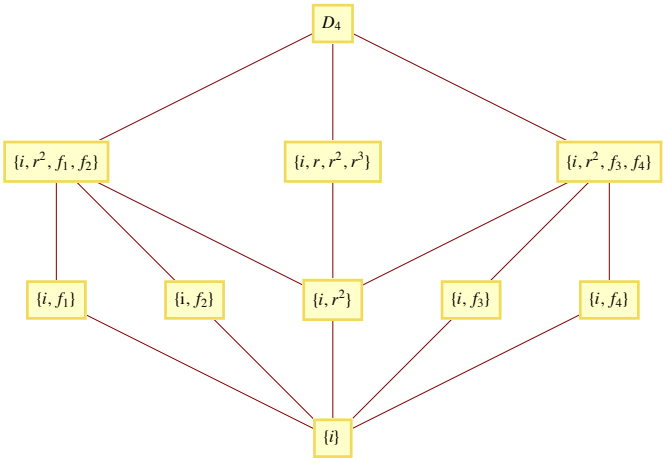
$f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ $f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

$f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ $f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$

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	$\square$	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.

$$\begin{aligned}(t_1\, t_2 \cdots t_r)^{-1} &= t_r^{-1} \cdots t_2^{-1}\, t_1^{-1} && \text{by Exercies 3 of Section 11.3}\\ &= t_r \cdots t_2\, t_1 && \text{since each transposition inverts itself.}\end{aligned}$$ ■

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 $4 \le j \le n$; and let g be defined by $g(1) = 1$, $g(2) = 3$, $g(3) = 2$, and $g(j) = j$ for $4 \le j \le n$. 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 $n \ge 3$.

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

$$\begin{aligned}\theta(i) &= I & \theta(f_1) &= F_1\\ \theta(r_1) &= R_1 & \theta(f_2) &= F_2\\ \theta(r_2) &= R_2 & \theta(f_3) &= F_3\end{aligned}$$

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

$$\theta(f)_{kj} = 1 \iff f(j) = k$$

That θ is a bijection follows from the existence of θ^{-1}. If A is a rook matrix,

$$\begin{aligned}\theta^{-1}(A)(j) = k &\iff \text{The 1 in column } j \text{ of } A \text{ appears in row } k\\ &\iff A_{kj} = 1\end{aligned}$$

For $f, g \in S_n$,

$$\begin{aligned}\theta(f \circ g)_{k\,j} = 1 &\iff (f \circ g)(j) = k\\ &\iff \exists\ l \text{ such that } g(j) = l \text{ and } f(l) = k\\ &\iff \exists\ l \text{ such that } \theta(g)_{lj} = 1 \text{ and } \theta(f)_{k\,l} = 1\\ &\iff (\theta(f)\,\theta(g))_{k\,j} = 1\end{aligned}$$

Therefore, θ is an isomorphism. ■

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 $e(a) = aG$ 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 alterative, 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 homomorphisrn 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) $$\begin{aligned}f(0) &= f(a \wedge \overline{a})\\ &= f(a) \bigwedge f\left(\bar{a}\right)\\ &= f(a) \bigwedge \overline{f(a)}\\ &= 0\end{aligned}$$

and

$$\begin{aligned}f(1) &= f(a \vee \overline{a})\\ &= f(a) \bigvee f\left(\bar{a}\right)\\ &= f(a) \bigvee \overline{f(a)}\\ &= 1\end{aligned}$$

Note : The 0 and 1 of B_1 may be different than those of B_2.

(ii) $a \le b \Rightarrow a = a \bigwedge b$ by Supplementary Exercise 4 of Chapter 13

$\Rightarrow f(a) = f(a \bigwedge b) = f(a) \bigwedge f(b)$

$\Rightarrow f(a) \le f(b)$ 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 $f(a) \bigwedge f(b) = f(a \wedge b), f(a) \bigwedge f(h) \in f(B_1)$.

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) $e(1111) = 1\,111\,111$ and $e(1001) = 1\,001\,001$

(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 $M_{2\times2}(\mathbb{R})$ 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) $(a + b)(c + d) = (a + b)c + (a + b)d$
$= ac + bc + ad + bd$

(b) $(a + b)(a + b) = aa + ba + ab + bb$ by part a
$= aa + ab + ab + bb$ since R is commutative
$= a^2 + 2ab + b^2$

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 $n + 1$.

$$g_m x^m + \text{LDT's} \;\overline{)\; f_{n+1} x^{n+1} + \text{LDT's}} \;\; \frac{f_{n+1} \cdot g_m{}^{-1} x^{n+1-m}}{f_{n+1} x^{n+1} + \text{LDT's}}$$
$$h(x)$$

