How To Prove It: A Structured Approach
Third Edition
Solutions Manual

Daniel J. Velleman
Department of Mathematics and Statistics, Amherst College
Department of Mathematics and Statistics, University of Vermont

Contents

Introduction

1. We use the formula $2^{ab} - 1 = (2^b - 1)(1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b})$ from the proof of Conjecture 2.
   (a) $2^{15} - 1 = 2^{3 \cdot 5} - 1 = (2^5 - 1) \cdot (1 + 2^5 + 2^{10}) = 31 \cdot 1057$.
   (b) $2^{32,767} - 1 = 2^{1057 \cdot 31} - 1 = (2^{31} - 1)(1 + 2^{31} + \cdots + 2^{1056 \cdot 31})$. The first factor is $2^{31} - 1 = 2{,}147{,}483{,}647$.
2. When $n = 1$, $3^n - 1 = 2$, which is prime. For all $n > 1$, $3^n - 1$ is an even integer larger than 2, so it is not prime. If n is not prime, then $3^n - 2^n$ is not prime. If n is prime, then $3^n - 2^n$ may be either prime or composite.
3. (a) The method gives $m = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$, which is prime.
   (b) The method gives $m = 2 \cdot 5 \cdot 11 + 1 = 111 = 3 \cdot 37$; 3 and 37 are both prime.
4. Using the method of the proof of Theorem 4, with $n = 5$, we get $x = 6! + 2 = 722$. The five consecutive composite numbers are $722 = 2 \cdot 361$, $723 = 3 \cdot 241$, $724 = 2 \cdot 362$, $725 = 5 \cdot 145$, and $726 = 2 \cdot 363$.
5. $2^5 - 1 = 31$ and $2^7 - 1 = 127$ are Mersenne primes. Therefore, by Euclid's theorem, $2^4(2^5 - 1) = 496$ and $2^6(2^7 - 1) = 8128$ are both perfect.
6. No. The remainder when any integer $n > 3$ is divided by 3 will be either 0, 1, or 2. If it is 0, then n is divisible by 3, so it is composite. If it is 1, then $n + 2$ is divisible by 3 and therefore composite. If it is 2, then $n + 4$ is divisible by 3 and composite. Thus, the numbers n, $n + 2$, and $n + 4$ cannot all be prime.
7. The positive integers smaller than 220 that divide 220 are 1, 2, 4, 5, 10, 11, 20, 22, 44, 55, and 110, and $1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$. The positive integers smaller than 284 that divide 284 are 1, 2, 4, 71, and 142, and $1 + 2 + 4 + 71 + 142 = 220$.

Chapter 1

Section 1.1

1. (a) $(R \vee H) \wedge \neg(H \wedge T)$, where R stands for the statement "We'll have a reading assignment," H stands for "We'll have homework problems," and T stands for "We'll have a test."
   (b) $\neg G \vee (G \wedge \neg S)$, where G stands for "You'll go skiing," and S stands for "There will be snow."
   (c) $\neg[(\sqrt{7} < 2) \vee (\sqrt{7} = 2)]$.
2. (a) $(J \wedge B) \vee \neg(J \vee B)$, where J stands for "John is telling the truth" and B stands for "Bill is telling the truth."
   (b) $(F \vee C) \wedge \neg(F \wedge P)$, where F stands for "I'll have fish," C stands for "I'll have chicken," and P stands for "I'll have mashed potatoes."
   (c) $S \wedge N \wedge F$, where S stands for "6 is divisible by 3," N stands for "9 is divisible by 3," and F stands for "15 is divisible by 3."
3. Let A stand for the statement "Alice is in the room" and B for "Bob is in the room."
   (a) $\neg(A \wedge B)$.
   (b) $\neg A \wedge \neg B$.
   (c) $\neg A \vee \neg B$; this is equivalent to the formula in (a).
   (d) $\neg(A \vee B)$; this is equivalent to the formula in (b).
4. Let P stand for "Ralph is tall," Q for "Ed is tall," R for "Ralph is handsome," and S for "Ed is handsome."
   (a) $(P \wedge Q) \vee (R \wedge S)$.

(b) $(P \vee R) \wedge (Q \vee S)$.

(c) $\neg(P \vee R) \wedge \neg(Q \vee S)$.

(d) $\neg[(P \wedge R) \vee (Q \wedge S)]$.

5. (a) and (c) are well-formed formulas.

6. (a) I won't buy the pants without the shirt.

(b) I won't buy the pants and I won't buy the shirt.

(c) Either I won't buy the pants or I won't buy the shirt.

7. (a) Either Steve or George is happy, and either Steve or George is not happy.

(b) Either Steve is happy, or George is happy and Steve isn't, or George isn't happy.

(c) Either Steve is happy, or George is happy and either Steve or George isn't happy.

8. (a) Either taxes will go up or the deficit will go up.

(b) Taxes and the deficit will not both go up, but it is not the case that taxes won't go up and the deficit also won't go up.

(c) Either taxes will go up and the deficit won't, or the deficit will go up and taxes won't.

9. See exercise 7 in Section 1.2 for the determination of whether these arguments are valid.

(a) Let J stand for "Jane will win the math prize," P for "Pete will win the math prize," and C for "Pete will win the chemistry prize." The premises are: $\neg(J \wedge P)$, $P \vee C$, J. The conclusion is C.

(b) Let B stand for "The main course will be beef," F for "The main course will be fish," P for "The vegetable will be peas," and C for "The vegetable will be corn." The premises are: $B \vee F$, $P \vee C$, $\neg(F \wedge C)$. The conclusion is $\neg(B \wedge P)$.

(c) Let J stand for "John is telling the truth," B for "Bill is telling the truth," and S for "Sam is telling the truth." The premises are $J \vee B$, $\neg S \vee \neg B$. The conclusion is $J \vee \neg S$.

(d) Let S stand for "Sales will go up," E for "Expenses will go up," and B for "The boss will be happy." There is only one premise: $(S \wedge B) \vee (E \wedge \neg B)$. The conclusion is $\neg(S \wedge E)$.

Section 1.2

1. (a)

P	Q	$\neg P \vee Q$
F	F	T
F	T	T
T	F	F
T	T	T

(b)

S	G	$(S \vee G) \wedge (\neg S \vee \neg G)$
F	F	F
F	T	T
T	F	T
T	T	F

2. (a)

P	Q	$\neg[P \wedge (Q \vee \neg P)]$
F	F	T
F	T	T
T	F	T
T	T	F

(b)

P	Q	R	$(P \vee Q) \wedge (\neg P \vee R)$
F	F	F	F
F	F	T	F
F	T	F	T
F	T	T	T
T	F	F	F
T	F	T	T
T	T	F	F
T	T	T	T

3. (a)

P	Q	$P + Q$
F	F	F
F	T	T
T	F	T
T	T	F

(b) Here are two possibilities: $(P \wedge \neg Q) \vee (Q \wedge \neg P)$, or $(P \vee Q) \wedge \neg(P \wedge Q)$. The truth table is the same as in part (a).

4. $\neg(\neg P \wedge \neg Q)$. The truth table is the same as the truth table for $P \vee Q$.

5. (a)

P	Q	$P \downarrow Q$
F	F	T
F	T	F
T	F	F
T	T	F

(b) $\neg(P \vee Q)$.

(c) $\neg P$ is equivalent to $P \downarrow P$, $P \vee Q$ is equivalent to $(P \downarrow Q) \downarrow (P \downarrow Q)$, and $P \wedge Q$ is equivalent to $(P \downarrow P) \downarrow (Q \downarrow Q)$.

6. (a)

P	Q	$P \mid Q$
F	F	T
F	T	T
T	F	T
T	T	F

(b) $\neg(P \wedge Q)$.

(c) $\neg P$ is equivalent to $P \mid P$, $P \vee Q$ is equivalent to $(P \mid P) \mid (Q \mid Q)$, and $P \wedge Q$ is equivalent to $(P \mid Q) \mid (P \mid Q)$.

7. We use the premises and conclusions identified in exercise 9 of Section 1.1.

(a) Valid: premises are all true only in line 6 of the following truth table, and the conclusion is also true in that line.

			Premises		Conclusion	
J	P	C	$\neg(J \wedge P)$	$(P \vee C)$	J	C
F	F	F	T	F	F	F
F	F	T	T	T	F	T
F	T	F	T	T	F	F
F	T	T	T	T	F	T
T	F	F	T	F	T	F
T	F	T	T	T	T	T
T	T	F	F	T	T	F
T	T	T	F	T	T	T

(b) Invalid. Here is a line of the truth table in which all premises are true but the conclusion is false:

					Premises		Conclusion
B	F	P	C	$B \vee F$	$P \vee C$	$\neg(F \wedge C)$	$\neg(B \wedge P)$
T	T	T	F	T	T	T	F

(c) Valid: premises are all true in lines 3, 5, 6, and 7 of the following truth table, and the conclusion is also true in all of those lines.

			Premises		Conclusion
J	B	S	$J \vee B$	$\neg S \vee \neg B$	$J \vee \neg S$
F	F	F	F	T	T
F	F	T	F	T	F
F	T	F	T	T	T
F	T	T	T	F	F
T	F	F	T	T	T
T	F	T	T	T	T
T	T	F	T	T	T
T	T	T	T	F	T

(d) Invalid. Here is a line of the truth table in which the premises are all true but the conclusion is false:

			Premise	Conclusion
S	E	B	$(S \wedge B) \vee (E \wedge \neg B)$	$\neg(S \wedge E)$
T	T	T	T	F

8. The following truth table shows that (a) and (c) are equivalent, as are (b) and (e):

		(a)	(b)	(c)	(d)	(e)
P	Q	$(P \wedge Q) \vee (\neg P \wedge \neg Q)$	$\neg P \vee Q$	$(P \vee \neg Q) \wedge (Q \vee \neg P)$	$\neg(P \vee Q)$	$(Q \wedge P) \vee \neg P$
F	F	T	T	T	T	T
F	T	F	T	F	F	T
T	F	F	F	F	F	F
T	T	T	T	T	F	T

9. The following truth table shows that (b) is a contradiction and (c) is a tautology:

		(a)	(b)	(c)
P	Q	$(P \vee Q) \wedge (\neg P \vee \neg Q)$	$(P \vee Q) \wedge (\neg P \wedge \neg Q)$	$(P \vee Q) \vee (\neg P \vee \neg Q)$
F	F	F	F	T
F	T	T	F	T
T	F	T	F	T
T	T	F	F	T

Formula (d) is also a tautology, as the following truth table shows:

P	Q	R	$[P \wedge (Q \vee \neg R)] \vee (\neg P \vee R)$
F	F	F	T
F	F	T	T
F	T	F	T
F	T	T	T
T	F	F	T
T	F	T	T
T	T	F	T
T	T	T	T

10. (a)

P	Q	$\neg(P \vee Q)$	$\neg P \wedge \neg Q$
F	F	T	T
F	T	F	F
T	F	F	F
T	T	F	F

(b)

P	Q	R	$P \wedge (Q \vee R)$	$(P \wedge Q) \vee (P \wedge R)$	$P \vee (Q \wedge R)$	$(P \vee Q) \wedge (P \vee R)$
F	F	F	F	F	F	F
F	F	T	F	F	F	F
F	T	F	F	F	F	F
F	T	T	F	F	T	T
T	F	F	F	F	T	T
T	F	T	T	T	T	T
T	T	F	T	T	T	T
T	T	T	T	T	T	T

11. (a) $\neg(\neg P \wedge \neg Q)$ is equivalent to $\neg\neg P \vee \neg\neg Q$ (De Morgan's law),
which is equivalent to $P \vee Q$ (double negation law).

(b) $(P \wedge Q) \vee (P \wedge \neg Q)$ is equivalent to $P \wedge (Q \vee \neg Q)$ (distributive law),
which is equivalent to P (tautology law).

(c) $\neg(P \wedge \neg Q) \vee (\neg P \wedge Q)$ is equivalent to $(\neg P \vee \neg\neg Q) \vee (\neg P \wedge Q)$ (De Morgan's law),
which is equivalent to $(\neg P \vee Q) \vee (\neg P \wedge Q)$ (double negation law),
which is equivalent to $\neg P \vee (Q \vee (\neg P \wedge Q))$ (associative law),
which is equivalent to $\neg P \vee (Q \vee (Q \wedge \neg P))$ (commutative law),
which is equivalent to $\neg P \vee Q$ (absorption law).

12. (a) $\neg(\neg P \vee Q) \vee (P \wedge \neg R)$
is equivalent to $(\neg\neg P \wedge \neg Q) \vee (P \wedge \neg R)$ (De Morgan's law),
which is equivalent to $(P \wedge \neg Q) \vee (P \wedge \neg R)$ (double negation law),
which is equivalent to $P \wedge (\neg Q \vee \neg R)$ (distributive law),
which is equivalent to $P \wedge \neg(Q \wedge R)$ (De Morgan's law).

(b) $\neg(\neg P \wedge Q) \vee (P \wedge \neg R)$
is equivalent to $(\neg\neg P \vee \neg Q) \vee (P \wedge \neg R)$ (De Morgan's law),
which is equivalent to $(P \vee \neg Q) \vee (P \wedge \neg R)$ (double negation law),
which is equivalent to $(\neg Q \vee P) \vee (P \wedge \neg R)$ (commutative law),
which is equivalent to $\neg Q \vee (P \vee (P \wedge \neg R))$ (associative law),
which is equivalent to $\neg Q \vee P$ (absorption law).

(c) $(P \wedge R) \vee [\neg R \wedge (P \vee Q)]$
is equivalent to $(P \wedge R) \vee [(\neg R \wedge P) \vee (\neg R \wedge Q)]$ (distributive law),
which is equivalent to $(P \wedge R) \vee [(P \wedge \neg R) \vee (Q \wedge \neg R)]$ (commutative law),
which is equivalent to $[(P \wedge R) \vee (P \wedge \neg R)] \vee (Q \wedge \neg R)$ (associative law),
which is equivalent to $[P \wedge (R \vee \neg R)] \vee (Q \wedge \neg R)$ (distributive law),
which is equivalent to $P \vee (Q \wedge \neg R)$ (tautology law).

13. $\neg(P \vee Q)$ is equivalent to $\neg(\neg\neg P \vee \neg\neg Q)$ (double negation law),
which is equivalent to $\neg\neg(\neg P \wedge \neg Q)$ (first De Morgan's law),
which is equivalent to $\neg P \wedge \neg Q$ (double negation law).

14. We use the associative law for $\wedge$ twice:

$$[P \wedge (Q \wedge R)] \wedge S \text{ is equivalent to } [(P \wedge Q) \wedge R] \wedge S$$
$$\text{which is equivalent to } (P \wedge Q) \wedge (R \wedge S).$$

15. 2^n.

16. $P \vee \neg Q$. (You can check this by making the truth table.)

17. $(P \wedge \neg Q) \vee (Q \wedge \neg P)$. (You can check this by making the truth table.)

18. If the conclusion is a tautology, then the argument is valid. If the conclusion is a contradiction and there is at least one line of the truth table in which all the premises are true, then the argument is not valid. If one of the premises is a tautology, then you can delete that premise without affecting the validity of the argument. If one of the premises is a contradiction, then the argument is valid.

Section 1.3

1. (a) $D(6) \wedge D(9) \wedge D(15)$, where $D(x)$ means "x is divisible by 3."
   (b) $D(x, 2) \wedge D(x, 3) \wedge \neg D(x, 4)$, where $D(x, y)$ means "x is divisible by y."
   (c) $N(x) \wedge N(y) \wedge [(P(x) \wedge \neg P(y)) \vee (P(y) \wedge \neg P(x))]$, where $N(x)$ means "x is a natural number" and $P(x)$ means "x is prime."
2. (a) $M(x) \wedge M(y) \wedge [(T(x, y) \vee T(y, x)]$, where $M(x)$ means "x is a man" and $T(x, y)$, means "x is taller than y."
   (b) $(B(x) \vee B(y)) \wedge (R(x) \vee R(y))$, where $B(x)$ means "x has brown eyes" and $R(x)$ means "x has red hair."
   (c) $(B(x) \wedge R(x)) \vee (B(y) \wedge R(y))$, where the letters have the same meanings as in part (b).
3. (a) $\{x \mid x \text{ is a planet}\}$.
   (b) $\{x \mid x \text{ is an Ivy League school}\}$.
   (c) $\{x \mid x \text{ is a state in the United States}\}$.
   (d) $\{x \mid x \text{ is a province or territory in Canada}\}$.
4. (a) $\{x \mid x \text{ is the square of a positive integer}\}$.
   (b) $\{x \mid x \text{ is a power of 2}\}$.
   (c) $\{x \mid x \text{ is an integer and } 10 \leq x < 20\}$.
5. (a) $(-3 \in \mathbb{R}) \wedge (13 - 2(-3) > 1)$. Bound variables: x; no free variables. This statement is true.
   (b) $(4 \in \mathbb{R}) \wedge (4 < 0) \wedge (13 - 2(4) > 1)$. Bound variables: x; no free variables. This statement is false.
   (c) $\neg[(5 \in \mathbb{R}) \wedge (13 - 2(5) > c)]$. Bound variables: x; free variables: c.
6. (a) $(w \in \mathbb{R}) \wedge (13 - 2w > c)$. Bound variables: x; free variables: w, c.
   (b) $(4 \in \mathbb{R}) \wedge (13 - 2(4)$ is a prime number). Bound variables: x, y; no free variables. This statement is true.
   (c) (4 is a prime number) $\wedge (13 - 2(4) > 1)$. Bound variables: x, y; no free variables. This statement is false.
7. (a) $\{-1, 1/2\}$.

(b) $\{1/2\}$.

(c) $\{-1\}$.

(d) $\varnothing$.

8. (a) $\{x \mid$ Elizabeth Taylor was once married to $x\} = \{$Conrad Hilton Jr., Michael Wilding, Michael Todd, Eddie Fisher, Richard Burton, John Warner, Larry Fortensky$\}$.

   (b) $\{x \mid x$ is a logical connective studied in Section 1.1$\} = \{\wedge, \vee, \neg\}$.

   (c) $\{x \mid x$ is the author of this book$\} = \{$Daniel J. Velleman$\}$.

9. (a) $\{x \in \mathbb{R} \mid x^2 - 4x + 3 = 0\} = \{1, 3\}$.

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

   (c) $\{x \in \mathbb{R} \mid 5 \in \{y \in \mathbb{R} \mid x^2 + y^2 < 50\}\} = \{x \in \mathbb{R} \mid 5 \in \mathbb{R} \wedge x^2 + 25 < 50\} = \{x \in \mathbb{R} \mid x^2 < 25\} = \{x \in \mathbb{R} \mid -5 < x < 5\}$. Examples of elements: -4, 2, 4.9, π.

Section 1.4

1. (a) $\{3, 12\}$.

   (b) $\{1, 12, 20, 35\}$.

   (c) $\{1, 3, 12, 20, 35\}$.

   The sets in parts (a) and (b) are both subsets of the set in part (c).

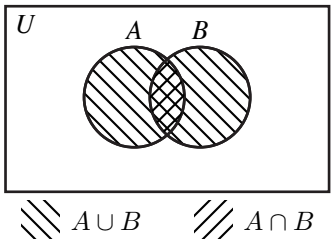
2. (a) {United States, Germany, China, Australia, France, India, Brazil}.

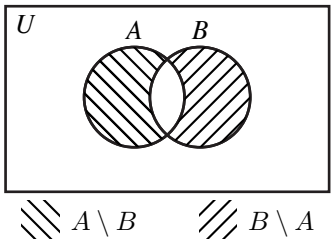
   (b) $\varnothing$.

   (c) {France}.

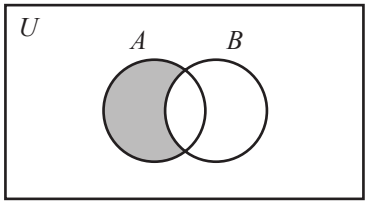
   The set in part (b) is disjoint from both of the other sets, and also a subset of both other sets. The set in part (c) is a subset of the set in part (a).

3. In the diagram on the left below, the set $(A \cup B) \setminus (A \cap B)$ is represented by the region that is striped but not crosshatched. In the diagram on the right, the set $(A \setminus B) \cup (B \setminus A)$ is represented by the region that striped (in either direction).

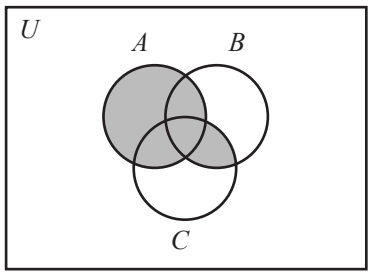




4. (a) Both Venn diagrams look like this:



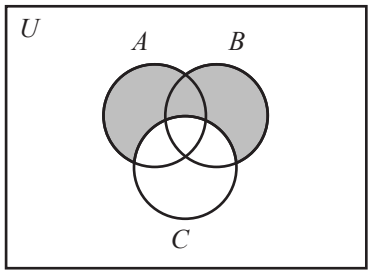
(b) Both Venn diagrams look like this:



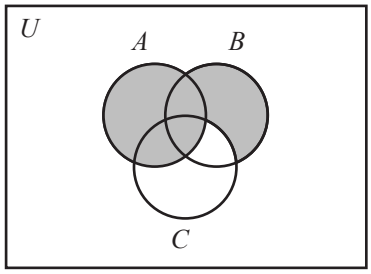
5. (a) $x \in A \setminus (A \cap B)$ is equivalent to $x \in A \wedge \neg(x \in A \wedge x \in B)$ (definitions of $\setminus$, $\cap$),
which is equivalent to $x \in A \wedge (x \notin A \vee x \notin B)$ (De Morgan's law),
which is equivalent to $(x \in A \wedge x \notin A) \vee (x \in A \wedge x \notin B)$ (distributive law),
which is equivalent to $x \in A \wedge x \notin B$ (contradiction law),
which is equivalent to $x \in A \setminus B$ (definition of $\setminus$).

(b) $x \in A \cup (B \cap C)$ is equivalent to $x \in A \vee (x \in B \wedge x \in C)$ (definitions of $\cup$, $\cap$),
which is equivalent to $(x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$ (distributive law),
which is equivalent to $x \in (A \cup B) \cap (A \cup C)$ (definitions of $\cup$, $\cap$).

6. (a) Both Venn diagrams look like this:



(b) Both Venn diagrams look like this:



7. (a) $x \in (A \cup B) \setminus C$ is equivalent to $(x \in A \vee x \in B) \wedge x \notin C$ (definitions of $\cup$, $\setminus$),
which is equivalent to $(x \in A \wedge x \notin C) \vee (x \in B \wedge x \notin C)$ (distributive law),
which is equivalent to $x \in (A \setminus C) \cup (B \setminus C)$ (definitions of $\setminus$, $\cup$).

(b) $x \in A \cup (B \setminus C)$ is equivalent to $x \in A \vee (x \in B \wedge x \notin C)$ (definitions of $\cup$, $\setminus$),
which is equivalent to $(x \in A \vee x \in B) \wedge (x \in A \vee x \notin C)$ (distributive law),
which is equivalent to $(x \in A \vee x \in B) \wedge \neg(x \notin A \wedge x \in C)$ (De Morgan's law),

which is equivalent to $x \in (A \cup B) \setminus (C \setminus A)$ (definitions of $\cup$, $\setminus$).

8. (a) $x \in (A \setminus B) \cap C$ is equivalent to $(x \in A \wedge x \notin B) \wedge x \in C$ (definitions of $\setminus$, $\cap$),
which is equivalent to $x \in A \wedge (x \notin B \wedge x \in C)$ (associative law),
which is equivalent to $x \in A \wedge (x \in C \wedge x \notin B)$ (commutative law),
which is equivalent to $(x \in A \wedge x \in C) \wedge x \notin B$ (associative law),
which is equivalent to $x \in (A \cap C) \setminus B$ (definitions of $\cap$, $\setminus$).

(b) $x \in (A \cap B) \setminus B$ is equivalent to $(x \in A \wedge x \in B) \wedge x \notin B$ (definitions of $\cap$, $\setminus$).
This is clearly a contradiction, so $(A \cap B) \setminus B = \varnothing$.

(c) $x \in A \setminus (A \setminus B)$ is equivalent to $x \in A \wedge \neg(x \in A \wedge x \notin B)$ (definition of $\setminus$),
which is equivalent to $x \in A \wedge (x \notin A \vee x \in B)$ (De Morgan's law),
which is equivalent to $(x \in A \wedge x \notin A) \vee (x \in A \wedge x \in B)$ (distributive law),
which is equivalent to $x \in A \wedge x \in B$ (contradiction law),
which is equivalent to $x \in A \cap B$ (definition of $\cap$).

9. (a) $x \in (A \setminus B) \setminus C$ means $(x \in A \wedge x \notin B) \wedge x \notin C$.
(b) $x \in A \setminus (B \setminus C)$ means $x \in A \wedge \neg(x \in B \wedge x \notin C)$
which is equivalent to $x \in A \wedge (x \notin B \vee x \in C)$ (De Morgan's law),
which is equivalent to $(x \in A \wedge x \notin B) \vee (x \in A \wedge x \in C)$ (distributive law).

(c) $x \in (A \setminus B) \cup (A \cap C)$ means $(x \in A \wedge x \notin B) \vee (x \in A \wedge x \in C)$.
(d) $x \in (A \setminus B) \cap (A \setminus C)$ means $(x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C)$
which is equivalent to $((x \in A \wedge x \notin B) \wedge x \in A) \wedge x \notin C$ (associative law),
which is equivalent to $(x \in A \wedge (x \in A \wedge x \notin B)) \wedge x \notin C$ (commutative law),
which is equivalent to $((x \in A \wedge x \in A) \wedge x \notin B) \wedge x \notin C$ (associative law),
which is equivalent to $(x \in A \wedge x \notin B) \wedge x \notin C$ (idempotent law).

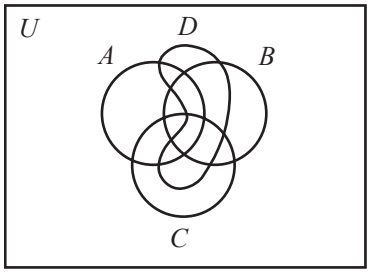
(e) $x \in A \setminus (B \cup C)$ means $x \in A \wedge \neg(x \in B \vee x \in C)$
which is equivalent to $x \in A \wedge (x \notin B \wedge x \notin C)$ (De Morgan's law),
which is equivalent to $(x \in A \wedge x \notin B) \wedge x \notin C$ (associative law).

This shows that sets (a), (d), and (e) are equal, and sets (b) and (c) are equal.

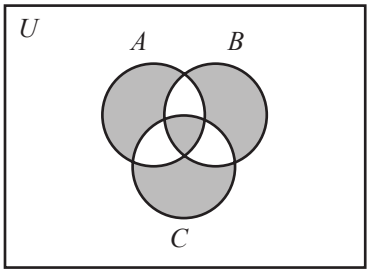
10. (a) $A = \{1, 2\}$, $B = \{2, 3\}$. $(A \cup B) \setminus B = \{1, 2, 3\} \setminus \{2, 3\} = \{1\} \neq \{1, 2\} = A$.
(b) $x \in (A \cup B) \setminus B$ is equivalent to $(x \in A \vee x \in B) \wedge x \notin B$ (definitions of $\cup$, $\setminus$),
which is equivalent to $(x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin B)$ (distributive law),
which is equivalent to $x \in A \wedge x \notin B$ (contradiction law),
which is equivalent to $x \in A \setminus B$ (definition of $\setminus$).

11. The Venn diagram for $(A \setminus B) \cup B$ looks the same as the Venn diagram for $A \cup B$, so $(A \setminus B) \cup B = A \cup B$. Therefore $A \subseteq (A \setminus B) \cup B$, but the two sets need not be equal. For example, if $A = \{1, 2\}$ and $B = \{2, 3\}$ then $(A \setminus B) \cup B = \{1\} \cup \{2, 3\} = \{1, 2, 3\} \neq \{1, 2\} = A$.

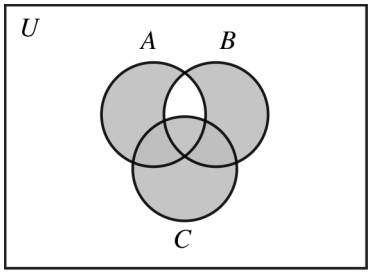
12. (a) There is no region corresponding to the set $(A \cap D) \setminus (B \cup C)$, but this set could have elements.
(b) Here is one possibility:



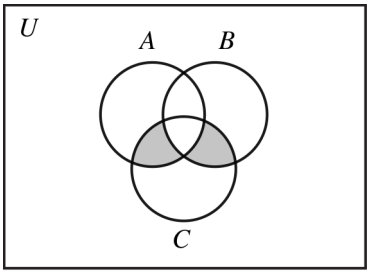
13. (a) The Venn diagrams are given in the solution to exercise 6. Those diagrams show that $(A \cup B) \setminus C \subseteq A \cup (B \setminus C)$.
    (b) $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$, $C = \{3, 4, 5\}$. $(A \cup B) \setminus C = \{1, 2, 3, 4\} \setminus \{3, 4, 5\} = \{1, 2\}$, $A \cup (B \setminus C) = \{1, 2, 3\} \cup \{2\} = \{1, 2, 3\}$.
14. The Venn diagrams for both sets look like this:



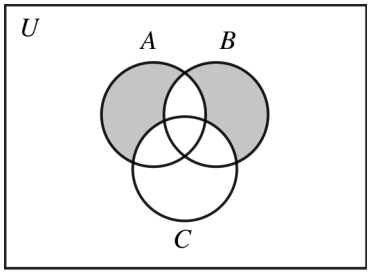
15. (a) $(A \triangle B) \cup C = (A \cup C) \triangle (B \setminus C)$.



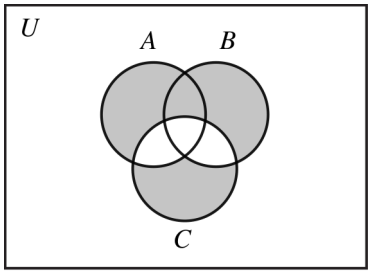
(b) $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$.



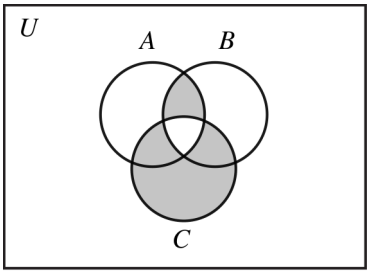
(c) $(A \triangle B) \setminus C = (A \setminus C) \triangle (B \setminus C)$.



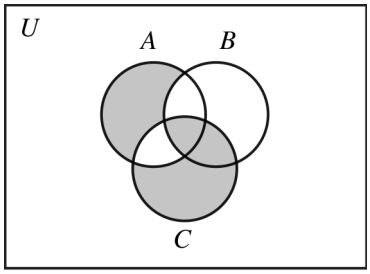
16. (a) $(A \cup B) \triangle C = (A \triangle C) \triangle (B \setminus A)$.



(b) $(A \cap B) \triangle C = (A \triangle C) \triangle (A \setminus B)$.



(c) $(A \setminus B) \triangle C = (A \triangle C) \triangle (A \cap B)$.



17. All of the following answers can be confirmed with Venn diagrams.
    (a) $C \setminus B$.
    (b) $C \setminus B$.
    (c) $A \cup B$.

Section 1.5

1. (a) $(S \vee \neg E) \rightarrow \neg H$, where S stands for "This gas has an unpleasant smell," E stands for "This gas is explosive," and H stands for "This gas is hydrogen."

   (b) $(F \wedge H) \rightarrow D$, where F stands for "George has a fever," H stands for "George has a headache," and D stands for "George will go to the doctor."

   (c) $(F \rightarrow D) \wedge (H \rightarrow D)$, where the letters have the same meanings as in part (b).

   (d) $(x \neq 2) \rightarrow (P(x) \rightarrow O(x))$, where $P(x)$ stands for "x is prime" and $O(x)$ stands for "x is odd."

2. (a) $H \rightarrow (P \wedge A)$, where H stands for "Mary will sell her house," P stands for "Mary can get a good price," and A stands for "Mary can find a nice apartment."

   (b) $M \rightarrow (C \wedge P)$, where C stands for "you have a good credit history," P stands for "you have an adequate down payment," and M stands for "you will get a mortgage."

   (c) $\neg S \rightarrow D$, where D stands for "John will drop out of school," and S stands for "someone will stop him."

   (d) $(D(x,4) \vee D(x,6)) \rightarrow \neg P(x)$, where $D(x,y)$ means "x is divisible by y" and $P(x)$ means "x is prime."

3. Let R stand for "It is raining," W for "It is windy," and S for "It is sunny."

   (a) $R \rightarrow (W \wedge \neg S)$.

   (b) $(W \wedge \neg S) \rightarrow R$. This is the converse of (a).

   (c) $R \rightarrow (W \wedge \neg S)$. This is the same as (a).

   (d) $(W \wedge \neg S) \rightarrow R$. This is the converse of (a).

   (e) $(S \vee \neg W) \rightarrow \neg R$
   which is equivalent to $R \rightarrow \neg(S \vee \neg W)$ (contrapositive law),
   which is equivalent to $R \rightarrow (\neg S \wedge W)$ (De Morgan's law),
   which is equivalent to (a).

   (f) $(R \rightarrow W) \wedge (R \rightarrow \neg S)$
   which is equivalent to $(\neg R \vee W) \wedge (\neg R \vee \neg S)$ (conditional law),
   which is equivalent to $\neg R \vee (W \wedge \neg S)$ (distributive law),
   which is equivalent to $R \rightarrow (W \wedge \neg S)$ (conditional law),
   which is the same as (a).

   (g) $(W \rightarrow R) \vee (\neg S \rightarrow R)$
   which is equivalent to $(\neg W \vee R) \vee (S \vee R)$ (conditional law),
   which is equivalent to $(\neg W \vee S) \vee (R \vee R)$ (commutative, associative laws),
   which is equivalent to $\neg(W \wedge \neg S) \vee R$ (De Morgan's, idempotent laws),
   which is equivalent to $(W \wedge \neg S) \rightarrow R$ (conditional law),
   which is the converse of (a).

4. (a) Let S stand for "Sales will go up," E for "Expenses will go up," and B for "The boss will be happy." Valid.

				Premises		Conclusion
S	E	B	$S \vee E$	$S \to B$	$E \to \neg B$	$\neg(S \wedge E)$
F	F	F	F	T	T	T
F	F	T	F	T	T	T
F	T	F	T	T	T	T
F	T	T	T	T	F	T
T	F	F	T	F	T	T
T	F	T	T	T	T	T
T	T	F	T	F	T	F
T	T	T	T	T	F	F

(b) Let T stand for "The tax rate will go up," U for "The unemployment rate will go up," R for "There will be a recession," and G for "GDP will go up." Valid. To shorten the truth table, we take some shortcuts. "-" indicates an entry that could be T or F.

				Premises			Conclusion
T	U	R	G	$(T \wedge U) \to R$	$G \to \neg R$	$G \wedge T$	$\neg U$
F	-	-	-	T	-	F	-
T	-	-	F	-	T	F	-
T	F	-	T	T	-	T	T
T	T	F	T	F	T	T	F
T	T	T	T	T	F	T	F

(c) Let W stand for "The warning light will come on," P for "The pressure is too high," and C for "The relief valve is clogged." Invalid. Here is a line of the truth table in which the premises are all true but the conclusion is false:

			Premises		Conclusion
W	P	C	$W \leftrightarrow (P \wedge C)$	$\neg C$	$W \leftrightarrow P$
F	T	F	T	T	F

5. (a) Let J stand for "Jones will be convicted," P for "Jones will go to prison," and S for "Smith will testify agains Jones." Invalid. Here is a line of the truth table in which the premises are all true but the conclusion is false.

			Premises		Conclusion
J	P	S	$J \to P$	$J \to S$	$\neg S \to \neg P$
F	T	F	T	T	F

(b) Let D stand for "The Democrats will have a majority in the Senate," R for "The Republicans will have a majority in the senate," and B for "The bill will pass." Valid.

			Premises		Conclusion
D	R	B	$(D \vee R) \wedge \neg(D \wedge R)$	$B \to D$	$R \to \neg B$
F	F	F	F	T	T
F	F	T	F	F	T
F	T	F	T	T	T
F	T	T	T	F	F
T	F	F	T	T	T
T	F	T	T	T	T
T	T	F	F	T	T
T	T	T	F	T	F

6. (a)

P	Q	$P \leftrightarrow Q$	$(P \wedge Q) \vee (\neg P \wedge \neg Q)$
F	F	T	T
F	T	F	F
T	F	F	F
T	T	T	T

(b) $(P \to Q) \vee (P \to R)$ is equivalent to $(\neg P \vee Q) \vee (\neg P \vee R)$ (conditional law),
which is equivalent to $(\neg P \vee \neg P) \vee (Q \vee R)$ (commutative, associative laws),
which is equivalent to $\neg P \vee (Q \vee R)$ (idempotent law),
which is equivalent to $P \to (Q \vee R)$ (conditional law).

7. (a) $(P \to R) \wedge (Q \to R)$
is equivalent to $(\neg P \vee R) \wedge (\neg Q \vee R)$ (conditional law),
which is equivalent to $(\neg P \wedge \neg Q) \vee R$ (distributive law),
which is equivalent to $\neg(P \vee Q) \vee R$ (De Morgan's law),
which is equivalent to $(P \vee Q) \to R$ (conditional law).

(b) $(P \to R) \vee (Q \to R)$
is equivalent to $(\neg P \vee R) \vee (\neg Q \vee R)$ (conditional law),
which is equivalent to $(\neg P \vee \neg Q) \vee (R \vee R)$ (commutative, associative laws),
which is equivalent to $\neg(P \wedge Q) \vee R$ (De Morgan's, idempotent laws),
which is equivalent to $(P \wedge Q) \to R$ (conditional law).

8. (a)

P	Q	R	$(P \to Q) \wedge (Q \to R)$	$(P \to R) \wedge [(P \leftrightarrow Q) \vee (R \leftrightarrow Q)]$
F	F	F	T	T
F	F	T	T	T
F	T	F	F	F
F	T	T	T	T
T	F	F	F	F
T	F	T	F	F
T	T	F	F	F
T	T	T	T	T

(b) $(P \to Q) \vee (Q \to R)$
is equivalent to $(\neg P \vee Q) \vee (\neg Q \vee R)$ (conditional law),
which is equivalent to $(\neg P \vee R) \vee (Q \vee \neg Q)$ (commutative, associative laws),
which is a tautology (tautology law).

9. $\neg(P \to \neg Q)$. The equivalence can be checked with a truth table.

10. $\neg((P \to Q) \to \neg(Q \to P))$. The equivalence can be checked with a truth table.

11. (a)

P	Q	$(P \vee Q) \leftrightarrow Q$	$P \to Q$
F	F	T	T
F	T	T	T
T	F	F	F
T	T	T	T

(b)

P	Q	$(P \wedge Q) \leftrightarrow Q$	$Q \to P$
F	F	T	T
F	T	F	F
T	F	T	T
T	T	T	T

12. (a), (b), and (d) are equivalent; (c) and (e) are equivalent. This can be seen in the following truth table.

P	Q	R	(a) $P \to (Q \to R)$	(b) $Q \to (P \to R)$	(c) $(P \to Q) \wedge (P \to R)$	(d) $(P \wedge Q) \to R$	(e) $P \to (Q \wedge R)$
F	F	F	T	T	T	T	T
F	F	T	T	T	T	T	T
F	T	F	T	T	T	T	T
F	T	T	T	T	T	T	T
T	F	F	T	T	F	T	F
T	F	T	T	T	F	T	F
T	T	F	F	F	F	F	F
T	T	T	T	T	T	T	T

Chapter 2

Section 2.1

1. (a) $\forall x[\exists y F(x,y) \to S(x)]$, where $F(x,y)$ stands for "x has forgiven y," and $S(x)$ stands for "x is a saint."
   (b) $\neg\exists x[C(x) \wedge \forall y(D(y) \to S(x,y))]$, where $C(x)$ stands for "x is in the calculus class," $D(y)$ stands for "y is in the discrete math class," and $S(x,y)$ stands for "x is smarter than y."
   (c) $\forall x(\neg(x = m) \to L(x,m))$, where $L(x,y)$ stands for "x likes y," and m stands for Mary.
   (d) $\exists x(P(x) \wedge S(j,x)) \wedge \exists y(P(y) \wedge S(r,y))$, where $P(x)$ stands for "x is a police officer," $S(x,y)$ stands for "x saw y," j stands for Jane, and r stands for Roger.
   (e) $\exists x(P(x) \wedge S(j,x) \wedge S(r,x))$, where the letters have the same meanings as in part (d).
2. (a) $\forall x[B(x) \to \exists y(U(y,x) \wedge R(y))]$, where $B(x)$ stands for "x has bought a Rolls Royce with cash," $U(y,x)$ stands for "y is an uncle of x," and $R(y)$ stands for "y is rich."
   (b) $\exists x(D(x) \wedge M(x)) \to \forall x[\exists y(F(y,x) \wedge D(y)) \to Q(x)]$, where $D(x)$ stands for "x is in the dorm," $M(x)$ stands for "x has the measles," $F(y,x)$ stands for "y is a friend of x," and $Q(x)$ stands for "x will have to be quarantined."
   (c) $\neg\exists x F(x) \to \forall x[A(x) \to \exists y(D(y) \wedge T(x,y))]$, where $F(x)$ stands for "x failed the test," $A(x)$ stands for "x got an A," $D(x)$ stands for "x got a D," and $T(x,y)$ stands for "x will tutor y."
   (d) $\exists x D(x) \to D(j)$, where $D(x)$ stands for "x can do it" and j stands for Jones.
   (e) $D(j) \to \forall x D(x)$, where the letters have the same meanings as in part (d).
3. (a) $\forall z(z > x \to z > y)$. Free variables: x, y.
   (b) $\forall a[\exists x(ax^2 + 4x - 2 = 0) \leftrightarrow (a > -2 \vee a = -2)]$. No free variables.
   (c) $\forall x(x^3 - 3x < 3 \to x < 10)$. No free variables.
   (d) $(\exists x(x^2 + 5x = w) \wedge \exists y(4 - y^2 = w)) \to (-10 < w \wedge w < 10)$. Free variables: w.
4. (a) All unmarried men are unhappy.
   (b) y is a sister of one of x's parents; i.e., y is x's blood aunt.
5. (a) Every prime number other than 2 is odd.
   (b) There is a largest perfect number.
6. (a) There is no real number that is a solution to both of the equations $x^2+2x+3 = 0$ and $x^2+2x-3 = 0$. This is true, because $x^2 + 2x + 3$ and $x^2 + 2x - 3$ cannot both be 0.
   (b) It is not the case that both of the equations $x^2 + 2x + 3 = 0$ and $x^2 + 2x - 3 = 0$ have real solutions. This is true, because the equation $x^2 + 2x + 3 = 0$ has no real solution.
   (c) Both of the equations $x^2 + 2x + 3 = 0$ and $x^2 + 2x - 3 = 0$ have no real solutions. This is false, because $x = 1$ is a solution to the second equation.

7. We translate each statement into English before saying whether it is true or false.
   (a) There is someone who is a parent of everyone. False; no one person is a parent of everyone.
   (b) Everyone is a parent of someone. False; some people have no children.
   (c) No one is a parent of anyone. False; some people have children.
   (d) Someone has no children. True.
   (e) Someone is not a parent of someone. True; for example, Barack Obama is not a parent of Angelina Jolie.
8. (a), (d), and (e) are true; (b), (c), and (f) are false.
9. (a), (c), (e), and (f) are true; (b) and (d) are false.
10. (a), (d), (e), and (f) are true; (b) and (c) are false.