Therefore,

$$h(x) = f(x) - (f_{n+1} \cdot g_m{}^{-1} x^{n+1-m})\, g(x) \Rightarrow$$
$$f(x) = (f_{n+1} \cdot g_m{}^{-1} x^{n+1-m})\, g(x) + h(x)$$

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 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:

$$\frac{1}{a_0 + a_1\sqrt{2}} = \frac{1}{a_0 + a_1\sqrt{2}} \cdot \frac{a_0 - a_1\sqrt{2}}{a_0 - a_1\sqrt{2}}$$
$$= \frac{a_0 - a_1\sqrt{2}}{a_0{}^2 - 2\,a_1{}^2}$$
$$= \frac{a_0}{a_0{}^2 - 2\,a_1{}^2} - \frac{a_1}{a_0{}^2 - 2\,a_1{}^2}\sqrt{2}$$

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 $\pm\sqrt{3}$. $\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} \;\middle|\; a, b \in \mathbb{Q}\right\}$ 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,

$$\mathbb{Z}_2(c) = \{0,\ 1,\ c,\ c^2,\ c + 1,\ c^2 + 1,\ c^2 + c + 1,\ c^2 + c\}.$$
$$= \{a_0 + a_1 c + a_2 c^2 \mid a_i \in \mathbb{Z}_2\}$$

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) $f(x) = 1 + 2x + 2^2 x^2 + 2^3 x^3 + \cdots$
$= (2x)^0 + (2x)^1 + (2x)^2 + (2x)^3 + \cdots$
$= \frac{1}{1-2x}$

The last step follows from the formula for the sum of a geometric series.

9. (a) $(x^4 - 2x^3 + x^2)^{-1} = (x^2 (x^2 - 2x + 1))^{-1}$
$= x^{-2}(1 - 2x + x^2)^{-1}$
$= x^{-2}\left(\sum_{k=0}^{\infty} (k+1) x^k \right)$ by Example 2 of 16.5
$= \sum_{k=-2}^{\infty} (k+2) x^k$

Supplementary Exercises—Chapter 16

1. (a) This ring is not commutative.

$(A + B)^2 = (A + B) \cdot (A + B)$
$= (A + B) \cdot A + (A + B) \cdot B$
$= A \cdot A + B \cdot A + A \cdot B + B \cdot B$
$= A^2 + B \cdot A + A \cdot B + B^2$

(b) Yes

3. (a) By Theorem 16.1.1 show:

(1) $[D\ +]$ is a subgroup of the group $[M_{2\times2}(\mathbb{R});\ +]$. 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 ac and bd 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 $M_{2\times2}(\mathbb{R})$ 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,

$a^2 + a + 1 = b + a + 1$
$= 1 + 1 = 0$

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. $g(0) = 0, g(1) = 1,$

$g(a) = a^3 + a^2 + a = 1 + b + a = 1 + 1 = 0,$ 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 $x^k, 0 \le k \le 6$, is not a multiple of $p(x)$, the recieved polynomial is also not a multiple of $p(x)$. The following *Mathematica* calculation verifies this last claim.

```
({{#, PolynomialRemainder[#, x^3 + x + 1, x, Modulus → 2]} & /@ Range[0, 6]}) //
 Prepend[#, {"Monomial", "Remainder"}] &
```

Monomial	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	$x^2 + 1$

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
$\Rightarrow e(a) = 111001$
$\Rightarrow a = 101$

```
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
$\Rightarrow e(a) = 110100$ (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.

$$
\begin{array}{r}
1 + 2x + 3x^2 + 4x^3 + \cdots \\
\hline
1 - 2x + x^2 \;\big)\; 1 \\
\quad 1 - 2x + 2x^2 \\
\hline
\quad\quad 2x - x^2 \\
\quad\quad 2x - 4x^2 + 2x^3 \\
\hline
\quad\quad\quad\quad 3x^2 - 2x^3 \\
\quad\quad\quad\quad 3x^2 - 6x^3 + 3x^4 \\
\hline
\quad\quad\quad\quad\quad\quad 4x^3 - 3x^4 \\
\quad\quad\quad\quad\quad\quad 4x^3 - 8x^4 + 4x^5 \\
\hline
\quad\quad\quad\quad\quad\quad\quad\quad 5x^4 - 4x^5 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \ddots
\end{array}
$$

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) $a_0 = a_1 = 1, a_2 = 0, a_3 = 1, a_4 = 1, a_5 = 0, \ldots$.

$$
\begin{aligned}
g(x) &= 1 + x + 0x^2 + x^3 + x^4 + 0x^5 + x^6 + x^7 + \cdots \\
&= (1 + x) + x^3(1 + x) + x^6(1 + x) + \cdots \\
&= (1 + x)(1 + x^3 + x^6 + \cdots) \\
&= \frac{(1+x)}{(1-x^3)}
\end{aligned}
$$