Section 2.2

1. (a) Let $M(x)$ stand for "x is majoring in math," $F(x, y)$ for "x and y are friends," and $H(y)$ for "y needs help with his or her homework."

$$\begin{aligned}
&\neg\forall x[M(x) \to \exists y(F(x,y) \wedge H(y))] \\
&\qquad \text{is equivalent to } \exists x\neg[M(x) \to \exists y(F(x,y) \wedge H(y))] && \text{(quantifier negation law),} \\
&\text{which is equivalent to } \exists x\neg[\neg M(x) \vee \exists y(F(x,y) \wedge H(y))] && \text{(conditional law),} \\
&\text{which is equivalent to } \exists x[M(x) \wedge \neg\exists y(F(x,y) \wedge H(y))] && \text{(De Morgan's law),} \\
&\text{which is equivalent to } \exists x[M(x) \wedge \forall y\neg(F(x,y) \wedge H(y))] && \text{(quantifier negation law),} \\
&\text{which is equivalent to } \exists x[M(x) \wedge \forall y(\neg F(x,y) \vee \neg H(y))] && \text{(De Morgan's law),} \\
&\text{which is equivalent to } \exists x[M(x) \wedge \forall y(F(x,y) \to \neg H(y))] && \text{(conditional law).}
\end{aligned}$$

   (b) Let $R(x, y)$ stand for "x and y are roommates" and $L(x, y)$ for "x likes y."

$$\begin{aligned}
&\neg\forall x\exists y(R(x,y) \wedge \forall z\neg L(y,z)) \\
&\qquad \text{is equivalent to } \exists x\neg\exists y(R(x,y) \wedge \forall z\neg L(y,z)) && \text{(quantifier negation law),} \\
&\text{which is equivalent to } \exists x\forall y\neg(R(x,y) \wedge \forall z\neg L(y,z)) && \text{(quantifier negation law),} \\
&\text{which is equivalent to } \exists x\forall y(\neg R(x,y) \vee \neg\forall z\neg L(y,z)) && \text{(De Morgan's law),} \\
&\text{which is equivalent to } \exists x\forall y(\neg R(x,y) \vee \exists z\neg\neg L(y,z)) && \text{(quantifier negation law),} \\
&\text{which is equivalent to } \exists x\forall y(\neg R(x,y) \vee \exists z L(y,z)) && \text{(double negation law),} \\
&\text{which is equivalent to } \exists x\forall y(R(x,y) \to \exists z L(y,z)) && \text{(conditional law).}
\end{aligned}$$

   (c)
$$\begin{aligned}
&\neg\forall x[(x \in A \vee x \in B) \to (x \in C \wedge x \notin D)] \\
&\qquad \text{is equivalent to } \exists x\neg[(x \in A \vee x \in B) \to (x \in C \wedge x \notin D)] && \text{(quantifier negation law),} \\
&\text{which is equivalent to } \exists x\neg[\neg(x \in A \vee x \in B) \vee (x \in C \wedge x \notin D)] && \text{(conditional law),} \\
&\text{which is equivalent to } \exists x[(x \in A \vee x \in B) \wedge \neg(x \in C \wedge x \notin D)] && \text{(De Morgan's law),} \\
&\text{which is equivalent to } \exists x[(x \in A \vee x \in B) \wedge (x \notin C \vee x \in D)] && \text{(De Morgan's law).}
\end{aligned}$$

   (d)
$$\begin{aligned}
&\neg\exists x\forall y[y > x \to \exists z(z^2 + 5z = y)] \\
&\qquad \text{is equivalent to } \forall x\neg\forall y[y > x \to \exists z(z^2 + 5z = y)] && \text{(quantifier negation law),} \\
&\text{which is equivalent to } \forall x\exists y\neg[y > x \to \exists z(z^2 + 5z = y)] && \text{(quantifier negation law),} \\
&\text{which is equivalent to } \forall x\exists y\neg[\neg(y > x) \vee \exists z(z^2 + 5z = y)] && \text{(conditional law),}
\end{aligned}$$

which is equivalent to $\forall x \exists y[y > x \wedge \neg \exists z(z^2 + 5z = y)]$ (De Morgan's law),
which is equivalent to $\forall x \exists y[y > x \wedge \forall z(z^2 + 5z \neq y)]$ (quantifier negation law).

2. (a) Let $F(x)$ stand for "x is in the freshman class" and $R(x, y)$ for "x and y are roommates."

$\neg \exists x(F(x) \wedge \neg \exists y R(x, y))$
is equivalent to $\forall x \neg(F(x) \wedge \neg \exists y R(x, y))$ (quantifier negation law),
which is equivalent to $\forall x(\neg F(x) \vee \exists y R(x, y))$ (De Morgan's law),
which is equivalent to $\forall x(F(x) \rightarrow \exists y R(x, y))$ (conditional law).

(b) Let $L(x, y)$ stand for "x likes y."

$\neg[\forall x \exists y L(x, y) \wedge \neg \exists x \forall y L(x, y)]$
is equivalent to $\neg \forall x \exists y L(x, y) \vee \exists x \forall y L(x, y)$ (De Morgan's law),
which is equivalent to $\exists x \forall y \neg L(x, y) \vee \exists x \forall y L(x, y)$ (quantifier negation laws).

(c) $\neg \forall a \in A \exists b \in B(a \in C \leftrightarrow b \in C)$
is equivalent to $\exists a \in A \forall b \in B \neg(a \in C \leftrightarrow b \in C)$ (quantifier negation laws),
which is equivalent to $\exists a \in A \forall b \in B \neg((a \in C \rightarrow b \in C) \wedge (b \in C \rightarrow a \in C))$ (meaning of biconditional),
which is equivalent to $\exists a \in A \forall b \in B \neg(\neg(a \in C \wedge b \notin C) \wedge \neg(b \in C \wedge a \notin C))$ (conditional law),
which is equivalent to $\exists a \in A \forall b \in B((a \in C \wedge b \notin C) \vee (b \in C \wedge a \notin C))$ (De Morgan's law).

(d) $\neg \forall y > 0 \exists x(ax^2 + bx + c = y)$ is equivalent to $\exists y > 0 \forall x(ax^2 + bx + c \neq y)$ by quantifier negation laws.

3. (a) True, because $0^2+0^2+0^2 = 0$, $1^2+0^2+0^2 = 1$, $1^2+1^2+0^2 = 2$, $1^2+1^2+1^2 = 3$, $2^2+0^2+0^2 = 4$, $2^2 + 1^2 + 0^2 = 5$, and $2^2 + 1^2 + 1^2 = 6$.

(b) False, because the equation has two solutions, $x = 1$ and $x = 3$.

(c) True, because $x = 5$ is the only natural number solution to the equation. ($x = -1$ is also a solution, but -1 is not a natural number.)

(d) True, because x and y can both be 5.

4. $\neg \forall x P(x)$ is equivalent to $\neg \forall x \neg \neg P(x)$ (double negation law),
which is equivalent to $\neg \neg \exists x \neg P(x)$ (first quantifier negation law),
which is equivalent to $\exists x \neg P(x)$ (double negation law).

5. $\neg \exists x \in A\, P(x)$ is equivalent to $\neg \exists x(x \in A \wedge P(x))$ (expanding abbreviation),
which is equivalent to $\forall x \neg(x \in A \wedge P(x))$ (quantifier negation law),
which is equivalent to $\forall x(x \notin A \vee \neg P(x))$ (De Morgan's law),
which is equivalent to $\forall x(x \in A \rightarrow \neg P(x))$ (conditional law),
which is equivalent to $\forall x \in A \neg P(x)$ (abbreviation).

6. $\exists x(P(x) \vee Q(x))$ is equivalent to $\neg \neg \exists x(P(x) \vee Q(x))$ (double negation law),
which is equivalent to $\neg \forall x \neg(P(x) \vee Q(x))$ (quantifier negation law),

which is equivalent to $\neg\forall x(\neg P(x) \wedge \neg Q(x))$ (De Morgan's law),
which is equivalent to $\neg(\forall x\neg P(x) \wedge \forall x\neg Q(x))$ (distributive law for $\forall$ and $\wedge$),
which is equivalent to $\neg\forall x\neg P(x) \vee \neg\forall x\neg Q(x)$ (De Morgan's law),
which is equivalent to $\neg\neg\exists x P(x) \vee \neg\neg\exists x Q(x)$ (quantifier negation law),
which is equivalent to $\exists x P(x) \vee \exists x Q(x)$ (double negation law).

7. $\exists x(P(x) \to Q(x))$ is equivalent to $\exists x(\neg P(x) \vee Q(x))$ (conditional law),
which is equivalent to $\exists x\neg P(x) \vee \exists x Q(x)$ (exercise 6),
which is equivalent to $\neg\forall x P(x) \vee \exists x Q(x)$ (quantifier negation law),
which is equivalent to $\forall x P(x) \to \exists x Q(x)$ (conditional law).

8. $(\forall x \in A\, P(x)) \wedge (\forall x \in B\, P(x))$
is equivalent to $\forall x(x \in A \to P(x)) \wedge \forall x(x \in B \to P(x))$ (expanding abbreviation),
which is equivalent to $\forall x[(x \in A \to P(x)) \wedge (x \in B \to P(x))]$ (distributive law),
which is equivalent to $\forall x[(x \notin A \vee P(x)) \wedge (x \notin B \vee P(x))]$ (conditional law),
which is equivalent to $\forall x[(x \notin A \wedge x \notin B) \vee P(x)]$ (distributive law),
which is equivalent to $\forall x[\neg(x \in A \vee x \in B) \vee P(x)]$ (De Morgan's law),
which is equivalent to $\forall x[x \notin (A \cup B) \vee P(x)]$ (definition of $\cup$),
which is equivalent to $\forall x[x \in (A \cup B) \to P(x)]$ (conditional law),
which is equivalent to $\forall x \in (A \cup B)\, P(x)$ (abbreviation).

9. No. For example, if the universe of discourse is $\mathbb{N}$, $P(x)$ stands for "x is even," and $Q(x)$ stands for "x is odd," then $\forall x(P(x) \vee Q(x))$ means "Every natural number is either even or odd," which is true, but $\forall x P(x) \vee \forall x Q(x)$ means "Either every natural number is even or every natural number is odd," which is false.

10. (a) $\exists x \in A\, P(x) \vee \exists x \in B\, P(x)$
is equivalent to $\exists x(x \in A \wedge P(x)) \vee \exists x(x \in B \wedge P(x))$ (expanding abbreviation),
which is equivalent to $\exists x[(x \in A \wedge P(x)) \vee (x \in B \wedge P(x))]$ (distributive law),
which is equivalent to $\exists x[(x \in A \vee x \in B) \wedge P(x)]$ (distributive law),
which is equivalent to $\exists x[x \in A \cup B \wedge P(x)]$ (definition of $\cup$),
which is equivalent to $\exists x \in A \cup B\, P(x)$ (abbreviation).

(b) No. Suppose A is the set of even natural numbers, B is the set of odd natural numbers, and $P(x)$ stands for "x is prime." Then $\exists x \in A\, P(x) \wedge \exists x \in B\, P(x)$ means "There is at least one even prime number and there is at least one odd prime number," which is true, but $\exists x \in A \cap B\, P(x)$ means "There is at least one number that is both even and odd and is prime," which is false.

11. $A \subseteq B$ means $\forall x(x \in A \to x \in B)$
which is equivalent to $\forall x(x \notin A \vee x \in B)$ (conditional law),
which is equivalent to $\forall x\neg(x \in A \wedge x \notin B)$ (De Morgan's law),
which is equivalent to $\neg\exists x(x \in A \wedge x \notin B)$ (quantifier negation law),
which is equivalent to $A \setminus B = \varnothing$ (definitions of $\setminus$, $\varnothing$).

12. $C \subseteq A \cup B$ means $\forall x(x \in C \to (x \in A \vee x \in B))$
which is equivalent to $\forall x(x \notin C \vee (x \in A \vee x \in B))$ (conditional law),
which is equivalent to $\forall x((x \notin C \vee x \in A) \vee x \in B)$ (associative law),

which is equivalent to $\forall x(\neg(x \in C \wedge x \notin A) \vee x \in B)$ (De Morgan's law),
which is equivalent to $\forall x((x \in C \wedge x \notin A) \to x \in B)$ (conditional law),
which is equivalent to $C \setminus A \subseteq B$ (definitions of $\setminus$, $\subseteq$).

13. (a) $A \subseteq B$ means $\forall x(x \in A \to x \in B)$
which is equivalent to $\forall x((x \in A \vee x \in B) \leftrightarrow x \in B)$ (Sec. 1.5, exercise 11(a)),
which is equivalent to $A \cup B = B$ (definition of $\cup$).

(b) $A \subseteq B$ means $\forall x(x \in A \to x \in B)$
which is equivalent to $\forall x((x \in A \wedge x \in B) \leftrightarrow x \in A)$ (Sec. 1.5, exercise 11(b)),
which is equivalent to $A \cap B = A$ (definition of $\cap$).

14. $A \cap B = \varnothing$ means $\neg\exists x(x \in A \wedge x \in B)$
which is equivalent to $\forall x\neg(x \in A \wedge x \in B)$ (quantifier negation law),
which is equivalent to $\forall x(x \notin A \vee x \notin B)$ (De Morgan's law),
which is equivalent to $\forall x(x \in A \to x \notin B)$ (conditional law),
which is equivalent to $\forall x((x \in A \wedge x \notin B) \leftrightarrow x \in A)$ (Sec. 1.5, exercise 11(b)),
which is equivalent to $A \setminus B = A$ (definition of $\setminus$).

15. None of these statements are equivalent to each other.
(a) x is a teacher of exactly one person; i.e., x is a teacher who has exactly one student.
(b) Someone is a teacher of exactly one person; i.e., some teacher has exactly one student.
(c) There is exactly one person who teaches someone; i.e., there is exactly one teacher.
(d) There is someone who is taught by exactly one person; i.e., some student has exactly one teacher.
(e) There is exactly one person who is a teacher of exactly one person; i.e., there is exactly one person who is a teacher with only one student (there may be other teachers with more students).
(f) There is exactly one pair of people, the first of whom is a teacher of the second; this is equivalent to saying that there is exactly one teacher, and that teacher has exactly one student.

Section 2.3

1. (a) $\forall x(x \in \mathcal{F} \to \forall y(y \in x \to y \in A))$.
(b) $\forall x(x \in A \to \exists n \in \mathbb{N}(x = 2n + 1))$.
(c) $\forall n \in \mathbb{N}\exists m \in \mathbb{N}(n^2 + n + 1 = 2m + 1)$.
(d) We work this out in several steps:
i. $\exists x(x \in \mathscr{P}(\bigcup_{i\in I} A_i) \wedge x \notin \bigcup_{i\in I} \mathscr{P}(A_i))$.
ii. $\exists x(x \subseteq \bigcup_{i\in I} A_i \wedge \forall i \in I(x \notin \mathscr{P}(A_i)))$.
iii. $\exists x(\forall y(y \in x \to y \in \bigcup_{i\in I} A_i) \wedge \forall i \in I(x \not\subseteq A_i))$.
iv. $\exists x(\forall y(y \in x \to \exists i \in I(y \in A_i)) \wedge \forall i \in I\exists y(y \in x \wedge y \notin A_i))$.
2. (a) $\exists A \in \mathcal{F}(x \in A) \wedge \forall B \in \mathcal{G}(x \notin B)$.
(b) $\forall x((x \in B \wedge x \notin C) \to x \in A)$.
(c) $\forall i \in I(x \in A_i \vee x \in B_i)$.
(d) $\forall i \in I(x \in A_i) \vee \forall i \in I(x \in B_i)$.
3. $\mathscr{P}(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$.

4. $\bigcap \mathcal{F} = \{\text{red, green, blue}\} \cap \{\text{orange, red, blue}\} \cap \{\text{purple, red, green, blue}\} = \{\text{red, blue}\}$. $\bigcup \mathcal{F} = \{\text{red, green, blue}\} \cup \{\text{orange, red, blue}\} \cup \{\text{purple, red, green, blue}\} = \{\text{red, green, blue, orange, purple}\}$.

5. $\bigcap \mathcal{F} = \{3,7,12\} \cap \{5,7,16\} \cap \{5,12,23\} = \varnothing$.
$\bigcup \mathcal{F} = \{3,7,12\} \cup \{5,7,16\} \cup \{5,12,23\} = \{3,5,7,12,16,23\}$.

6. (a) $A_2 = \{2,3,1,4\}$, $A_3 = \{3,4,2,6\}$, $A_4 = \{4,5,3,8\}$, $A_5 = \{5,6,4,10\}$.
   (b) $\bigcap_{i\in I} A_i = A_2 \cap A_3 \cap A_4 \cap A_5 = \{2,3,1,4\} \cap \{3,4,2,6\} \cap \{4,5,3,8\} \cap \{5,6,4,10\} = \{4\}$. $\bigcup_{i\in I} A_i = A_2 \cup A_3 \cup A_4 \cup A_5 = \{2,3,1,4\} \cup \{3,4,2,6\} \cup \{4,5,3,8\} \cup \{5,6,4,10\} = \{1,2,3,4,5,6,8,10\}$.

7. $A_{1750} = \{\text{Johann Sebastian Bach, Johann Wolfgang von Goethe, David Hume, George Washington}\}$. $A_{1751} = A_{1752} = A_{1753} = A_{1754} = A_{1755} = \{\text{Johann Wolfgang von Goethe, David Hume, George Washington}\}$. $A_{1756} = A_{1757} = A_{1758} = A_{1759} = \{\text{Johann Wolfgang von Goethe, David Hume, Wolfgang Amadeus Mozart, George Washington}\}$. Therefore $\bigcup_{y\in Y} A_y = \{\text{Johann Sebastian Bach, Johann Wolfgang von Goethe, David Hume, Wolfgang Amadeus Mozart, George Washington}\}$ and $\bigcap_{y\in Y} A_y = \{\text{Johann Wolfgang von Goethe, David Hume, George Washington}\}$.

8. (a) $A_2 = \{2,4\}$, $A_3 = \{3,6\}$, $B_2 = \{2,3\}$, $B_3 = \{3,4\}$.
   (b) $\bigcap_{i\in I}(A_i \cup B_i) = (A_2 \cup B_2) \cap (A_3 \cup B_3) = \{2,3,4\} \cap \{3,4,6\} = \{3,4\}$,
   $(\bigcap_{i\in I} A_i) \cup (\bigcap_{i\in I} B_i) = (A_2 \cap A_3) \cup (B_2 \cap B_3) = \varnothing \cup \{3\} = \{3\}$.
   (c) They are not equivalent.

9. (a) $x \in \bigcup_{i\in I}(A_i \setminus B_i)$ means $\exists i \in I(x \in A_i \wedge x \notin B_i)$,
   $x \in (\bigcup_{i\in I} A_i) \setminus (\bigcup_{i\in I} B_i)$ means $\exists i \in I(x \in A_i) \wedge \neg\exists i \in I(x \in B_i)$,
   $x \in (\bigcup_{i\in I} A_i) \setminus (\bigcap_{i\in I} B_i)$ means $\exists i \in I(x \in A_i) \wedge \neg\forall i \in I(x \in B_i)$.
   (b) $\bigcup_{i\in I}(A_i \setminus B_i) = (A_2 \setminus B_2) \cup (A_3 \setminus B_3) = \{4\} \cup \{6\} = \{4,6\}$,
   $(\bigcup_{i\in I} A_i) \setminus (\bigcup_{i\in I} B_i) = (A_2 \cup A_3) \setminus (B_2 \cup B_3) = \{2,3,4,6\} \setminus \{2,3,4\} = \{6\}$,
   $(\bigcup_{i\in I} A_i) \setminus (\bigcap_{i\in I} B_i) = (A_2 \cup A_3) \setminus (B_2 \cap B_3) = \{2,3,4,6\} \setminus \{3\} = \{2,4,6\}$.
   None of the statements are equivalent.

10. One example is $I = \{1,2\}$, $A_1 = \{a,b\}$, $A_2 = \{c,d\}$, $B_1 = \{a,e\}$, $B_2 = \{b,f\}$.

$$\bigcup_{i\in I}(A_i \cap B_i) = (A_1 \cap B_1) \cup (A_2 \cap B_2) = \{a\} \cup \varnothing = \{a\},$$
$$(\bigcup_{i\in I} A_i) \cap (\bigcup_{i\in I} B_i) = (A_1 \cup A_2) \cap (B_1 \cup B_2) = \{a,b,c,d\} \cap \{a,b,e,f\} = \{a,b\}.$$

11. $x \in \mathscr{P}(A \cap B)$ is equivalent to $\forall y(y \in x \to (y \in A \wedge y \in B))$ (Example 2.3.3, 4),
which is equivalent to $\forall y(y \notin x \vee (y \in A \wedge y \in B))$ (conditional law),
which is equivalent to $\forall y((y \notin x \vee y \in A) \wedge (y \notin x \vee y \in B))$ (distributive law),
which is equivalent to $\forall y((y \in x \to y \in A) \wedge (y \in x \to y \in B))$ (conditional law),
which is equivalent to $\forall y(y \in x \to y \in A) \wedge \forall y(y \in x \to y \in B)$ (distributive law),
which is equivalent to $x \in \mathscr{P}(A) \cap \mathscr{P}(B)$ (Example 2.3.3, 5).

12. One example is $A = \{1,2\}$ and $B = \{2,3\}$.

$$\mathscr{P}(A \cup B) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\},$$
$$\mathscr{P}(A) \cup \mathscr{P}(B) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2.3\}\}.$$

13. (a) $x \in \bigcup_{i\in I}(A_i \cup B_i)$ means $\exists i \in I(x \in A_i \vee x \in B_i)$
which is equivalent to $\exists i \in I(x \in A_i) \vee \exists i \in I(x \in B_i)$ (distributive law),
which is equivalent to $x \in (\bigcup_{i\in I} A_i) \cup (\bigcup_{i\in I} B_i)$ (definitions of $\bigcup$, $\cup$).

(b) $x \in (\bigcap \mathcal{F}) \cap (\bigcap \mathcal{G})$ means $\forall A \in \mathcal{F}(x \in A) \wedge \forall A \in \mathcal{G}(x \in A)$
which is equivalent to $\forall A \in \mathcal{F} \cup \mathcal{G}(x \in A)$ (Sec. 2.2, exercise 8),
which is equivalent to $x \in \bigcap(\mathcal{F} \cup \mathcal{G})$ (Definition of $\bigcap$).

(c) $x \in \bigcap_{i \in I}(A_i \setminus B_i)$ means $\forall i \in I(x \in A_i \wedge x \notin B_i)$
which is equivalent to $\forall i \in I(x \in A_i) \wedge \forall i \in I(x \notin B_i)$ (distributive law),
which is equivalent to $\forall i \in I(x \in A_i) \wedge \neg\exists i \in I(x \in B_i)$ (quantifier negation law),
which is equivalent to $x \in (\bigcap_{i \in I} A_i) \setminus (\bigcup_{i \in I} B_i)$ (Definitions of $\bigcap$, $\bigcup$, $\setminus$).

14. (a) $B_3 = A_{1,3} \cup A_{2,3} = \{1,3,4\} \cup \{2,3,5\} = \{1,2,3,4,5\}$,
$B_4 = A_{1,4} \cup A_{2,4} = \{1,4,5\} \cup \{2,4,6\} = \{1,2,4,5,6\}$.
(b) $\bigcap_{j \in J} B_j = B_3 \cap B_4 = \{1,2,4,5\}$.
(c) For each $i \in I$, let $C_i = \bigcap_{j \in J} A_{i,j}$. Then

$$C_1 = A_{1,3} \cap A_{1,4} = \{1,3,4\} \cap \{1,4,5\} = \{1,4\},$$
$$C_2 = A_{2,3} \cap A_{2,4} = \{2,3,5\} \cap \{2,4,6\} = \{2\},$$
$$\bigcup_{i \in I}(\bigcap_{j \in J} A_{i,j}) = \bigcup_{i \in I} C_i = C_1 \cup C_2 = \{1,2,4\}.$$

This is not equal to the set in part (b).
(d) $x \in \bigcap_{j \in J}(\bigcup_{i \in I} A_{i,j})$ means $\forall j \in J \exists i \in I(x \in A_{i,j})$ and $x \in \bigcup_{i \in I}(\bigcap_{j \in J} A_{i,j})$ means $\exists i \in I \forall j \in J(x \in A_{i,j})$. They are not equivalent.

15. (a) $x \in \bigcup \mathcal{F}$ means $\exists A \in \mathcal{F}(x \in A)$. If $\mathcal{F} = \varnothing$ then this statement will be false, no matter what x is, because there is no set $A \in \mathcal{F}$.
(b) $x \in \bigcap \mathcal{F}$ means $\forall A \in \mathcal{F}(x \in A)$. If $\mathcal{F} = \varnothing$ then this statement will be vacuously true, no matter what x is.

16. (a) Since U is the set of all sets and R is a set, $R \in U$. Since $\forall A \in U(A \in R \leftrightarrow A \notin A)$, we conclude that $R \in R \leftrightarrow R \notin R$. But this is impossible, since the formula $P \leftrightarrow \neg P$ is a contradiction (make a truth table).
(b) We could rephrase the reasoning in part (a) as follows: Suppose U is any set whose elements are sets. Let $R = \{A \in U \mid A \notin A\}$. Then $\forall A \in U(A \in R \leftrightarrow A \notin A)$. If $R \in U$ then, as in part (a), we conclude that $R \in R \leftrightarrow R \notin R$, which is impossible. Therefore $R \notin U$. What this rephrasing of the proof shows is that if U is any set whose elements are sets, then we can come up with a set R such that $R \notin U$. Thus, U could not have been the set of all sets. Many mathematicians interpret this as meaning that there cannot be a set of all sets.

Chapter 3

Section 3.1

1. (a) Hypotheses: n is an integer larger than 1 and n is not prime. Conclusion: $2^n - 1$ is not prime. The hypotheses are true when $n = 6$, so the theorem tells us that $2^6 - 1$ is not prime. This is correct, since $2^6 - 1 = 63 = 9 \cdot 7$.
(b) We can conclude that 32767 is not prime. This is correct, since $32767 = 151 \cdot 217$.
(c) The theorem tells us nothing; 11 is prime, so the hypotheses are not satisfied.

2. (a) Hypothesis: $b^2 > 4ac$. Conclusion: The quadratic equation $ax^2 + bx + c = 0$ has exactly two real solutions.

(b) Because a, b, and c are free variables in the hypothesis and conclusion, but x is not.

(c) $b^2 = 25 > 24 = 4ac$, so we can conclude that the equation $2x^2 - 5x + 3$ has exactly two real solutions. This is correct; the solutions are $x = 3/2$ and $x = 1$.

(d) $b^2 = 16 < 24 = 4ac$, so the hypothesis is not true and we cannot conclude anything.

3. Hypotheses: n is a natural number, $n > 2$, and n is not prime. Conclusion: $2n + 13$ is not prime. One counterexample is $n = 8$.

4. Suppose $0 < a < b$. Then $b - a > 0$. Multiplying both sides by the positive number $b + a$, we get $(b + a) \cdot (b - a) > (b + a) \cdot 0$, or in other words $b^2 - a^2 > 0$. Since $b^2 - a^2 > 0$, it follows that $a^2 < b^2$. Therefore if $0 < a < b$ then $a^2 < b^2$.

5. Suppose $a < b < 0$. Multiplying the inequality $a < b$ by the negative number a (and reversing the direction of the inequality) we can conclude that $a^2 > ab$, and similarly multiplying by b we get $ab > b^2$. Therefore $a^2 > ab > b^2$, so $a^2 > b^2$, as required. Thus, if $a < b < 0$ then $a^2 > b^2$.

6. Suppose $0 < a < b$. Dividing the inequality $a < b$ by the positive number ab, we get

$$\frac{1}{b} = \frac{a}{ab} < \frac{b}{ab} = \frac{1}{a}.$$

Thus, if $0 < a < b$ then $1/b < 1/a$.

7. Suppose $a^3 > a$. Then $a^3 - a > 0$. Multiplying this inequality by the positive number $a^2 + 1$, we get

$$a^5 - a = (a^3 - a)(a^2 + 1) > 0 \cdot (a^2 + 1) = 0,$$

so $a^5 > a$. Thus, if $a^3 > a$ then $a^5 > a$.

8. We will prove the contrapositive. Suppose $x \notin B$. Then since $x \in A$, it follows that $x \in A \setminus B$. But we also know that $A \setminus B \subseteq C \cap D$, so we can conclude that $x \in C \cap D$, and therefore $x \in D$. Thus, if $x \notin D$ then $x \in B$.

9. Suppose $x \in A$. To prove that if $x \in D$ then $x \notin B$ we will prove the contrapositive, so suppose $x \in B$. Then since $x \in A$ and $x \in B$, $x \in A \cap B$, and since $A \cap B \subseteq C \setminus D$, we can conclude that $x \in C \setminus D$, and therefore $x \notin D$. Thus, if $x \in D$ then $x \notin B$. Therefore if $x \in A$, then if $x \in D$ then $x \notin B$.

10. Suppose $a < b$. Adding b to both sides of this inequality we get $a + b < 2b$, and then dividing by 2 we conclude that $(a + b)/2 < b$. Therefore if $a < b$ then $(a + b)/2 < b$.

11. We prove the contrapositive. Suppose $x = 8$. Then

$$\frac{\sqrt[3]{x} + 5}{x^2 + 6} = \frac{7}{70} = \frac{1}{10} \neq \frac{1}{8} = \frac{1}{x}.$$

Thus, if $(\sqrt[3]{x} + 5)/(x^2 + 6) = 1/x$ then $x \neq 8$.

12. We will prove the contrapositive. Suppose $c \leq d$. Multiplying both sides of this inequality by the positive number a, we get $ac \leq ad$. Also, multiplying both sides of the given inequality $a < b$ by the positive number d gives us $ad < bd$. Combining $ac \leq ad$ and $ad < bd$, we can conclude that $ac < bd$. Thus, if $ac \geq bd$ then $c > d$.

13. Suppose $x > 1$. Then $3x > 3$, so $3x + 2y > 3 + 2y$. Combining this with the fact that $3x + 2y \leq 5$, we conclude that $3 + 2y < 5$. Therefore $2y < 2$, so $y < 1$. Thus, if $x > 1$ then $y < 1$.

14. Suppose $x^2 + y = -3$ and $2x - y = 2$. Adding these equations, we get $x^2 + 2x = -1$, so $x^2 + 2x + 1 = 0$. We can rewrite this as $(x + 1)^2 = 0$, so $x + 1 = 0$, and therefore $x = -1$. Thus, if $x^2 + y = -3$ and $2x - y = 2$ then $x = -1$.

15. Since $x > 3 > 0$, by the theorem in Example 3.2.1, $x^2 > 9$. Also, multiplying both sides of the given inequality $y < 2$ by -2 (and reversing the direction of the inequality, since -2 is negative) we get $-2y > -4$. Finally, adding the inequalities $x^2 > 9$ and $-2y > -4$ gives us $x^2 - 2y > 5$.

16. (a) The reasoning is backwards. The proof proves that if $x = 7$ then $(2x - 5)/(x - 4) = 3$, not that if $(2x - 5)/(x - 4) = 3$ then $x = 7$.

    (b) Suppose $(2x - 5)/(x - 4) = 3$. Multiplying both sides of this equation by $x - 4$, we conclude that $2x - 5 = 3(x - 4) = 3x - 12$. Subtracting $2x$ from both sides we get $-5 = x - 12$, and finally adding 12 to both sides gives us $7 = x$. Thus, if $(2x - 5)/(x - 4) = 3$ then $x = 7$.

17. (a) The mistake is the step "Since $x \neq 3$, $x^2 \neq 9$." If $x = -3$ then $x \neq 3$, but $x^2 = 9$, so this step is incorrect.

    (b) One counterexample is $x = -3$, $y = 1$.

Section 3.2

1. (a) Suppose P. Since $P \to Q$, it follows that Q. But then, since $Q \to R$, we can conclude R. Thus, $P \to R$.

    (b) Suppose P. To prove that $Q \to R$, we will prove the contrapositive, so suppose $\neg R$. Since $\neg R \to (P \to \neg Q)$, it follows that $P \to \neg Q$, and since we know P, we can conclude $\neg Q$. Thus, $Q \to R$, so $P \to (Q \to R)$.

2. (a) Suppose P. Since $P \to Q$, it follows that Q. But then since $R \to \neg Q$, we can conclude that $\neg R$. Thus, $P \to \neg R$.

    (b) Suppose Q. If we assume $Q \to \neg P$, then we can conclude $\neg P$, which contradicts the given information that P. Therefore $\neg(Q \to \neg P)$. Thus, $Q \to \neg(Q \to \neg P)$.

3. Suppose $x \in A$. Since $A \subseteq C$, $x \in C$. But then since B and C are disjoint, it follows that $x \notin B$. Thus, if $x \in A$ then $x \notin B$.

4. Suppose $x \in C$. Suppose $x \notin B$. Since $x \in A$ and $x \notin B$, $x \in A \setminus B$. But then since $x \in C$, this contradicts the fact that $A \setminus B$ and C are disjoint. Therefore $x \in B$. Thus, if $x \in C$ then $x \in B$.

5. Suppose $x \in A \setminus B$ and $x \in B \setminus C$. Since $x \in A \setminus B$, $x \in A$ and $x \notin B$, and since $x \in B \setminus C$, $x \in B$ and $x \notin C$. But now we have $x \in B$ and $x \notin B$, which is a contradiction. Therefore it cannot be the case that $x \in A \setminus B$ and $x \in B \setminus C$.

6. Suppose $a \in A \setminus B$. This means that $a \in A$ and $a \notin B$. Since $a \in A$ and $a \in C$, $a \in A \cap C$. But then since $A \cap C \subseteq B$, it follows that $a \in B$, and this contradicts the fact that $a \notin B$. Thus, $a \notin A \setminus B$.

7. Suppose $a \notin C$. Since $a \in A$ and $A \subseteq B$, $a \in B$. Since $a \in B$ and $a \notin C$, $a \in B \setminus C$, which contradicts the given information that $a \notin B \setminus C$. Therefore $a \in C$.

8. Suppose $y = 0$. Substituting into the equation $y + x = 2y - x$, we get $x = -x$. Therefore $2x = 0$, so $x = 0$. But this contradicts the given information that x and y are not both zero. Therefore $y \neq 0$.

9. Suppose $a < 1/a < b < 1/b$. Suppose $a \geq 1$. Dividing this inequality by the positive number a, we get $1 \geq 1/a$, and combining the inequalities $a \geq 1$ and $1 \geq 1/a$ we can conclude that $a \geq 1/a$, contradicting the fact that $a < 1/a$. Thus, $a < 1$. Next, suppose that $a > 0$. Then dividing $a < 1$ by a we get $1 < 1/a$, and since $1/a < b$ it follows that $b > 1$. Dividing by b gives us $1 > 1/b$, and together with $b > 1$ this implies that $b > 1/b$, contradicting the fact that $b < 1/b$. We conclude that $a \leq 0$. But we know that a is nonzero, so in fact $a < 0$.

    We are now finally ready to prove that $a < -1$. Suppose that $a \geq -1$. Dividing by the positive number $-a$, we conclude that $-1 \geq 1/a$. Combining $a \geq -1$ and $-1 \geq 1/a$ we get $a \geq 1/a$, contradicting the fact that $a < 1/a$. Therefore $a < -1$.

10. Suppose $x^2y = 2x + y$. To prove that if $y \neq 0$ then $x \neq 0$, we will prove the contrapositive. Suppose $x = 0$. Substituting into the equation $x^2y = 2x + y$ we get $0 = 0 + y = y$. Thus, if $y \neq 0$ then $x \neq 0$. This proves that if $x^2y = 2x + y$, then if $y \neq 0$ then $x \neq 0$.

11. Suppose $x \neq 0$. Suppose $y = (3x^2 + 2y)/(x^2 + 2)$. Multiplying by $x^2 + 2$, we get $x^2y + 2y = 3x^2 + 2y$, and therefore $x^2y = 3x^2$. Since $x \neq 0$, $x^2 \neq 0$, so we can divide both sides by x^2 to conclude that $y = 3$. Thus, if $x \neq 0$, then if $y = (3x^2 + 2y)/(x^2 + 2)$ then $y = 3$.

12. (a) The sentence "Then $x = 3$ and $y = 8$" is incorrect. The assumption that the conclusion is false means $\neg((x \neq 3) \wedge (y \neq 8))$, and by one of De Morgan's laws this is equivalent to $(x = 3) \vee (y = 8)$. So the sentence should say "Then $x = 3$ or $y = 8$," not "Then $x = 3$ and $y = 8$."

    (b) One counterexample is $x = 3$, $y = 7$.

13. (a) The sentence "Since $x \notin B$ and $B \subseteq C$, $x \notin C$" is incorrect. It is possible to have $x \notin B$ and $B \subseteq C$, but $x \in C$.

    (b) One counterexample is $A = \{1\}$, $B = \{2\}$, $C = \{1, 2\}$, and $x = 1$.

14.

		Premises		Conclusion
P	Q	$P \to Q$	$\neg Q$	$\neg P$
F	F	T	T	T
F	T	T	F	T
T	F	F	T	F
T	T	T	F	F

15.

			Premise	Conclusion
P	Q	R	$P \to (Q \to R)$	$\neg R \to (P \to \neg Q)$
F	F	F	T	T
F	F	T	T	T
F	T	F	T	T
F	T	T	T	T
T	F	F	T	T
T	F	T	T	T
T	T	F	F	F
T	T	T	T	T

16. (a)

			Premises		Conclusion
P	Q	R	$P \to Q$	$Q \to R$	$P \to R$
F	F	F	T	T	T
F	F	T	T	T	T
F	T	F	T	F	T
F	T	T	T	T	T
T	F	F	F	T	F
T	F	T	F	T	T
T	T	F	T	F	F
T	T	T	T	T	T

    (b) The truth table is the same as the one for exercise 15, but with the premise and conclusion reversed.

17. (a)

			Premises		Conclusion
P	Q	R	$P \to Q$	$R \to \neg Q$	$P \to \neg R$
F	F	F	T	T	T
F	F	T	T	T	T
F	T	F	T	T	T
F	T	T	T	F	T
T	F	F	F	T	T
T	F	T	F	T	F
T	T	F	T	T	T
T	T	T	T	F	F

(b)

		Premise	Conclusion
P	Q	P	$Q \to \neg(Q \to \neg P)$
F	F	F	T
F	T	F	F
T	F	T	T
T	T	T	T

18. No. Here is a counterexample to the proposed theorem: $x = -3$, $y = 4$.

Section 3.3

1. Suppose $\exists x(P(x) \to Q(x))$. Then we can choose some x_0 such that $P(x_0) \to Q(x_0)$. Now suppose that $\forall x P(x)$. Then in particular, $P(x_0)$, and since $P(x_0) \to Q(x_0)$, it follows that $Q(x_0)$. Since we have found a particular value of x for which $Q(x)$ holds, we can conclude that $\exists x Q(x)$. Thus $\forall x P(x) \to \exists x Q(x)$.
2. Suppose A and $B \setminus C$ are disjoint. Let x be an arbitrary element of $A \cap B$. Then $x \in A$ and $x \in B$. Suppose $x \notin C$. Then since $x \in B$ and $x \notin C$, $x \in B \setminus C$. But we also have $x \in A$, so this contradicts the fact that A and $B \setminus C$ are disjoint. Therefore $x \in C$. Since x was arbitrary, we can conclude that $A \cap B \subseteq C$.
3. Suppose that $A \subseteq B \setminus C$, but A and C are not disjoint. Then we can choose some x such that $x \in A$ and $x \in C$. Since $x \in A$ and $A \subseteq B \setminus C$, it follows that $x \in B \setminus C$, which means that $x \in B$ and $x \notin C$. But now we have both $x \in C$ and $x \notin C$, which is a contradiction. Thus, if $A \subseteq B \setminus C$ then A and C are disjoint.
4. Let X be an arbitrary element of $\mathscr{P}(A)$. Then $X \subseteq A$. Suppose $x \in X$. Then since $X \subseteq A$, $x \in A$, and therefore since $A \subseteq \mathscr{P}(A)$, $x \in \mathscr{P}(A)$. Since x was arbitrary, it follows that $X \subseteq \mathscr{P}(A)$, so $X \in \mathscr{P}(\mathscr{P}(A))$. Since X was arbitrary, we can conclude that $\mathscr{P}(A) \subseteq \mathscr{P}(\mathscr{P}(A))$.
5. (a) The easiest example is $A = \varnothing$.
   (b) By exercise 4, another example is $A = \mathscr{P}(\varnothing) = \{\varnothing\}$.
6. (a) Suppose $x \neq 1$. Let $y = (2x+1)/(x-1)$, which is defined since $x \neq 1$. Then
$$\frac{y+1}{y-2} = \frac{\frac{2x+1}{x-1} + 1}{\frac{2x+1}{x-1} - 2} = \frac{\frac{3x}{x-1}}{\frac{3}{x-1}} = x.$$
   (b) Suppose y is a real number such that $(y+1)/(y-2) = x$. Suppose $x = 1$. Then $(y+1)/(y-2) = 1$, so $y + 1 = y - 2$, and therefore $1 = -2$, which is a contradiction. Therefore $x \neq 1$.
7. Suppose $x > 2$. Let $y = (x + \sqrt{x^2-4})/2$, which is defined since $x^2 - 4 > 0$. Then
$$y + \frac{1}{y} = \frac{x + \sqrt{x^2-4}}{2} + \frac{2}{x + \sqrt{x^2-4}} = \frac{2x^2 + 2x\sqrt{x^2-4}}{2(x + \sqrt{x^2-4})} = \frac{2x(x + \sqrt{x^2-4})}{2(x + \sqrt{x^2-4})} = x.$$

8. Suppose $\mathcal{F}$ is a family of sets and $A \in \mathcal{F}$. Let x be an arbitrary element of A. By the definition of $\bigcup \mathcal{F}$, since $x \in A$ and $A \in \mathcal{F}$, $x \in \bigcup \mathcal{F}$. Since x was an arbitrary element of A, it follows that $A \subseteq \bigcup \mathcal{F}$.

9. Suppose $\mathcal{F}$ is a family of sets and $A \in \mathcal{F}$. Suppose $x \in \bigcap \mathcal{F}$. Then by the definition of $\bigcap \mathcal{F}$, since $x \in \bigcap \mathcal{F}$ and $A \in \mathcal{F}$, $x \in A$. But x was an arbitrary element of $\bigcap \mathcal{F}$, so it follows that $\bigcap \mathcal{F} \subseteq A$.

10. Let x be an arbitrary element of B. Suppose $C \in \mathcal{F}$. By assumption, $\forall A \in \mathcal{F}(B \subseteq A)$, so $B \subseteq C$. Since $x \in B$, it follows that $x \in C$. But C was an arbitrary element of $\mathcal{F}$, so it follows that $\forall C \in \mathcal{F}(x \in C)$, and therefore $x \in \bigcap \mathcal{F}$. Since x was an arbitrary element of B, we can conclude that $B \subseteq \bigcap \mathcal{F}$.

11. Suppose $\varnothing \in \mathcal{F}$. Suppose $\bigcap \mathcal{F} \neq \varnothing$. Then we can choose some x such that $x \in \bigcap \mathcal{F}$. By the definition of $\bigcap \mathcal{F}$, since $x \in \bigcap \mathcal{F}$ and $\varnothing \in \mathcal{F}$, $x \in \varnothing$. But this is a contradiction, since $\varnothing$ has no elements. Therefore $\bigcap \mathcal{F} = \varnothing$.

12. Suppose $\mathcal{F} \subseteq \mathcal{G}$, and let x be an arbitrary element of $\bigcup \mathcal{F}$. By the definition of $\bigcup \mathcal{F}$, this means that we can choose a set $A \in \mathcal{F}$ such that $x \in A$. Since $A \in \mathcal{F}$ and $\mathcal{F} \subseteq \mathcal{G}$, $A \in \mathcal{G}$. Since $x \in A$ and $A \in \mathcal{G}$, $x \in \bigcup \mathcal{G}$. But x was an arbitrary element of $\bigcup \mathcal{F}$, so we can conclude that $\bigcup \mathcal{F} \subseteq \bigcup \mathcal{G}$.

13. Suppose $\mathcal{F} \subseteq \mathcal{G}$, and let x be an arbitrary element of $\bigcap \mathcal{G}$. Suppose $A \in \mathcal{F}$. Since $\mathcal{F} \subseteq \mathcal{G}$, it follows that $A \in \mathcal{G}$. By the definition of $\bigcap \mathcal{G}$, since $x \in \bigcap \mathcal{G}$ and $A \in \mathcal{G}$, $x \in A$. Since A was an arbitrary element of $\mathcal{F}$, we conclude that $\forall A \in \mathcal{F}(x \in A)$, which means $x \in \bigcap \mathcal{F}$. Since x was an arbitrary element of $\bigcap \mathcal{G}$, this shows that $\bigcap \mathcal{G} \subseteq \bigcap \mathcal{F}$.

14. Suppose $x \in \bigcup_{i \in I} \mathscr{P}(A_i)$. Then we can choose some $i \in I$ such that $x \in \mathscr{P}(A_i)$, or in other words $x \subseteq A_i$. Now let a be an arbitrary element of x. Then $a \in A_i$, and therefore $a \in \bigcup_{i \in I} A_i$. Since a was an arbitrary element of x, it follows that $x \subseteq \bigcup_{i \in I} A_i$, which means that $x \in \mathscr{P}(\bigcup_{i \in I} A_i)$. Thus $\bigcup_{i \in I} \mathscr{P}(A_i) \subseteq \mathscr{P}(\bigcup_{i \in I} A_i)$.

15. Suppose $i \in I$. Let x be an arbitrary element of $\bigcap_{i \in I} A_i$. Then $x \in A_i$. Since x was an arbitrary element of $\bigcap_{i \in I} A_i$, it follows that $\bigcap_{i \in I} A_i \subseteq A_i$, and therefore $\bigcap_{i \in I} A_i \in \mathscr{P}(A_i)$. Since i was arbitrary, we conclude that $\bigcap_{i \in I} A_i \in \bigcap_{i \in A} \mathscr{P}(A_i)$.

16. Suppose $\mathcal{F} \subseteq \mathscr{P}(B)$. Let y be an arbitrary element of $\bigcup \mathcal{F}$. Then we can choose some $x \in \mathcal{F}$ such that $y \in x$. Since $x \in \mathcal{F}$ and $\mathcal{F} \subseteq \mathscr{P}(B)$, $x \in \mathscr{P}(B)$, which means that $x \subseteq B$. Since $y \in x$ and $x \subseteq B$, $y \in B$. But y was an arbitrary element of $\bigcup \mathcal{F}$, so we can conclude that $\bigcup \mathcal{F} \subseteq B$.

17. Suppose $x \in \bigcup \mathcal{F}$. Then we can choose some $A \in \mathcal{F}$ such that $x \in A$. Let B be an arbitrary element of $\mathcal{G}$. Since every element of $\mathcal{F}$ is a subset of every element of $\mathcal{G}$, $A \subseteq B$. Since $x \in A$, it follows that $x \in B$. But B was an arbitrary element of $\mathcal{G}$, so we can conclude that $\forall B \in \mathcal{G}(x \in B)$, which means that $x \in \bigcap \mathcal{G}$. Thus, $\bigcup \mathcal{F} \subseteq \bigcap \mathcal{G}$.

18. (a) Suppose $a \mid b$ and $a \mid c$. Then we can choose integers j and k such that $ja = b$ and $ka = c$. Therefore $b + c = ja + ka = (j + k)a$. Since $j + k$ is an integer, this shows that $a \mid (b + c)$.

    (b) Suppose $ac \mid bc$ and $c \neq 0$. Since $ac \mid bc$, we can choose some integer k such that $kac = bc$. Since $c \neq 0$, we can divide both sides of this equation by c to conclude that $ka = b$, and therefore $a \mid b$.

19. (a) Let x and y be arbitrary real numbers. Let $z = (y - x)/2$. Then

$$x + z = x + \frac{y - x}{2} = \frac{y + x}{2} = y - \frac{y - x}{2} = y - z.$$

    (b) No. For example, if $x = 1$ and $y = 2$, then the only value of z that would make the equation $x + z = y - z$ true is $z = 1/2$, which is not an integer.

20. The sentence "Then for every real number x, $x^2 < 0$" is incorrect. The assumption that the conclusion is false means $\neg \forall x(x^2 \geq 0)$, which is equivalent to $\exists x(x^2 < 0)$. So the sentence should say "Then for some real number x, $x^2 < 0$," not "Then for every real number x, $x^2 < 0$."

21. (a) In the second sentence of the proof, x was introduced as an arbitrary element of A, not an arbitrary element of B, so it is incorrect to conclude at the end of the proof that $\forall x \in B(x \neq 0)$. To prove this goal, x would have to be introduced with the sentence "Let x be an arbitrary element of B."
    (b) One counterexample is $A = \{1\}$, $B = \{0, 1\}$.

22. Based on the logical form of the statement to be proven, the proof should have this outline:

    Let $x = \ldots$.
      Let y be an arbitrary real number.
        [Proof of $xy^2 = y - x$ goes here.]
      Since y was arbitrary, $\forall y \in \mathbb{R}(xy^2 = y - x)$.
    Thus, $\exists x \in \mathbb{R} \forall y \in \mathbb{R}(xy^2 = y - x)$.

    This outline makes it clear that y should be introduced into the proof *after* x. Therefore, x cannot be defined in terms of y, because y will not yet have been introduced into the proof when x is being defined. But in the given proof, x is defined in terms of y in the first sentence. (The mistake has been disguised by the fact that the sentence "Let y be an arbitrary real number" has been left out of the proof. If you try to add this sentence to the proof, you will find that there is nowhere it could be added that would lead to a correct proof of the incorrect theorem.)

23. (a) The mistake is in the sentence "But then every element of A is in both $\bigcup \mathcal{F}$ and $\bigcup \mathcal{G}$, and this is impossible since $\bigcup \mathcal{F}$ and $\bigcup \mathcal{G}$ are disjoint." If A is the empty set then it will be vacuously true that every element of A is in both $\bigcup \mathcal{F}$ and $\bigcup \mathcal{G}$, but $\bigcup \mathcal{F}$ and $\bigcup \mathcal{G}$ could still be disjoint.
    (b) One counterexample is $\mathcal{F} = \{\varnothing, \{1\}\}$, $\mathcal{G} = \{\varnothing, \{2\}\}$.

24. (a) The proof assumes that the values of x and y are the same, but they might not be.
    (b) The theorem is incorrect. One counterexample is $x = 1$, $y = 0$.

25. Let x be an arbitrary real number. Let $y = 2x$. Now let z be an arbitrary real number. Then

$$(x + z)^2 - (x^2 + z^2) = (x^2 + 2xz + z^2) - (x^2 + z^2) = 2xz = yz.$$

26. (a) Goal of the form $\forall x P(x)$ and given of the form $\exists x P(x)$: In both cases you introduce a new variable x into the proof, but you don't specify the value of x. Goal of the form $\exists x P(x)$ and given of the form $\forall x P(x)$: In both cases you specify a value to be assigned to x in the statement $P(x)$.
    (b) If you are proving the goal $\forall x P(x)$ and you use proof by contradiction, then you will assume $\neg \forall x P(x)$, which is equivalent to $\exists x \neg P(x)$. If you are proving $\exists x P(x)$ and you use proof by contradiction, then you will assume $\neg \exists x P(x)$, which is equivalent to $\forall x \neg P(x)$. So a goal with one kind of quantifier is converted to a given with the other kind when you use proof by contradiction.

Section 3.4

1. ($\rightarrow$) Suppose $\forall x(P(x) \wedge Q(x))$. Let y be arbitrary. Then since $\forall x(P(x) \wedge Q(x))$, $P(y) \wedge Q(y)$, and so in particular $P(y)$. Since y was arbitrary, this shows that $\forall x P(x)$. A similar argument proves $\forall x Q(x)$: for arbitrary y, $P(y) \wedge Q(y)$, and therefore $Q(y)$. Thus, $\forall x P(x) \wedge \forall x Q(x)$.
   ($\leftarrow$) Suppose $\forall x P(x) \wedge \forall x Q(x)$. Let y be arbitrary. Then since $\forall x P(x)$, $P(y)$, and similarly since $\forall x Q(x)$, $Q(y)$. Thus, $P(y) \wedge Q(y)$, and since y was arbitrary, it follows that $\forall x(P(x) \wedge Q(x))$.

2. Suppose $A \subseteq B$ and $A \subseteq C$. Let x be an arbitrary element of A. Then since $x \in A$ and $A \subseteq B$, $x \in B$, and since $x \in A$ and $A \subseteq C$, $x \in C$. Thus $x \in B \cap C$, and since x was arbitrary it follows that $A \subseteq B \cap C$.

3. Let C be an arbitrary set. Suppose $x \in C \setminus B$. Then $x \in C$ and $x \notin B$. If $x \in A$ then, since $A \subseteq B$, $x \in B$, which is a contradiction. Therefore $x \notin A$. Since $x \in C$ and $x \notin A$, $x \in C \setminus A$. But x was an arbitrary element of $C \setminus B$, so we can conclude that $C \setminus B \subseteq C \setminus A$.

4. Suppose that $A \subseteq B$ and $A \nsubseteq C$. Since $A \nsubseteq C$, we can choose some $a \in A$ such that $a \notin C$. Since $a \in A$ and $A \subseteq B$, $a \in B$. Since $a \in B$ and $a \notin C$, $B \nsubseteq C$.

5. Suppose $A \subseteq B \setminus C$ and $A \neq \varnothing$. Since $A \neq \varnothing$, we can choose some $a \in A$, and since $A \subseteq B \setminus C$, $a \in B \setminus C$. Therefore $a \in B$ and $a \notin C$, so $B \nsubseteq C$.

6. Let x be arbitrary. Then

$$\begin{aligned} x \in A \setminus (B \cap C) &\text{ iff } x \in A \wedge \neg(x \in B \wedge x \in C) && \text{(definitions of } \setminus, \cap), \\ &\text{iff } x \in A \wedge (x \notin B \vee x \notin C) && \text{(De Morgan's law)}, \\ &\text{iff } (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C) && \text{(distributive law)}, \\ &\text{iff } x \in (A \setminus B) \cup (A \setminus C) && \text{(definitions of } \setminus, \cup). \end{aligned}$$

7. Let A and B be arbitrary sets. Let x be arbitrary, and suppose that $x \in \mathscr{P}(A \cap B)$. Then $x \subseteq A \cap B$. Now let y be an arbitrary element of x. Then since $x \subseteq A \cap B$, $y \in A \cap B$, and therefore $y \in A$. Since y was arbitrary, this shows that $x \subseteq A$, so $x \in \mathscr{P}(A)$. A similar argument shows that $x \subseteq B$, and therefore $x \in \mathscr{P}(B)$. Thus, $x \in \mathscr{P}(A) \cap \mathscr{P}(B)$.

   Now suppose that $x \in \mathscr{P}(A) \cap \mathscr{P}(B)$. Then $x \in \mathscr{P}(A)$ and $x \in \mathscr{P}(B)$, so $x \subseteq A$ and $x \subseteq B$. Suppose that $y \in x$. Then since $x \subseteq A$ and $x \subseteq B$, $y \in A$ and $y \in B$, so $y \in A \cap B$. Thus, $x \subseteq A \cap B$, so $x \in \mathscr{P}(A \cap B)$.

8. ($\rightarrow$) Suppose $A \subseteq B$. Let x be an arbitrary element of $\mathscr{P}(A)$. Then $x \subseteq A$. Suppose $y \in x$. Then since $x \subseteq A$, $y \in A$, and since $A \subseteq B$, $y \in B$. Since y was arbitrary, this shows that $x \subseteq B$, so $x \in \mathscr{P}(B)$. And since x was arbitrary, this shows that $\mathscr{P}(A) \subseteq \mathscr{P}(B)$.

   ($\leftarrow$) Suppose $\mathscr{P}(A) \subseteq \mathscr{P}(B)$. Clearly $A \subseteq A$, so $A \in \mathscr{P}(A)$. Since $\mathscr{P}(A) \subseteq \mathscr{P}(B)$, it follows that $A \in \mathscr{P}(B)$, and therefore $A \subseteq B$.

9. Suppose that x and y are odd. Then we can choose integers j and k such that $x = 2j+1$ and $y = 2k+1$. Therefore $xy = (2j+1)(2k+1) = 4jk + 2j + 2k + 1 = 2(2jk + j + k) + 1$. Since $2jk + j + k$ is an integer, it follows that xy is odd.

10. Suppose that x and y are odd. Then we can choose integers j and k such that $x = 2j+1$ and $y = 2k+1$. Therefore $x - y = (2j+1) - (2k+1) = 2(j-k)$. Since $j - k$ is an integer, $x - y$ is even.

11. Let n be an arbitrary integer.

    ($\rightarrow$) We will prove the contrapositive. Suppose n is odd. Then we can choose some integer k such that $n = 2k+1$. Therefore $n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$, which is odd, since $4k^3 + 6k^2 + 3k$ is an integer. Therefore, if n^3 is even then n is even.

    ($\leftarrow$) Suppose n is even. Then we can choose some integer k such that $n = 2k$. Therefore $n^3 = 8k^3 = 2(4k^3)$, so n^3 is even.

12. (a) The mistake is in the sentence "Similarly, since n is odd we have $n = 2k+1$." The letter k already stands for something (it was introduced in the previous sentence), so we need to use a different letter. The sentence should be "Similarly, since n is odd, we can choose some integer j such that $n = 2j + 1$."

    (b) The theorem is incorrect. One counterexample is $m = 2$, $n = 5$.

13. Let $x \in \mathbb{R}$ be arbitrary.

    ($\rightarrow$) Suppose $\exists y \in \mathbb{R}(x + y = xy)$. Then we can let y_0 be some real number such that $x + y_0 = xy_0$. Suppose $x = 1$. Then $1 + y_0 = 1 \cdot y_0 = y_0$, so $1 = 0$, which is a contradiction. Therefore $x \neq 1$.

    ($\leftarrow$) Suppose $x \neq 1$. Let $y = x/(x-1)$, which is defined since $x \neq 1$. Then

$$x + y = x + \frac{x}{x-1} = \frac{x^2 - x}{x-1} + \frac{x}{x-1} = \frac{x^2}{x-1} = x \cdot \frac{x}{x-1} = xy.$$

14. Let $z = 1$. Let $x \in \mathbb{R}^+$ be arbitrary.

($\rightarrow$) Suppose $\exists y \in \mathbb{R}(y - x = y/x)$. Then we can let y_0 be some real number such that $y_0 - x = y_0/x$. Suppose $x = z = 1$. Then $y_0 - 1 = y_0/1 = y_0$, so $-1 = 0$, which is a contradiction. Therefore $x \neq z$.

($\leftarrow$) Suppose $x \neq z = 1$. Let $y = x^2/(x-1)$, which is defined since $x \neq 1$. Then

$$y - x = \frac{x^2}{x-1} - x = \frac{x^2}{x-1} - \frac{x^2 - x}{x-1} = \frac{x}{x-1} = \frac{\frac{x^2}{x-1}}{x} = \frac{y}{x}.$$

15. Suppose $x \in \bigcup\{A \setminus B \mid A \in \mathcal{F}\}$. Then we can choose some $A \in \mathcal{F}$ such that $x \in A \setminus B$, so $x \in A$ and $x \notin B$. Since $x \in A$ and $x \notin B$, $A \nsubseteq B$, so $A \notin \mathscr{P}(B)$. Since $A \in \mathcal{F}$ and $A \notin \mathscr{P}(B)$, $A \in \mathcal{F} \setminus \mathscr{P}(B)$. Since $x \in A$ and $A \in \mathcal{F} \setminus \mathscr{P}(B)$, $x \in \bigcup(\mathcal{F} \setminus \mathscr{P}(B))$. Since x was arbitrary, we conclude that $\bigcup\{A \setminus B \mid A \in \mathcal{F}\} \subseteq \bigcup(\mathcal{F} \setminus \mathscr{P}(B))$.

16. Suppose that $\bigcup\mathcal{F}$ and $\bigcap\mathcal{G}$ are not disjoint. Then we can choose some x such that $x \in \bigcup\mathcal{F}$ and $x \in \bigcap\mathcal{G}$. Since $x \in \bigcup\mathcal{F}$, we can choose some $A \in \mathcal{F}$ such that $x \in A$. Since we are given that every element of $\mathcal{F}$ is disjoint from some element of $\mathcal{G}$, there must be some $B \in \mathcal{G}$ such that $A \cap B = \varnothing$. Since $x \in A$, it follows that $x \notin B$. But we also have $x \in \bigcap\mathcal{G}$ and $B \in \mathcal{G}$, from which it follows that $x \in B$, which is a contradiction. Thus, $\bigcup\mathcal{F}$ and $\bigcap\mathcal{G}$ must be disjoint.

17. Let A be an arbitrary set. Suppose $x \in A$. Clearly $A \subseteq A$, so $A \in \mathscr{P}(A)$. Since $x \in A$ and $A \in \mathscr{P}(A)$, $x \in \bigcup\mathscr{P}(A)$. Since x was arbitrary, we can conclude that $A \subseteq \bigcup\mathscr{P}(A)$.

Now suppose $x \in \bigcup\mathscr{P}(A)$. Then we can choose some $B \in \mathscr{P}(A)$ such that $x \in B$. Since $B \in \mathscr{P}(A)$, $B \subseteq A$. Since $x \in B$ and $B \subseteq A$, $x \in A$. Since x was arbitrary, we can conclude that $\bigcup\mathscr{P}(A) \subseteq A$.

We have proven that $A \subseteq \bigcup\mathscr{P}(A)$ and $\bigcup\mathscr{P}(A) \subseteq A$. It follows that $A = \bigcup\mathscr{P}(A)$.

18. (a) Suppose $x \in \bigcup(\mathcal{F} \cap \mathcal{G})$. Then we can choose some $A \in \mathcal{F} \cap \mathcal{G}$ such that $x \in A$. Since $A \in \mathcal{F} \cap \mathcal{G}$, $A \in \mathcal{F}$ and $A \in \mathcal{G}$. Since $x \in A$ and $A \in \mathcal{F}$, $x \in \bigcup\mathcal{F}$, and similarly since $x \in A$ and $A \in \mathcal{G}$, $x \in \bigcup\mathcal{G}$. Therefore, $x \in (\bigcup\mathcal{F}) \cap (\bigcup\mathcal{G})$. Since x was arbitrary, this shows that $\bigcup(\mathcal{F} \cap \mathcal{G}) \subseteq (\bigcup\mathcal{F}) \cap (\bigcup\mathcal{G})$.

(b) The sentence "Thus, we can choose a set A such that $A \in \mathcal{F}$, $A \in \mathcal{G}$, and $x \in A$" is incorrect. It should say "Thus, we can choose a set $A_1 \in \mathcal{F}$ such that $x \in A_1$, and we can choose a set $A_2 \in \mathcal{G}$ such that $x \in A_2$." We cannot assume the sets A_1 and A_2 are the same, so we have to give them different names.

(c) One example is $\mathcal{F} = \{\{1\}, \{2\}\}$, $\mathcal{G} = \{\{1\}, \{1, 2\}\}$.

19. ($\rightarrow$) Suppose $(\bigcup\mathcal{F}) \cap (\bigcup\mathcal{G}) \subseteq \bigcup(\mathcal{F} \cap \mathcal{G})$. Let A be an arbitrary element of $\mathcal{F}$ and let B be an arbitrary element of $\mathcal{G}$. Suppose $x \in A \cap B$. Then $x \in A$ and $x \in B$. Since $x \in A$ and $A \in \mathcal{F}$, $x \in \bigcup\mathcal{F}$, and since $x \in B$ and $B \in \mathcal{G}$, $x \in \bigcup\mathcal{G}$. Therefore $x \in (\bigcup\mathcal{F}) \cap (\bigcup\mathcal{G})$, and since $(\bigcup\mathcal{F}) \cap (\bigcup\mathcal{G}) \subseteq \bigcup(\mathcal{F} \cap \mathcal{G})$, it follows that $x \in \bigcup(\mathcal{F} \cap \mathcal{G})$. Since x was arbitrary, we can conclude that $A \cap B \subseteq \bigcup(\mathcal{F} \cap \mathcal{G})$.

($\leftarrow$) Suppose $\forall A \in \mathcal{F} \forall B \in \mathcal{G}(A \cap B \subseteq \bigcup(\mathcal{F} \cap \mathcal{G}))$. Let x be an arbitrary element of $(\bigcup\mathcal{F}) \cap (\bigcup\mathcal{G})$. Then $x \in \bigcup\mathcal{F}$ and $x \in \bigcup\mathcal{G}$, so we can choose sets $A \in \mathcal{F}$ and $B \in \mathcal{G}$ such that $x \in A$ and $x \in B$. By assumption, $A \cap B \subseteq \bigcup(\mathcal{F} \cap \mathcal{G})$. Since $x \in A$ and $x \in B$, $x \in A \cap B$, and therefore $x \in \bigcup(\mathcal{F} \cap \mathcal{G})$. Since x was arbitrary, it follows that $(\bigcup\mathcal{F}) \cap (\bigcup\mathcal{G}) \subseteq \bigcup(\mathcal{F} \cap \mathcal{G})$.

20. ($\rightarrow$) Suppose $\bigcup\mathcal{F}$ and $\bigcup\mathcal{G}$ are disjoint. Let $A \in \mathcal{F}$ and $B \in \mathcal{G}$ be arbitrary. Suppose $x \in A \cap B$. Then $x \in A$ and $A \in \mathcal{F}$, and therefore $x \in \bigcup\mathcal{F}$, and also $x \in B$ and $B \in \mathcal{G}$, so $x \in \bigcup\mathcal{G}$. But this contradicts the fact that $\bigcup\mathcal{F}$ and $\bigcup\mathcal{G}$ are disjoint. Therefore there can be no elements in $A \cap B$, so A and B are disjoint.

($\leftarrow$) Assume that for all $A \in \mathcal{F}$ and $B \in \mathcal{G}$, A and B are disjoint. Suppose $x \in (\bigcup\mathcal{F}) \cap (\bigcup\mathcal{G})$. Then $x \in \bigcup\mathcal{F}$ and $x \in \bigcup\mathcal{G}$, so we can choose $A \in \mathcal{F}$ and $B \in \mathcal{G}$ such that $x \in A$ and $x \in B$. But then A and B are not disjoint, which contradicts our assumption. Therefore $\bigcup\mathcal{F}$ and $\bigcup\mathcal{G}$ are disjoint.

21. (a) Suppose $x \in (\bigcup\mathcal{F}) \setminus (\bigcup\mathcal{G})$. Then $x \in \bigcup\mathcal{F}$ and $x \notin \bigcup\mathcal{G}$. Since $x \in \bigcup\mathcal{F}$, we can choose some $A \in \mathcal{F}$ such that $x \in A$. If $A \in \mathcal{G}$ then since $x \in A$, $x \in \bigcup\mathcal{G}$, which is a contradiction. Therefore

$A \notin \mathcal{G}$, so $A \in \mathcal{F} \setminus \mathcal{G}$. Since $x \in A$ and $A \in \mathcal{F} \setminus \mathcal{G}$, $x \in \bigcup(\mathcal{F} \setminus \mathcal{G})$. Sionce x was arbitrary, $(\bigcup \mathcal{F}) \setminus (\bigcup \mathcal{G}) \subseteq \bigcup(\mathcal{F} \setminus \mathcal{G})$.

(b) The mistake is in the sentence "Since $x \in A$ and $A \notin \mathcal{G}$, $x \notin \bigcup \mathcal{G}$." The statement $x \notin \bigcup \mathcal{G}$ means $\neg\exists A(A \in \mathcal{G} \wedge x \in A)$, but what has been proven is $\exists A(A \notin \mathcal{G} \wedge x \in A)$, which does not mean the same thing.

(c) ($\rightarrow$) Suppose $\bigcup(\mathcal{F} \setminus \mathcal{G}) \subseteq (\bigcup \mathcal{F}) \setminus (\bigcup \mathcal{G})$. Let $A \in \mathcal{F} \setminus \mathcal{G}$ and $B \in \mathcal{G}$ be arbitrary. Suppose $A \cap B \neq \varnothing$. Then we can choose some $x \in A \cap B$. Since $x \in A$ and $A \in \mathcal{F} \setminus \mathcal{G}$, $x \in \bigcup(\mathcal{F} \setminus \mathcal{G})$. Since $\bigcup(\mathcal{F} \setminus \mathcal{G}) \subseteq (\bigcup \mathcal{F}) \setminus (\bigcup \mathcal{G})$, $x \in (\bigcup \mathcal{F}) \setminus (\bigcup \mathcal{G})$, so $x \in \bigcup \mathcal{F}$ and $x \notin \bigcup \mathcal{G}$. But $x \in B$ and $B \in \mathcal{G}$, so $x \in \bigcup \mathcal{G}$, which is a contradiction. Therefore A and B must be disjoint, as required.

($\leftarrow$) Suppose $\forall A \in (\mathcal{F} \setminus \mathcal{G})\forall B \in \mathcal{G}(A \cap B = \varnothing)$. Let x be an arbitrary element of $\bigcup(\mathcal{F} \setminus \mathcal{G})$. Then we can choose some $A \in \mathcal{F} \setminus \mathcal{G}$ such that $x \in A$. Since $A \in \mathcal{F} \setminus \mathcal{G}$, $A \in \mathcal{F}$, and since $x \in A$, it follows that $x \in \bigcup \mathcal{F}$. Now suppose $x \in \bigcup \mathcal{G}$. Then we can choose some set $B \in \mathcal{G}$ such that $x \in B$. Since $A \in \mathcal{F} \setminus \mathcal{G}$ and $B \in \mathcal{G}$, by our assumption $A \cap B = \varnothing$ But $x \in A \cap B$, so we have reached a contradiction Therefore $x \notin \bigcup \mathcal{G}$. Since $x \in \bigcup \mathcal{F}$ and $x \notin \bigcup \mathcal{G}$, $x \in (\bigcup \mathcal{F}) \setminus (\bigcup \mathcal{G})$. Since x was arbitrary, we can conclude that $\bigcup(\mathcal{F} \setminus \mathcal{G}) \subseteq (\bigcup \mathcal{F}) \setminus (\bigcup \mathcal{G})$.

(d) One example is $\mathcal{F} = \{\{1, 2\}, \{3\}\}$, $\mathcal{G} = \{\{1\}, \{2, 3\}\}$.

22. Suppose that $\bigcup \mathcal{F} \nsubseteq \bigcup \mathcal{G}$. Then there is some $x \in \bigcup \mathcal{F}$ such that $x \notin \bigcup \mathcal{G}$. Since $x \in \bigcup \mathcal{F}$, we can choose some $A \in \mathcal{F}$ such that $x \in A$. Now let $B \in \mathcal{G}$ be arbitrary. If $A \subseteq B$, then since $x \in A$, $x \in B$. But then since $x \in B$ and $B \in \mathcal{G}$, $x \in \bigcup \mathcal{G}$, which we already know is false. Therefore $A \nsubseteq B$. Since B was arbitrary, this shows that for all $B \in \mathcal{G}$, $A \nsubseteq B$. Thus, we have shown that there is some $A \in \mathcal{F}$ such that for all $B \in \mathcal{G}$, $A \nsubseteq B$.

23. (a) The proof proves that $B \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I}(B \cap A_i)$ by proving that $\forall x(x \in B \cap (\bigcup_{i \in I} A_i) \leftrightarrow x \in \bigcup_{i \in I}(B \cap A_i))$, which is proven by letting x be arbitrary and then proving both directions of the biconditional. For both directions, the crucial step is the use of existential instantiation to choose i_0.

(b) Let x be arbitrary. Suppose $x \in B \setminus (\bigcup_{i \in I} A_i)$. Then $x \in B$ and $x \notin \bigcup_{i \in I} A_i$. Now let $i \in I$ be arbitrary. If $x \in A_i$ then $x \in \bigcup_{i \in I} A_i$, which is a contradiction. Therefore $x \notin A_i$. Since we also know that $x \in B$, we can conclude that $x \in B \setminus A_i$. Since i was arbitrary, this proves that $\forall i \in I(x \in B \setminus A_i)$, so $x \in \bigcap_{i \in I}(B \setminus A_i)$.

Now suppose $x \in \bigcap_{i \in I}(B \setminus A_i)$. Since $I \neq \varnothing$, we can choose some i_0 such that $i_0 \in I$. Since $x \in \bigcap_{i \in I}(B \setminus A_i)$, $x \in B \setminus A_{i_0}$, so $x \in B$. Suppose $x \in \bigcup_{i \in I} A_i$. Then we can choose some $i_1 \in I$ such that $x \in A_{i_1}$. But since $x \in \bigcap_{i \in I}(B \setminus A_i)$ we also know that $x \in B \setminus A_{i_1}$, so $x \notin A_{i_1}$. This is a contradiction. Therefore $x \notin \bigcup_{i \in I} A_i$. Since $x \in B$ and $x \notin \bigcup_{i \in} A_i$, $x \in B \setminus (\bigcup_{i \in I} A_i)$.

We have proven that $\forall x(x \in B \setminus (\bigcup_{i \in I} A_i) \leftrightarrow x \in \bigcap_{i \in I}(B \setminus A_i))$, so $B \setminus (\bigcup_{i \in I} A_i) = \bigcap_{i \in I}(B \setminus A_i)$.

(c) $B \setminus (\bigcap_{i \in I} A_i) = \bigcup_{i \in I}(B \setminus A_i)$. Proof: Let x be arbitrary. Suppose $x \in B \setminus (\bigcap_{i \in I} A_i)$. Then $x \in B$ and $x \notin \bigcap_{i \in I} A_i$. Since $x \notin \bigcap_{i \in I} A_i$, we can choose some $i_0 \in I$ such that $x \notin A_{i_0}$. Since $x \in B$ and $x \notin A_{i_0}$, $x \in B \setminus A_{i_0}$. Therefore $x \in \bigcup_{i \in I}(B \setminus A_i)$.

Now suppose $x \in \bigcup_{i \in I}(B \setminus A_i)$. Then we can choose some $i_0 \in I$ such that $x \in B \setminus A_{i_0}$. Since $x \in B \setminus A_{i_0}$, $x \in B$ and $x \notin A_{i_0}$. Since $x \notin A_{i_0}$, $x \notin \bigcap_{i \in I} A_i$. Since $x \in B$ and $x \notin \bigcap_{i \in I} A_i$, $x \in B \setminus (\bigcap_{i \in I} A_i)$.

We have shown that $\forall x(x \in B \setminus (\bigcap_{i \in I} A_i) \leftrightarrow x \in \bigcup_{i \in I}(B \setminus A_i)$. Therefore $B \setminus (\bigcap_{i \in I} A_i) = \bigcup_{i \in I}(B \setminus A_i)$.

24. (a) Suppose $x \in \bigcup_{i \in l}(A_i \setminus B_i)$. Then we can choose some $i \in I$ such that $x \in A_i \setminus B_i$, which means $x \in A_i$ and $x \notin B_i$. Since $x \in A_i$, $x \in \bigcup_{i \in l} A_i$, and since $x \notin B_i$, $x \notin \bigcap_{i \in l} B_i$. Thus, $x \in (\bigcup_{i \in l} A_i) \setminus (\bigcap_{i \in l} B_i)$. Since x was arbitrary, $\bigcup_{i \in I}(A_i \setminus B_i) \subseteq (\bigcup_{i \in I} A_i) \setminus (\bigcap_{i \in I} B_i)$.

(b) One example is $I = \{1, 2\}$, $A_1 = B_1 = \{1\}$, $A_2 = B_2 = \{2\}$.

25. (a) Suppose $x \in \bigcup_{i \in I}(A_i \cap B_i)$. Then we can choose some $i \in I$ such that $x \in A_i \cap B_i$, which means

that $x \in A_i$ and $x \in B_i$. Since $x \in A_i$, $x \in \bigcup_{i \in I} A_i$, and since $x \in B_i$, $x \in \bigcup_{i \in I} B_i$. Therefore $x \in (\bigcup_{i \in I} A_i) \cap (\bigcup_{i \in I} B_i)$. Since x was arbitrary, $\bigcup_{i \in I}(A_i \cap B_i) \subseteq (\bigcup_{i \in I} A_i) \cap (\bigcup_{i \in I} B_i)$.

(b) One example is $I = \{1, 2\}$, $A_1 = \{1\}$, $A_2 = \{2\}$, $B_1 = \{2\}$, $B_2 = \{1\}$.

26. Let a and b be arbitrary integers. Let $c = ab$. Then c is an integer, $a \mid c$, and $b \mid c$.

27. (a) Let n be an arbitrary integer.

($\rightarrow$) Suppose $15 \mid n$. Then we can choose some integer k such that $n = 15k$. Therefore $n = 3(5k)$, so $3 \mid n$, and also $n = 5(3k)$, so $5 \mid k$.

($\leftarrow$) Suppose $3 \mid n$ and $5 \mid n$. Then we can choose integers j and k such that $n = 3j = 5k$. Therefore $15(2k - j) = 30k - 15j = 6(5k) - 5(3j) = 6n - 5n = n$, so $15 \mid n$.

(b) Let $n = 30$. Then $6 \mid n$ and $10 \mid n$, but $60 \nmid n$.

Section 3.5

1. Suppose $x \in A \cap (B \cup C)$. Then $x \in A$, and either $x \in B$ or $x \in C$.
Case 1. $x \in B$. Then since $x \in A$, $x \in A \cap B$, so $x \in (A \cap B) \cup C$.
Case 2. $x \in C$. Then clearly $x \in (A \cap B) \cup C$.
Since x was arbitrary, we can conclude that $A \cap (B \cup C) \subseteq (A \cap B) \cup C$.

2. Suppose $x \in (A \cup B) \setminus C$. Then either $x \in A$ or $x \in B$, and also $x \notin C$.
Case 1. $x \in A$. Then $x \in A \cup (B \setminus C)$.
Case 2. $x \in B$. Then since $x \notin C$, $x \in B \setminus C$, so $x \in A \cup (B \setminus C)$.
Since x was arbitrary, we can conclude that $(A \cup B) \setminus C \subseteq A \cup (B \setminus C)$.

3. Suppose $x \in A \setminus (A \setminus B)$. Then $x \in A$ and $x \notin A \setminus B$. Since $x \notin A \setminus B$, either $x \notin A$ or $x \in B$. But it cannot be the case that $x \notin A$, since we know $x \in A$, so $x \in B$. Since $x \in A$ and $x \in B$, $x \in A \cap B$. This shows that $A \setminus (A \setminus B) \subseteq A \cap B$.

Now suppose $x \in A \cap B$. Then $x \in A$ and $x \in B$. Since $x \in B$, $x \notin A \setminus B$. Since $x \in A$ and $x \notin A \setminus B$, $x \in A \setminus (A \setminus B)$. Thus $A \cap B \subseteq A \setminus (A \setminus B)$.

We have shown that $A \setminus (A \setminus B) \subseteq A \cap B$ and $A \cap B \subseteq A \setminus (A \setminus B)$, so $A \setminus (A \setminus B) = A \cap B$.

4. Let x be arbitrary. Then

$$\begin{aligned}
x \in A \setminus (B \setminus C) &\text{ iff } x \in A \wedge \neg(x \in B \wedge x \notin C) && \text{(definition of } \setminus\text{)} \\
&\text{iff } x \in A \wedge (x \notin B \vee x \in C) && \text{(De Morgan's law)} \\
&\text{iff } (x \in A \wedge x \notin B) \vee (x \in A \wedge x \in C) && \text{(distributive law)} \\
&\text{iff } x \in (A \setminus B) \cup (A \cap C) && \text{(definitions of } \setminus\text{, } \cup\text{, and } \cap\text{)..}
\end{aligned}$$

Therefore $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$.

5. Suppose $x \in A$. We now consider two cases:
Case 1. $x \in C$. Then $x \in A \cap C$, so since $A \cap C \subseteq B \cap C$, $x \in B \cap C$, and therefore $x \in B$.
Case 2. $x \notin C$. Since $x \in A$, $x \in A \cup C$, so since $A \cup C \subseteq B \cup C$, $x \in B \cup C$. But $x \notin C$, so we must have $x \in B$.
Thus, $x \in B$, and since x was arbitrary, $A \subseteq B$.

6. Suppose $A \triangle B \subseteq A$. Suppose $B \not\subseteq A$. Then we can choose some $x \in B$ such that $x \notin A$. Since $x \in B$ and $x \notin A$, $x \in B \setminus A$, so $x \in (A \setminus B) \cup (B \setminus A) = A \triangle B$. But now we have $x \in A \triangle B$ and $x \notin A$, which contradicts the fact that $A \triangle B \subseteq A$. Therefore $B \subseteq A$.

7. ($\rightarrow$) Suppose $A \cup C \subseteq B \cup C$. Suppose $x \in A \setminus C$, which means $x \in A$ and $x \notin C$. Since $x \in A$, $x \in A \cup C$, and since $A \cup C \subseteq B \cup C$, $x \in B \cup C$. This means either $x \in B$ or $x \in C$. But we also know $x \notin C$, so $x \in B$. Since $x \in B$ and $x \notin C$, $x \in B \setminus C$. Since x was arbitrary, we conclude that $A \setminus C \subseteq B \setminus C$.

($\leftarrow$) Suppose $A \setminus C \subseteq B \setminus C$. Suppose $x \in A \cup C$.

Case 1. $x \in C$. Then $x \in B \cup C$.

Case 2. $x \notin C$. Since $x \in A \cup C$ and $x \notin C$, $x \in A$. Since $x \in A$ and $x \notin C$, $x \in A \setminus C$. Since $A \setminus C \subseteq B \setminus C$, it follows that $x \in B \setminus C$. Therefore $x \in B$, so $x \in B \cup C$.

Since these cases are exhaustive, we have proven that $x \in B \cup C$. Since x was arbitrary, we can conclude that $A \cup C \subseteq B \cup C$.

8. Suppose $x \in \mathscr{P}(A) \cup \mathscr{P}(B)$. Then either $x \in \mathscr{P}(A)$ or $x \in \mathscr{P}(B)$.

   Case 1. $x \in \mathscr{P}(A)$. Then $x \subseteq A$. Let y be an arbitrary element of x. Since $x \subseteq A$, $y \in A$, so $y \in A \cup B$. Since y was arbitrary, $x \subseteq A \cup B$, so $x \in \mathscr{P}(A \cup B)$.

   Case 2. $x \in \mathscr{P}(B)$. A similar argument shows $x \in \mathscr{P}(A \cup B)$.

   Since x was arbitrary, we have proven that $\mathscr{P}(A) \cup \mathscr{P}(B) \subseteq \mathscr{P}(A \cup B)$.

9. Suppose $\mathscr{P}(A) \cup \mathscr{P}(B) = \mathscr{P}(A \cup B)$. Clearly $A \cup B \subseteq A \cup B$, so $A \cup B \in \mathscr{P}(A \cup B)$. Since $\mathscr{P}(A) \cup \mathscr{P}(B) = \mathscr{P}(A \cup B)$, it follows that $A \cup B \in \mathscr{P}(A) \cup \mathscr{P}(B)$, so either $A \cup B \in \mathscr{P}(A)$ or $A \cup B \in \mathscr{P}(B)$.

   Case 1. $A \cup B \in \mathscr{P}(A)$. Then $A \cup B \subseteq A$. Suppose $x \in B$. Then $x \in A \cup B$, so since $A \cup B \subseteq A$, $x \in A$. Since x was arbitrary, $B \subseteq A$.

   Case 2. $A \cup B \in \mathscr{P}(B)$. A similar argument shows that $A \subseteq B$.

   Since these cases are exhaustive, we conclude that either $A \subseteq B$ or $B \subseteq A$.

10. ($\rightarrow$) Suppose $y + 1/x = 1 + y/x$. Then $y - 1 = y/x - 1/x = (y-1)/x$. If $y \neq 1$ then $y - 1 \neq 0$, so we can divide both sides of this equation by $y - 1$ and conclude that $1 = 1/x$, so $x = 1$. Thus, either $x = 1$ or $y = 1$.

    ($\leftarrow$) Suppose that either $x = 1$ or $y = 1$.

    Case 1. $x = 1$. Then $y + 1/x = y + 1 = 1 + y/x$.

    Case 2. $y = 1$. Then $y + 1/x = 1 + 1/x = 1 + y/x$.

11. Let x be an arbitrary real number and assume that $|x - 3| > 3$.

    Case 1. $x - 3 \geq 0$. Then $|x - 3| = x - 3$, so since $|x - 3| > 3$, $x - 3 > 3$, and therefore $x > 6$. Multiplying by x, which is positive, we conclude that $x^2 > 6x$.

    Case 2. $x - 3 < 0$. Then $|x - 3| = -(x - 3) = 3 - x$, so since $|x - 3| > 3$, $3 - x > 3$, so $3 > x + 3$ and therefore $0 > x$. Thus $x^2 \geq 0 > 6x$.

12. Let x be an arbitrary real number.

    ($\leftarrow$) Suppose $|x - 4| > 2$.

    Case 1. $x - 4 \geq 0$. Then $|x - 4| = x - 4$, so we have $x - 4 > 2$, and therefore $x > 6$. Adding x to both sides gives us $2x > 6 + x$, so $2x - 6 > x$. Since $x > 6$, this implies that $2x - 6$ is positive, so $|2x - 6| = 2x - 6 > x$.

    Case 2. $x - 4 < 0$. Then $|x - 4| = 4 - x$, so we have $4 - x > 2$, and therefore $x < 2$. Therefore $3x < 6$, and subtracting $2x$ from both sides we get $x < 6 - 2x$. Also, from $x < 2$ we get $2x < 4$, so $2x - 6 < -2$. Therefore $2x - 6$ is negative, so $|2x - 6| = 6 - 2x > x$.

    ($\rightarrow$) Suppose $|2x - 6| > x$.

    Case 1. $2x - 6 \geq 0$. Then $|2x - 6| = 2x - 6$, so $2x - 6 > x$, and therefore $x > 6$. Since $x > 6$, $x - 4 > 2 > 0$, so $|x - 4| = x - 4 > 2$.

    Case 2. $2x - 6 < 0$. Then $|2x - 6| = 6 - 2x$, so $6 - 2x > x$, and therefore $6 > 3x$ and $x < 2$. Thus $x - 4 < -2 < 0$, so $|x - 4| = 4 - x > 2$.

13. (a) Let a and b be arbitrary real numbers.

    ($\rightarrow$) Suppose $|a| \leq b$.

    Case 1. $a \geq 0$. Then $|a| = a$, so $a \leq b$. Also, since $b \geq a$ and $a \geq 0$, $b \geq 0$, so $-b \leq 0$. Therefore $-b \leq 0 \leq a \leq b$, so $-b \leq a \leq b$.

    Case 2. $a < 0$. Then $|a| = -a$, so $-a \leq b$, and therefore $a \geq -b$. Also, since $-b \leq a$ and $a < 0$, $-b < 0$, so $b > 0$. Therefore $-b \leq a < 0 < b$, so $-b \leq a \leq b$.

($\leftarrow$) Suppose $-b \leq a \leq b$. Then $a \leq b$ and $-b \leq a$, so $b \geq -a$.
Case 1. $a \geq 0$. Then $|a| = a \leq b$.
Case 2. $a < 0$. Then $|a| = -a \leq b$.

(b) Let x be an arbitrary real number. Clearly $|x| \leq |x|$, and by part (a) it follows that $-|x| \leq x \leq |x|$.

(c) Let x and y be arbitrary real numbers. By part (b), we have $-|x| \leq x \leq |x|$ and $-|y| \leq y \leq |y|$. Adding these two inequalities we get $-(|x| + |y|) \leq x + y \leq |x| + |y|$. By part (a), it follows that $|x + y| \leq |x| + |y|$.

(d) Let x and y be arbitrary real numbers. By part (c), $|x| = |(x + y) + (-y)| \leq |x + y| + |-y| = |x + y| + |y|$. Therefore $|x + y| \geq |x| - |y|$.

14. Let x be an arbitrary integer.
Case 1. x is even. Then we can choose some integer k such that $x = 2k$. Therefore $x^2 + x = (2k)^2 + 2k = 4k^2 + 2k = 2(2k^2 + k)$, so $x^2 + x$ is even.
Case 2. x is odd. Then we can choose some integer k such that $x = 2k + 1$. Therefore $x^2 + x = (2k + 1)^2 + (2k + 1) = 4k^2 + 4k + 1 + 2k + 1 = 4k^2 + 6k + 2 = 2(2k^2 + 3k + 1)$, so $x^2 + x$ is even.
Since there cases are exhaustive, we conclude that $x^2 + x$ is even.

15. Let x be an arbitrary integer.
Case 1. x is even. Then we can choose some integer k such that $x = 2k$. Therefore $x^4 = (2k)^4 = 16k^4 = 8(2k^4)$, so the quotient when x^4 is divided by 8 is $2k^4$, and the remainder is 0.
Case 2. x is odd. Then we can choose some integer k such that $x = 2k + 1$. Therefore $x^4 = (2k + 1)^4 = 16k^4 + 32k^3 + 24k^2 + 8k + 1 = 8(2k^4 + 4k^3 + 3k^2 + k) + 1$, so the quotient when x^4 is divided by 8 is $2k^4 + 4k^3 + 3k^2 + k$ and the remainder is 1.
Thus, the remainder when x^4 is divided by 8 is either 0 or 1.

16. (a) Suppose $x \in \bigcup(\mathcal{F} \cup \mathcal{G})$. Then we can choose some $A \in \mathcal{F} \cup \mathcal{G}$ such that $x \in A$. Since $A \in \mathcal{F} \cup \mathcal{G}$, either $A \in \mathcal{F}$ or $A \in \mathcal{G}$.
Case 1. $A \in \mathcal{F}$. Since $x \in A$ and $A \in \mathcal{F}$, $x \in \bigcup\mathcal{F}$, so $x \in (\bigcup\mathcal{F}) \cup (\bigcup\mathcal{G})$.
Case 2. $A \in \mathcal{G}$. Since $x \in A$ and $A \in \mathcal{G}$, $x \in \bigcup\mathcal{G}$, so $x \in (\bigcup\mathcal{F}) \cup (\bigcup\mathcal{G})$.
Thus, $x \in (\bigcup\mathcal{F}) \cup (\bigcup\mathcal{G})$.
Now suppose that $x \in (\bigcup\mathcal{F}) \cup (\bigcup\mathcal{G})$. Then either $x \in \bigcup\mathcal{F}$ or $x \in \bigcup\mathcal{G}$.
Case 1. $x \in \bigcup\mathcal{F}$. Then we can choose some $A \in \mathcal{F}$ such that $x \in A$. Since $A \in \mathcal{F}$, $A \in \mathcal{F} \cup \mathcal{G}$, so since $x \in A$, it follows that $x \in \bigcup(\mathcal{F} \cup \mathcal{G})$.
Case 2. $x \in \bigcup\mathcal{G}$. A similar argument shows that $x \in \bigcup(\mathcal{F} \cup \mathcal{G})$.
Thus, $x \in \bigcup(\mathcal{F} \cup \mathcal{G})$.

(b) $\bigcap(\mathcal{F} \cup \mathcal{G}) = (\bigcap\mathcal{F}) \cap (\bigcap\mathcal{G})$. Proof: Suppose $x \in \bigcap(\mathcal{F} \cup \mathcal{G})$. Let A be an arbitrary element of $\mathcal{F}$. Since $A \in \mathcal{F}$, $A \in \mathcal{F} \cup \mathcal{G}$, so since $x \in \bigcap(\mathcal{F} \cup \mathcal{G})$, $x \in A$. Since A was an arbitrary element of $\mathcal{F}$, this shows that $x \in \bigcap\mathcal{F}$. A similar argument shows that $x \in \bigcap\mathcal{G}$, so $x \in (\bigcap\mathcal{F}) \cap (\bigcap\mathcal{G})$.
Now suppose $x \in (\bigcap\mathcal{F}) \cap (\bigcap\mathcal{G})$. Then $x \in \bigcap\mathcal{F}$ and $x \in \bigcap\mathcal{G}$. Let A be an arbitrary element of $\mathcal{F} \cup \mathcal{G}$. Then either $A \in \mathcal{F}$ or $A \in \mathcal{G}$.
Case 1. $A \in \mathcal{F}$. Since $x \in \bigcap\mathcal{F}$ and $A \in \mathcal{F}$, $x \in A$.
Case 2. $A \in \mathcal{G}$. Since $x \in \bigcap\mathcal{G}$ and $A \in \mathcal{G}$, $x \in A$.
Thus $x \in A$, and since A was an arbitrary element of $\mathcal{F} \cup \mathcal{G}$, this prove that $x \in \bigcap(\mathcal{F} \cup \mathcal{G})$.

17. (a) Suppose $x \in B \cup (\bigcup\mathcal{F})$. Then either $x \in B$ or $x \in \bigcup\mathcal{F}$.
Case 1. $x \in B$. Since $x \in B$ and $B \in \mathcal{F} \cup \{B\}$, $x \in \bigcup(\mathcal{F} \cup \{B\})$.
Case 2. $x \in \bigcup\mathcal{F}$. Then we can choose is some $A \in \mathcal{F}$ such that $x \in A$. Since $x \in A$ and $A \in \mathcal{F} \cup \{B\}$, $x \in \bigcup(\mathcal{F} \cup \{B\})$.
Thus, $x \in \bigcup(\mathcal{F} \cup \{B\})$.
Now suppose $x \in \bigcup(\mathcal{F} \cup \{B\})$. Then we can choose some $A \in \mathcal{F} \cup \{B\}$ such that $x \in A$. Since $A \in \mathcal{F} \cup \{B\}$, either $A \in \mathcal{F}$ or $A = B$.
Case 1. $A \in \mathcal{F}$. Then since $x \in A$ and $A \in \mathcal{F}$, $x \in \bigcup\mathcal{F}$.

Case 2. $A = B$. Then since $x \in A$, $x \in B$.

Thus, either $x \in \bigcup \mathcal{F}$ or $x \in B$, so $x \in B \cup (\bigcup \mathcal{F})$.

(b) Suppose $x \in B \cup (\bigcap \mathcal{F})$. Then either $x \in B$ or $x \in \bigcap \mathcal{F}$.

Case 1. $x \in B$. Let $A \in \mathcal{F}$ be arbitrary. Since $x \in B$, $x \in B \cup A$. Since A was arbitrary, we can conclude that for all $A \in \mathcal{F}$, $x \in B \cup A$, so $x \in \bigcap_{A \in \mathcal{F}} (B \cup A)$.

Case 2. $x \in \bigcap \mathcal{F}$. Let $A \in \mathcal{F}$ be arbitrary. Since $x \in \bigcap \mathcal{F}$, $x \in A$, so $x \in B \cup A$. Since A was arbitrary, we can conclude that for all $A \in \mathcal{F}$, $x \in B \cup A$, so $x \in \bigcap_{A \in \mathcal{F}} (B \cup A)$.

Thus, $x \in \bigcap_{A \in \mathcal{F}} (B \cup A)$.

Now suppose $x \in \bigcap_{A \in \mathcal{F}} (B \cup A)$. If $x \in B$, then of course $x \in B \cup (\bigcap \mathcal{F})$. Now suppose $x \notin B$. Let $A \in \mathcal{F}$ be arbitrary. Since $x \in \bigcap_{A \in \mathcal{F}} (B \cup A)$, $x \in B \cup A$, so either $x \in B$ or $x \in A$. But $x \notin B$, so $x \in A$. Since A was arbitrary, we can conclude that $x \in \bigcap \mathcal{F}$, so $x \in B \cup (\bigcap \mathcal{F})$.

(c) $B \cap (\bigcup \mathcal{F}) = \bigcup_{A \in \mathcal{F}} (B \cap A)$ and $B \cap (\bigcap \mathcal{F}) = \bigcap (\mathcal{F} \cup \{B\})$. Proof: To prove the first equation, suppose $x \in B \cap (\bigcup \mathcal{F})$. Then $x \in B$ and $x \in \bigcup \mathcal{F}$. Since $x \in \bigcup \mathcal{F}$, we can choose some $A \in \mathcal{F}$ such that $x \in A$. Since $x \in B$ and $x \in A$, $x \in B \cap A$. And since $A \in \mathcal{F}$, it follows that $x \in \bigcup_{A \in \mathcal{F}} (B \cap A)$.

Now suppose $x \in \bigcup_{A \in \mathcal{F}} (B \cap A)$. Then we can choose some $A \in \mathcal{F}$ such that $x \in B \cap A$, so $x \in B$ and $x \in A$. Since $x \in A$ and $A \in \mathcal{F}$, $x \in \bigcup \mathcal{F}$. Since $x \in B$ and $x \in \bigcup \mathcal{F}$, $x \in B \cap (\bigcup \mathcal{F})$. This completes the proof that $B \cap (\bigcup \mathcal{F}) = \bigcup_{A \in \mathcal{F}} (B \cap A)$.

To prove the second equation, suppose $x \in B \cap (\bigcap \mathcal{F})$. Then $x \in B$ and $x \in \bigcap \mathcal{F}$. Let A be an arbitrary element of $\mathcal{F} \cup \{B\}$. Then either $A \in \mathcal{F}$ or $A = B$.

Case 1. $A \in \mathcal{F}$. Then since $x \in \bigcap \mathcal{F}$, $x \in A$.

Case 2. $A = B$. Then since $x \in B$, $x \in A$.

Since these cases are exhaustive, we conclude that $x \in A$. And since A was arbitrary, it follows that $x \in \bigcap (\mathcal{F} \cup \{B]\})$.

Now suppose $x \in \bigcap (\mathcal{F} \cup \{B\})$. Since $B \in \mathcal{F} \cup \{B\}$, it follows that $x \in B$. Now let A be an arbitrary element of $\mathcal{F}$. Then $A \in \mathcal{F} \cup \{B\}$, so since $x \in \bigcap (\mathcal{F} \cup \{B\})$, $x \in A$. Since A was arbitrary, this proves that $x \in \bigcap \mathcal{F}$. Since $x \in B$ and $x \in \bigcap \mathcal{F}$, $x \in B \cap (\bigcap \mathcal{F})$.

18. Suppose $x \in \bigcap \mathcal{H}$. If $x \in \bigcap \mathcal{F}$, then of course $x \in (\bigcap \mathcal{F}) \cup (\bigcap \mathcal{G})$. Now suppose $x \notin \bigcap \mathcal{F}$. Then we can choose some $A \in \mathcal{F}$ such that $x \notin A$. Now let $B \in \mathcal{G}$ be arbitrary. Since $A \in \mathcal{F}$ and $B \in \mathcal{G}$, by assumption $A \cup B \in \mathcal{H}$. Since $x \in \bigcap \mathcal{H}$, it follows that $x \in A \cup B$, so either $x \in A$ or $x \in B$. But we know $x \notin A$, so $x \in B$. Since B was arbitrary, we can conclude that $x \in \bigcap \mathcal{G}$. Thus $x \in (\bigcap \mathcal{F}) \cup (\bigcap \mathcal{G})$. Since x was arbitrary, we have proven that $\bigcap \mathcal{H} \subseteq (\bigcap \mathcal{F}) \cup (\bigcap \mathcal{G})$.

19. Let x be arbitrary.

($\rightarrow$) Suppose $x \in A \triangle B$. Then $x \in (A \setminus B) \cup (B \setminus A)$, so either $x \in A \setminus B$ or $x \in B \setminus A$. We now must prove $x \in A \leftrightarrow x \notin B$, so we will prove both directions of this biconditional.

($\rightarrow$) Suppose $x \in A$. Then $x \notin B \setminus A$, so it must be the case that $x \in A \setminus B$, and therefore $x \notin B$.

($\leftarrow$) Suppose $x \notin B$. Then $x \notin B \setminus A$, so it must be the case that $x \in A \setminus B$, and therefore $x \in A$.

This completes the $\rightarrow$ direction of the proof.

($\leftarrow$) Suppose $x \in A \leftrightarrow x \notin B$. We now consider two cases.

Case 1. $x \in A$. Then since $x \in A \leftrightarrow x \notin B$, $x \notin B$. Therefore $x \in A \setminus B$, so $x \in A \triangle B$.

Case 2. $x \notin A$. Then since $x \in A \leftrightarrow x \notin B$, $x \in B$. Therefore $x \in B \setminus A$, so $x \in A \triangle B$.

Since these cases are exhaustive, $x \in A \triangle B$.

20. ($\rightarrow$) Suppose that $A \triangle B$ and C are disjoint. Let x be an arbitrary element of $A \cap C$. Then $x \in A$ and $x \in C$. If $x \notin B$, then since $x \in A$, $x \in A \setminus B$, and therefore $x \in A \triangle B$. But also $x \in C$, so this contradicts our assumption that $A \triangle B$ and C are disjoint. Therefore $x \in B$. Since we also know $x \in C$, we have $x \in B \cap C$. Since x was an arbitrary element of $A \cap C$, this shows that $A \cap C \subseteq B \cap C$. A similar argument shows that $B \cap C \subseteq A \cap C$.

($\leftarrow$) Suppose that $A \cap C = B \cap C$. Suppose that $A \triangle B$ and C are not disjoint. Then we can choose

some x such that $x \in A \triangle B$ and $x \in C$. Since $x \in A \triangle B$, either $x \in A \setminus B$ or $x \in B \setminus A$.

Case 1. $x \in A \setminus B$. Then $x \in A$ and $x \notin B$. Since we also know $x \in C$, we can conclude that $x \in A \cap C$ but $x \notin B \cap C$. This contradicts the fact that $A \cap C = B \cap C$.

Case 2. $x \in B \setminus A$. Similarly, this leads to a contradiction.

Thus we can conclude that $A \triangle B$ and C are disjoint.

21. ($\rightarrow$) Suppose $A \triangle B \subseteq C$. Let x be an arbitrary element of $A \cup C$. Suppose $x \notin B \cup C$. Then $x \notin B$ and $x \notin C$. Since $x \in A \cup C$ and $x \notin C$, $x \in A$. But then since $x \in A$ and $x \notin B$, $x \in A \setminus B$, so $x \in A \triangle B$. Since $A \triangle B \subseteq C$, $x \in C$, which contradicts the fact that $x \notin C$. Therefore $x \in B \cup C$. Since x was an arbitrary element of $A \cup C$, this shows that $A \cup C \subseteq B \cup C$. A similar proof shows that $B \cup C \subseteq A \cup C$, so $A \cup C = B \cup C$.

($\leftarrow$) Suppose $A \cup C = B \cup C$. Let x be an arbitrary element of $A \triangle B$. Then $x \in (A \setminus B) \cup (B \setminus A)$, so either $x \in A \setminus B$ or $x \in B \setminus A$.

Case 1. $x \in A \setminus B$. Then $x \in A$ and $x \notin B$. Since $x \in A$, $x \in A \cup C$, so since $A \cup C = B \cup C$, $x \in B \cup C$. But $x \notin B$, so $x \in C$.

Case 2. $x \in B \setminus A$. A similar argument shows that $x \in C$.

Since x was an arbitrary element of $A \triangle B$, we can conclude that $A \triangle B \subseteq C$.

22. ($\rightarrow$) Suppose $C \subseteq A \triangle B$. Let x be an arbitrary element of C. Then since $C \subseteq A \triangle B$, $x \in A \triangle B = (A \setminus B) \cup (B \setminus A)$, so either $x \in A$ and $x \notin B$ or $x \in B$ and $x \notin A$. Thus either $x \in A$ or $x \in B$, so $x \in A \cup B$. Since x was arbitrary, this shows that $C \subseteq A \cup B$. Now suppose $A \cap B \cap C \neq \varnothing$. Then we can choose some x such that $x \in A$, $x \in B$, and $x \in C$. Since $x \in C$ and $C \subseteq A \triangle B$, $x \in A \triangle B$, so as before either $x \in A$ and $x \notin B$ or $x \in B$ and $x \notin A$. So either $x \notin A$ or $x \notin B$, which contradicts the fact that $x \in A$ and $x \in B$. Therefore $A \cap B \cap C = \varnothing$.

($\leftarrow$) Suppose $C \subseteq A \cup B$ and $A \cap B \cap C = \varnothing$. Let $x \in C$ be arbitrary. Then since $C \subseteq A \cup B$, $x \in A \cup B$, so either $x \in A$ or $x \in B$.

Case 1. $x \in A$. If $x \in B$ then $x \in A \cap B \cap C$, which contradicts the fact that $A \cap B \cap C = \varnothing$. Therefore $x \notin B$, so $x \in A \setminus B$ and therefore $x \in A \triangle B$.

Case 2. $x \in B$. Then a similar argument shows that $x \in B \setminus A$, so $x \in A \triangle B$.

Since x was arbitrary, this shows that $C \subseteq A \triangle B$.

23. (a) Suppose $x \in A \setminus C$. Then $x \in A$ and $x \notin C$.

Case 1. $x \in B$. Then since $x \notin C$, $x \in B \setminus C$, so $x \in (A \setminus B) \cup (B \setminus C)$.

Case 2. $x \notin B$. Then since $x \in A$, $x \in A \setminus B$, so $x \in (A \setminus B) \cup (B \setminus C)$.

Since x was arbitrary, we conclude that $A \setminus C \subseteq (A \setminus B) \cup (B \setminus C)$.

(b) Suppose $x \in A \triangle C$. Then either $x \in A \setminus C$ or $x \in C \setminus A$.

Case 1. $x \in A \setminus C$. Then by part (a), $x \in (A \setminus B) \cup (B \setminus C)$, so either $x \in A \setminus B$ or $x \in B \setminus C$. But if $x \in A \setminus B$ then $x \in A \triangle B$ and if $x \in B \setminus C$ then $x \in B \triangle C$, so either $x \in A \triangle B$ or $x \in B \triangle C$. Therefore $x \in (A \triangle B) \cup (B \triangle C)$.

Case 2. $x \in C \setminus A$. A similar argument shows that either $x \in B \setminus A$ or $x \in C \setminus B$, so $x \in (A \triangle B) \cup (B \triangle C)$.

Since x was arbitrary, $A \triangle C \subseteq (A \triangle B) \cup (B \triangle C)$.

24. (a) Suppose $x \in (A \cup B) \triangle C$. Then either $x \in (A \cup B) \setminus C$ or $x \in C \setminus (A \cup B)$.

Case 1. $x \in (A \cup B) \setminus C$. Then either $x \in A$ or $x \in B$, and $x \notin C$. We now break case 1 into two subcases, depending on whether $x \in A$ or $x \in B$:

Case 1a. $x \in A$. Then $x \in A \setminus C$, so $x \in A \triangle C$, so $x \in (A \triangle C) \cup (B \triangle C)$.

Case 1b. $x \in B$. Similarly, $x \in B \triangle C$, so $x \in (A \triangle C) \cup (B \triangle C)$.

Case 2. $x \in C \setminus (A \cup B)$. Then $x \in C$, $x \notin A$, and $x \notin B$. It follows that $x \in A \triangle C$ and $x \in B \triangle C$, so certainly $x \in (A \triangle C) \cup (B \triangle C)$.

(b) Here is one example: $A = \{1\}$, $B = \{2\}$, $C = \{1, 2\}$.

25. (a) Suppose $x \in (A \triangle C) \cap (B \triangle C)$. Then either $x \in A \setminus C$ or $x \in C \setminus A$, and also either $x \in B \setminus C$ or $x \in C \setminus B$.

    Case 1. $x \in C$. Then $x \notin A \setminus C$, so $x \in C \setminus A$, which implies that $x \notin A$. Since $x \notin A$, $x \notin A \cap B$. Therefore $x \in C \setminus (A \cap B)$, so $x \in (A \cap B) \triangle C$.

    Case 2. $x \notin C$. Then $x \notin C \setminus A$, so $x \in A \setminus C$, which implies that $x \in A$. Similarly, $x \notin C \setminus B$, so $x \in B \setminus C$ and therefore $x \in B$. Since $x \in A$, $x \in B$, and $x \notin C$, $x \in (A \cap B) \setminus C$, so $x \in (A \cap B) \triangle C$.

    Since x was arbitrary, this shows that $(A \triangle C) \cap (B \triangle C) \subseteq (A \cap B) \triangle C$.

    (b) No. One counterexample is $A = \{1\}$, $B = \{2\}$, $C = \{1, 2\}$.

26. $(A \triangle C) \setminus (B \triangle C) \subseteq (A \setminus B) \triangle C$, but the two sets are not always equal. To prove the subset statement, suppose $x \in (A \triangle C) \setminus (B \triangle C)$. Then $x \in A \triangle C$ and $x \notin B \triangle C$.

    Case 1. $x \in C$. Then since $x \in A \triangle C$, $x \notin A$. Therefore $x \notin A \setminus B$, so $x \in (A \setminus B) \triangle C$.

    Case 2. $x \notin C$. Then since $x \in A \triangle C$, $x \in A$, and since $x \notin B \triangle C$, $x \notin B$. Therefore $x \in A \setminus B$, so $x \in (A \setminus B) \triangle C$.

    Since x was an arbitrary element of $(A \triangle C) \setminus (B \triangle C)$, $(A \triangle C) \setminus (B \triangle C) \subseteq (A \setminus B) \triangle C$.

    To show that the sets need not be equal, we just need a counterexample. One counterexample is $A = \{1\}$, $B = \{1\}$, $C = \{1\}$.

27. The proof is incorrect, because it only establishes that either $0 < x$ or $x < 6$, but what must be proven is that $0 < x$ and $x < 6$. However, it can be fixed. In case 1 we have $x - 3 \geq 0$, so $x \geq 3 > 0$. Since the proof for this case already establishes $x < 6$, we have $0 < x < 6$. In case 2 we have $x - 3 < 0$, so $x < 3 < 6$, and the proof already shows $0 < x$, so $0 < x < 6$. Thus, the theorem is correct.

28. The proof is correct. When the statement $A \nsubseteq C$ is reexpressed as a positive statement it is an existential statement, so the proof uses existential instantiation to introduce x. Since $A \setminus B \subseteq C$, $x \in A \setminus B \to x \in C$. The proof uses modus tollens to conclude $x \notin A \setminus B$, and when this statement is reexpressed as a positive statement it becomes a disjunction. The proof then uses our last strategy for givens of the form $P \vee Q$ to conclude $x \in B$. Finally, when the goal $A \cap B \neq \varnothing$ is expressed as a positive statement it is an existential statement, and the proof establishes this by showing that x is an instance of the existential statement.

29. The proof is correct. Since the goal is a universal statement, the proof starts by introducing x as an arbitrary object. Then the proof proceeds by cases. In each case, the existential statement $\exists y \in \mathbb{R}(xy^2 \neq y - x)$ is proven by giving an example of the required real number y.

30. Suppose $\forall x P(x) \to \exists x Q(x)$.

    Case 1. $\forall x P(x)$. Then by our assumption, $\exists x Q(x)$, so we can choose some object a such that $Q(a)$. Since $Q(a)$ is true, $P(a) \to Q(a)$. Therefore $\exists x(P(x) \to Q(x))$.

    Case 2. $\neg \forall x P(x)$. Then $\exists x \neg P(x)$, so we can choose some a such that $\neg P(a)$. Since $P(a)$ is false, $P(a) \to Q(a)$. Therefore $\exists x(P(x) \to Q(x))$.

31. The proof is incorrect. In case 1, we cannot conclude that for all $x \in A$, $x \in B$. All we can say is that for all $x \in A$ *that fall under case 1*, $x \in B$. Similarly, in case 2 we cannot conclude that $\forall x \in A(x \in C)$.

    One way to understand the problem is to think about the structure of the proof. The proof begins with "Let x be an arbitrary element of A," but this beginning is inappropriate because the goal is not a universal statement. The goal is the disjunction $A \subseteq B \vee A \subseteq C$, so it would be appropriate to use proof by cases, proving $A \subseteq B$ in one case and $A \subseteq C$ in the other. But to use that strategy the proof should be structured like this:

    Case 1. _____
    Let x be an arbitrary element of A.
    [Proof of $x \in B$ goes here.]
    Since x was arbitrary, we can conclude that $A \subseteq B$.

Case 2. _____
Let x be an arbitrary element of A.
[Proof of $x \in C$ goes here.]
Since x was arbitrary, we can conclude that $A \subseteq C$.
Since these cases are exhaustive, either $A \subseteq B$ or $A \subseteq C$.

Notice that the arbitrary objects called x are introduced within each case. Therefore the division into cases cannot be based on a property of x, since x has not yet been introduced when the proof is broken into cases.

The proof cannot be fixed, because the theorem is false. Here is a counterexample to the theorem: $A = \{1, 2\}$, $B = \{1\}$, $C = \{2\}$.

32. Suppose $A \nsubseteq B$. Then we can choose some $a \in A$ such that $a \notin B$. Since $a \in A$ and $A \subseteq B \cup C$, $a \in B \cup C$, so either $a \in B$ or $x \in C$. But we also know $a \notin B$, so $a \in C$. Since $a \in A$ and $a \in C$, $A \cap C \neq \varnothing$. Thus, either $A \subseteq B$ or $A \cap C \neq \varnothing$.

33. Case 1. $\forall y P(y)$. Since we have assumed the universe of discourse is not the empty set, we can let a be some element of the universe of discourse. Then since $\forall y P(y)$ is true, $P(a) \to \forall y P(y)$, so $\exists x(P(x) \to \forall y P(y))$.
Case 2. $\neg\forall y P(y)$. Then $\exists x \neg P(x)$, so we can choose some object a such that $P(a)$ is false. Therefore $P(a) \to \forall y P(y)$ is true, so $\exists x(P(x) \to \forall y P(y))$.

Section 3.6

1. Let x be an arbitrary real number. Let $y = x/(x^2 + 1)$. Then

$$x - y = x - \frac{x}{x^2+1} = \frac{x^3 + x}{x^2 + 1} - \frac{x}{x^2+1} = \frac{x^3}{x^2+1} = x^2 \cdot \frac{x}{x^2+1} = x^2 y.$$

To see that y is unique, suppose that $x^2 z = x - z$. Then $z(x^2 + 1) = x$, and since $x^2 + 1 \neq 0$, we can divide both sides by $x^2 + 1$ to conclude that $z = x/(x^2 + 1) = y$.

2. Let $x = 4$. Let y be an arbitrary real number. Then $xy + x - 4 = 4y + 4 - 4 = 4y$.
To prove that x is unique, suppose z is a real number such that for every real number y, $zy + z - 4 = 4y$. Then in particular, setting $y = 0$ we get $z - 4 = 0$, so $z = 4 = x$.

3. Let x be an arbitrary real number, and assume that $x \neq 0$ and $x \neq 1$. Let $y = x^2/(x - 1)$, which is defined since $x \neq 1$. Then

$$y - x = \frac{x^2}{x-1} - x = \frac{x^2}{x-1} - \frac{x^2 - x}{x-1} = \frac{x}{x-1} = \frac{\frac{x^2}{x-1}}{x} = \frac{y}{x}.$$

To see that y is unique, suppose that z is a real number such that $z/x = z - x$. Multiplying both sides by x, we conclude that $z = zx - x^2$, so $x^2 = z(x - 1)$ and therefore $z = x^2/(x - 1) = y$.

4. Suppose $x \neq 0$. Let $y = 1/x$. Now let z be an arbitrary real number. Then $zy = z(1/x) = z/x$, as required.
To see that y is unique, suppose that y' is a number with the property that $\forall z \in \mathbb{R}(zy' = z/x)$. Then in particular, taking $z = 1$, we have $y' = 1/x$, so $y' = y$.

5. (a) Suppose $x \in \bigcup!\mathcal{F}$. Then $\exists! A(A \in \mathcal{F} \wedge x \in A)$, so we can let A be the unique set such that $A \in \mathcal{F}$ and $x \in A$. Since $x \in A$ and $A \in \mathcal{F}$, $x \in \bigcup \mathcal{F}$. Since x was arbitrary, $\bigcup!\mathcal{F} \subseteq \bigcup \mathcal{F}$.
(b) Let $\mathcal{F}$ be an arbitrary family of sets.
($\to$) Suppose $\bigcup!\mathcal{F} = \bigcup \mathcal{F}$. Let A and B be arbitrary elements of $\mathcal{F}$ and assume that $A \cap B \neq \varnothing$. Then we can choose some x such that $x \in A \cap B$, so $x \in A$ and $x \in B$. Since $x \in A$ and $A \in \mathcal{F}$,

$x \in \bigcup \mathcal{F}$. But $\bigcup! \mathcal{F} = \bigcup \mathcal{F}$, so we conclude that $x \in \bigcup! \mathcal{F}$, and therefore there is only one set in $\mathcal{F}$ that contains x as an element. Since $x \in A$ and $x \in B$, this implies that $A = B$. Since A and B were arbitrary, we conclude that $\mathcal{F}$ is pairwise disjoint.

($\leftarrow$) Suppose $\mathcal{F}$ is pairwise disjoint. We know from part (a) that $\bigcup! \mathcal{F} \subseteq \bigcup \mathcal{F}$, so we only need to show that $\bigcup \mathcal{F} \subseteq \bigcup! \mathcal{F}$. To prove this, suppose that $x \in \bigcup \mathcal{F}$. Then we can choose some $A \in \mathcal{F}$ such that $x \in A$. To see that A is unique, suppose $B \in \mathcal{F}$ and $x \in B$. Then since $x \in A$ and $x \in B$, $A \cap B \neq \varnothing$. Since $\mathcal{F}$ is pairwise disjoint, it follows that $B = A$. Therefore $x \in \bigcup! \mathcal{F}$.

6. (a) Let $A = \varnothing \in \mathscr{P}(U)$. Then clearly for any $B \in \mathscr{P}(U)$, $A \cup B = \varnothing \cup B = B$.

   To see that A is unique, suppose that $A' \in \mathscr{P}(U)$ and for all $B \in \mathscr{P}(U)$, $A' \cup B = B$. Then in particular, taking $B = \varnothing$, we can conclude that $A' \cup \varnothing = \varnothing$. But clearly $A' \cup \varnothing = A'$, so we have $A' = \varnothing = A$.

   (b) Let $A = U$. Let $B \in \mathscr{P}(U)$ be arbitrary. Then $B \subseteq U = A$, so $A \cup B = A$.

   To see that A is unique, suppose $A' \in \mathscr{P}(U)$ and $\forall B \in \mathscr{P}(U)(A' \cup B = A')$. In particular, since $U \in \mathscr{P}(U)$, $A' \cup U = A'$. But $A' \in \mathscr{P}(U)$, so $A' \subseteq U$ and therefore $A' \cup U = U$. Thus $A' = U = A$.

7. (a) Let $A = U$. Let $B \in \mathscr{P}(U)$ be arbitrary. Then $B \subseteq U = A$, so $A \cap B = B$.

   To see that A is unique, suppose $A' \in \mathscr{P}(U)$ and $\forall B \in \mathscr{P}(U)(A' \cap B = B)$. In particular, since $U \in \mathscr{P}(U)$, $A' \cap U = U$. But $A' \in \mathscr{P}(U)$, so $A' \subseteq U$ and therefore $A' \cap U = A'$. Thus $A' = U = A$.

   (b) Let $A = \varnothing$. Let $B \in \mathscr{P}(U)$ be arbitrary. Then $A \cap B = \varnothing \cap B = \varnothing = A$.

   To see that A is unique, suppose $A' \in \mathscr{P}(U)$ and $\forall B \in \mathscr{P}(U)(A' \cap B = A')$. Then in particular, since $\varnothing \in \mathscr{P}(U)$, $A' \cap \varnothing = A'$. But $A' \cap \varnothing = \varnothing$, so $A' = \varnothing = A$.

8. (a) Suppose $A \in \mathscr{P}(U)$. Let $B = U \setminus A$. Let $C \in \mathscr{P}(U)$ be arbitrary. Then $C \subseteq U$. We claim now that $C \setminus A = C \cap B$. To prove this, suppose that $x \in C \setminus A$. Then $x \in C$ and $x \notin A$. Since $x \in C$ and $C \subseteq U$, $x \in U$. Since $x \in U$ and $x \notin A$, $x \in U \setminus A = B$. Therefore $x \in C \cap B$.

   Now suppose $x \in C \cap B$. Then $x \in C$ and $x \in B = U \setminus A$, so $x \notin A$. Therefore $x \in C \setminus A$. This completes the proof that $C \setminus A = C \cap B$.

   Finally, we must prove that B is unique. So suppose that $B' \in \mathscr{P}(U)$ and $\forall C \in \mathscr{P}(U)(C \setminus A = C \cap B')$. In particular, $U \setminus A = U \cap B'$. But $B' \subseteq U$, so $U \cap B' = B'$. Therefore $B' = U \setminus A = B$.

   (b) Suppose $A \in \mathscr{P}(U)$. Let $B = U \setminus A$. Let $C \in \mathscr{P}(U)$ be arbitrary. Then $C \subseteq U$. We claim now that $C \cap A = C \setminus B$. To prove this, suppose that $x \in C \cap A$. Then $x \in C$ and $x \in A$. Since $x \in A$, $x \notin U \setminus A = B$, so $x \in C \setminus B$.

   Now suppose $x \in C \setminus B$. Then $x \in C$ and $x \notin B = U \setminus A$, so either $x \notin U$ or $x \in A$. But since $x \in C$ and $C \subseteq U$, $x \in U$. Therefore $x \in A$, so $x \in C \cap A$.

   Finally, we must prove that B is unique. So suppose that $B' \in \mathscr{P}(U)$ and $\forall C \in \mathscr{P}(U)(C \cap A = C \setminus B')$. Then in particular, $U \cap A = U \setminus B'$. Since $A \subseteq U$, $U \cap A = A$, so $U \setminus B' = A$. We claim now that $B' = U \setminus A$. To prove this, suppose $x \in B'$. Then $x \notin U \setminus B' = A$. Also, since $x \in B'$ and $B' \subseteq U$, $x \in U$. Thus $x \in U \setminus A$. Next, suppose $x \in U \setminus A$. Then $x \in U$ and $x \notin A = U \setminus B'$, so either $x \notin U$ or $x \in B'$. Since $x \in U$, $x \in B'$. This proves that $B' = U \setminus A = B$.

9. (a) Existence: Let $X = \varnothing$. Then for every set A, $A \triangle X = (A \setminus \varnothing) \cup (\varnothing \setminus A) = A \cup \varnothing = A$.

   Uniqueness: Suppose X_1 and X_2 are both identity elements for symmetric difference. Then $\forall A(A \triangle X_1 = A)$ and $\forall A(A \triangle X_2 = A)$. Applying the first statement to X_2 and the second to X_1 we conclude that $X_2 \triangle X_1 = X_2$ and $X_1 \triangle X_2 = X_1$. But $X_1 \triangle X_2 = X_2 \triangle X_1$, so $X_1 = X_2$.

   (b) Let A be an arbitrary set.

   Existence: Let $B = A$. Then $A \triangle B = (A \setminus A) \cup (A \setminus A) = \varnothing \cup \varnothing = \varnothing$.

   Uniqueness: Suppose B_1 and B_2 are both inverses of A. Then $A \triangle B_1 = A \triangle B_2 = \varnothing$, so

$$B_1 = B_1 \triangle \varnothing = B_1 \triangle (A \triangle B_2) = (B_1 \triangle A) \triangle B_2 = (A \triangle B_1) \triangle B_2 = \varnothing \triangle B_2 = B_2 \triangle \varnothing = B_2.$$

(c) Let A and B be arbitrary sets.
Existence: Let $C = A \triangle B$. Then

$$A \triangle C = A \triangle (A \triangle B) = (A \triangle A) \triangle B = \varnothing \triangle B = B.$$

Uniqueness: Suppose C_1 and C_2 are sets such that $A \triangle C_1 = A \triangle C_2 = B$. Then

$$C_1 = \varnothing \triangle C_1 = (A \triangle A) \triangle C_1 = A \triangle (A \triangle C_1) = A \triangle (A \triangle C_2) = (A \triangle A) \triangle C_2 = \varnothing \triangle C_2 = C_2.$$

(d) Let A be an arbitrary set. Let $B = A$. Suppose $C \subseteq A$. Then

$$B \triangle C = (A \setminus C) \cup (C \setminus A) = (A \setminus C) \cup \varnothing = A \setminus C.$$

To see that B is unique, suppose $B' \subseteq A$ and $\forall C \subseteq A(B' \triangle C = A \setminus C)$. Applying this statement with $C = \varnothing$ we get $B' \triangle \varnothing = A \setminus \varnothing = A$. But also $B' \triangle \varnothing = B'$, so $B' = A = B$.

10. Suppose first that $A = \varnothing$. Let $\mathcal{F} = \varnothing$. Then $\bigcup \mathcal{F} = \varnothing = A$, but $A \notin \mathcal{F}$, which is a contradiction. Therefore $A \neq \varnothing$, so A has at least one element. Let x be an element of A.
Now let $\mathcal{F} = \{\{x\}, A \setminus \{x\}\}$. Then $\bigcup \mathcal{F} = \{x\} \cup (A \setminus \{x\}) = A$, so by assumption $A \in \mathcal{F}$, and therefore either $A = \{x\}$ or $A = A \setminus \{x\}$. But clearly $A \neq A \setminus \{x\}$, because $x \in A$ but $x \notin A \setminus \{x\}$. Therefore $A = \{x\}$, so A has exactly one element.

11. Existence: We are given that for every $\mathcal{G} \subseteq \mathcal{F}$, $\bigcup \mathcal{G} \in \mathcal{F}$, so in particular, since $\mathcal{F} \subseteq \mathcal{F}$, $\bigcup \mathcal{F} \in \mathcal{F}$. Let $A = \bigcup \mathcal{F}$. Now suppose $B \in \mathcal{F}$. Then by exercise 8 of Section 3.3, $B \subseteq \bigcup \mathcal{F} = A$, as required.
Uniqueness: Suppose that $A_1 \in \mathcal{F}$, $A_2 \in \mathcal{F}$, $\forall B \in \mathcal{F}(B \subseteq A_1)$, and $\forall B \in \mathcal{F}(B \subseteq A_2)$. Applying this last fact with $B = A_1$ we can conclude that $A_1 \subseteq A_2$, and similarly the previous fact implies that $A_2 \subseteq A_1$. Thus $A_1 = A_2$.

12. (a) $\exists x \exists y[P(x) \wedge P(y) \wedge x \neq y \wedge \forall z(P(z) \rightarrow (z = x \vee z = y))]$.
(b) To prove that there are exactly two values of x for which $P(x)$ is true, find two objects a and b such that you can prove $P(a)$, $P(b)$, $a \neq b$, and $\forall z(P(z) \rightarrow (z = a \vee z = b))$.
(c) First, note that 0 and 1 are clearly solutions to the equation, and of course $0 \neq 1$. Now suppose z is also a solution, so $z^3 = z^2$. If $z \neq 0$ then we can divide both sides of this equation by z^2 to conclude that $z = 1$. Therefore either $z = 0$ or $z = 1$.

13. (a) Let $c = 9/4$. Then the equation is $x^2 + 3x + 9/4 = 0$, or equivalently $(x + 3/2)^2 = 0$. The unique solution to this equation is $x = -3/2$.
To see that c is unique, suppose $c' \neq 9/4$, and consider the equation $x^2 + 3x + c' = 0$.
Case 1. $c' > 9/4$. Then the equation can be rewritten $(x + 3/2)^2 + (c' - 9/4) = 0$, and this equation has no solutions because for all values of x, $(x + 3/2)^2 \geq 0$ and $c' - 9/4 > 0$.
Case 2. $c' < 9/4$. Then by the quadratic formula the equation has the two solutions $x = (-3 \pm \sqrt{9 - 4c'})/2$, and these solutions are distinct because $9 - 4c' > 0$.
Thus, $c = 9/4$ is the only value of c for which the equation $x^2 + 3x + c = 0$ has exactly one solution.
(b) For every real number x, there is a unique value of c for which $x^2 + 3x + c = 0$, namely $c = -x^2 - 3x$. Thus, there is more than one real number x such that there is a unique real number c such that $x^2 + 3x + c = 0$, so it is not the case that there is a unique such real number x.

Section 3.7

1. Existence: Let $A = \bigcup \mathcal{F}$. To prove (a), let X be an arbitrary element of $\mathcal{F}$. By exercise 8 in Section 3.3, $X \subseteq \bigcup \mathcal{F} = A$, so $X \in \mathscr{P}(A)$. Since X was arbitrary, this shows that $\mathcal{F} \subseteq \mathscr{P}(A)$. To prove (b), let B be an arbitrary set and assume that $\mathcal{F} \subseteq \mathscr{P}(B)$. By exercise 16 in Section 3.3, $A = \bigcup \mathcal{F} \subseteq B$.

Uniqueness: Suppose A_1 and A_2 are sets satisfying (a) and (b). In other words, (a1) $\mathcal{F} \subseteq \mathscr{P}(A_1)$, (b1) $\forall B(\mathcal{F} \subseteq \mathscr{P}(B) \to A_1 \subseteq B)$, (a2) $\mathcal{F} \subseteq \mathscr{P}(A_2)$, and (b2) $\forall B(\mathcal{F} \subseteq \mathscr{P}(B) \to A_2 \subseteq B)$. By (a1), we can plug in A_1 for B in (b2) to conclude that $A_2 \subseteq A_1$. Similarly, using (a2) and (b1) we get $A_1 \subseteq A_2$, so $A_1 = A_2$.

2. Existence: Let $m = 1$. To prove (a), let x be an arbitrary positive real number. Then $x < x + 1$, so $x/(x + 1) < 1 = m$. To prove (b), suppose y is a positive real number and for every positive real number x, $x/(x + 1) < y$. Suppose $y < 1$. Let $x = y/(1 - y)$. Then x is a positive real number, so $x/(x + 1) < y$, but also
$$\frac{x}{x+1} = \frac{\frac{y}{1-y}}{\frac{y}{1-y}+1} = \frac{\frac{y}{1-y}}{\frac{1}{1-y}} = \frac{y}{1} = y.$$
This is a contradiction. Therefore $m = 1 \leq y$.

   Uniqueness: Suppose m_1 and m_2 are positive real numbers with properties (a) and (b). In other words, (a1) for every positive real number x, $x/(x+1) < m_1$, (b1) if y is any positive real number with the property that for every positive real number x, $x/(x+1) < y$, then $m_1 \leq y$, (a2) for every positive real number x, $x/(x + 1) < m_2$, and (b2) if y is any positive real number with the property that for every positive real number x, $x/(x + 1) < y$, then $m_2 \leq y$. By (a1) and (b2), $m_2 \leq m_1$, and by (a2) and (b1), $m_1 \leq m_2$. Therefore $m_1 = m_2$.

3. $\mathscr{P}(A \setminus B) \setminus (\mathscr{P}(A) \setminus \mathscr{P}(B)) = \{\varnothing\}$. Proof: Since $\varnothing$ is a subset of every set, $\varnothing \in \mathscr{P}(B)$, so $\varnothing \notin \mathscr{P}(A) \setminus \mathscr{P}(B)$, and also $\varnothing \in \mathscr{P}(A \setminus B)$. Therefore $\varnothing \in \mathscr{P}(A \setminus B) \setminus (\mathscr{P}(A) \setminus \mathscr{P}(B))$, so $\{\varnothing\} \subseteq \mathscr{P}(A \setminus B) \setminus (\mathscr{P}(A) \setminus \mathscr{P}(B))$. For the other direction, suppose $X \in \mathscr{P}(A \setminus B) \setminus (\mathscr{P}(A) \setminus \mathscr{P}(B))$. Then $X \in \mathscr{P}(A \setminus B)$, so $X \subseteq A \setminus B$, and $X \notin \mathscr{P}(A) \setminus \mathscr{P}(B)$. Clearly $A \setminus B \subseteq A$, so since $X \subseteq A \setminus B$, $X \subseteq A$, and therefore $X \in \mathscr{P}(A)$. Since $X \notin \mathscr{P}(A) \setminus \mathscr{P}(B)$, it follows that $X \in \mathscr{P}(B)$, so $X \subseteq B$. We claim now that $X = \varnothing$. To see why, suppose $x \in X$. Then since $X \subseteq A \setminus B$, $x \notin B$, and since $X \subseteq B$, $x \in B$, which is a contradiction. Therefore X cannot have any elements, so $X = \varnothing$. This proves that $\mathscr{P}(A \setminus B) \setminus (\mathscr{P}(A) \setminus \mathscr{P}(B)) \subseteq \{\varnothing\}$, so the two sets are equal.

4. (a) $\to$ (b). Suppose (a) is true. Suppose $x \in A \cap B$, which means $x \in A$ and $x \in B$. Suppose $x \notin C$. Then since $x \in A$ and $x \notin C$, $x \in A \setminus C$, so $x \in A \triangle C$. Similarly, $x \in B \triangle C$, so this contradicts (a). Therefore $x \in C$. Since x was an arbitrary element of $A \cap B$, this shows that $A \cap B \subseteq C$.

   Now suppose $x \in C$. Suppose $x \notin A \cup B$. Then $x \notin A$ and $x \notin B$. Since $x \in C$ and $x \notin A$, $x \in A \triangle C$. Similarly $x \in B \triangle C$, so this contradicts (a). Therefore $x \in A \cup B$. Since x was an arbitrary element of C, we conclude that $C \subseteq A \cup B$.

   (b) $\to$ (c). Suppose (b) is true. Suppose $x \in A \triangle C$. Then either $x \in A \setminus C$ or $x \in C \setminus A$.

   Case 1. $x \in A \setminus C$. Then $x \in A$ and $x \notin C$. If $x \in B$ then $x \in A \cap B$, so by (b), $x \in C$, which is a contradiction. Therefore $x \notin B$. Since $x \in A$ and $x \notin B$, $x \in A \triangle B$.

   Case 2. $x \in C \setminus A$. Then $x \in C$ and $x \notin A$. By (b), since $x \in C$, $x \in A \cup B$. But then since $x \notin A$, $x \in B$. Since $x \in B$ and $x \notin A$, $x \in A \triangle B$.

   Thus, $x \in A \triangle B$. Since x was an arbitrary element of $A \triangle C$, this shows that $A \triangle C \subseteq A \triangle B$.

   (c) $\to$ (a). Suppose (c) is true. Suppose $(A \triangle C) \cap (B \triangle C) \neq \varnothing$. Then we can choose some $x \in (A \triangle C) \cap (B \triangle C)$, so $x \in A \triangle C$ and $x \in B \triangle C$. By (c), since $x \in A \triangle C$, $x \in A \triangle B$.

   Case 1. $x \in C$. Since $x \in A \triangle C$ and $x \in B \triangle C$, it follows that $x \notin A$ and $x \notin B$, which contradicts $x \in A \triangle B$.

   Case 2. $x \notin C$. Since $x \in A \triangle C$ and $x \in B \triangle C$, it follows that $x \in A$ and $x \in B$, which contradicts $x \in A \triangle B$.

   Thus we have reached a contradiction, so $(A \triangle C) \cap (B \triangle C) = \varnothing$.

5. Suppose $\mathscr{P}(\bigcup_{i \in l} A_i) \subseteq \bigcup_{i \in l} \mathscr{P}(A_i)$. It is clear that $\bigcup_{i \in l} A_i \subseteq \bigcup_{i \in l} A_i$, so $\bigcup_{i \in l} A_i \in \mathscr{P}(\bigcup_{i \in l} A_i)$ and therefore $\bigcup_{i \in l} A_i \in \bigcup_{i \in l} \mathscr{P}(A_i)$. By the definition of the union of a family, this means that we can choose some $i \in I$ such that $\bigcup_{i \in l} A_i \subseteq A_i$. Now let $j \in I$ be arbitrary. Then by exercise 8 in Section 3.3, $A_j \subseteq \bigcup_{i \in l} A_i$, so $A_j \subseteq A_i$.

6. (a) Suppose $x \in \bigcup_{i\in I} A_i$. Then we can choose some $i_0 \in I$ such that $x \in A_{i_0}$. Since $i_0 \in I$ and $I = \bigcup \mathcal{F}$, we can choose some $X_0 \in \mathcal{F}$ such that $i_0 \in X_0$. Since $x \in A_{i_0}$ and $i_0 \in X_0$, $x \in \bigcup_{i\in X_0} A_i$, and since $X_0 \in \mathcal{F}$ it follows that $x \in \bigcup_{X\in\mathcal{F}}(\bigcup_{i\in X} A_i)$.

   Next, suppose $x \in \bigcup_{X\in\mathcal{F}}(\bigcup_{i\in I} A_i)$. Then we can choose some $X_0 \in \mathcal{F}$ such that $x \in \bigcup_{i\in X_0} A_i$, which implies that we can choose $i_0 \in X_0$ such that $x \in A_{i_0}$. Since $i_0 \in X_0$ and $X_0 \in \mathcal{F}$, $i_0 \in \bigcup \mathcal{F} = I$. Since $x \in A_{i_0}$, it follows that $x \in \bigcup_{i\in I} A_i$.

   (b) Suppose $x \in \bigcap_{i\in I} A_i$. Let $X \in \mathcal{F}$ be arbitrary. Let $i \in X$ be arbitrary. Then since $i \in X$ and $X \in \mathcal{F}$, $i \in \bigcup \mathcal{F} = I$. Since $x \in \bigcap_{i\in I} A_i$, it follows that $x \in A_i$. Since i was arbitrary, we can conclude that $x \in \bigcap_{i\in X} A_i$. Since X was arbitrary, it follows that $x \in \bigcap_{X\in\mathcal{F}}(\bigcap_{i\in X} A_i)$.

   Now suppose $x \in \bigcap_{X\in\mathcal{F}}(\bigcap_{i\in X} A_i)$. Let $i \in I$ be arbitrary. Since $I = \bigcup \mathcal{F}$, this means that we can choose $X_0 \in \mathcal{F}$ such that $i \in X_0$. Since $x \in \bigcap_{X\in\mathcal{F}}(\bigcap_{i\in X} A_i)$ and $X_0 \in \mathcal{F}$, $x \in \bigcap_{i\in X_0} A_i$. But then since $i \in X_0$, $x \in A_i$. Since i was arbitrary, we can conclude that $x \in \bigcap_{i\in I} A_i$.

   (c) Suppose $x \in \bigcup_{i\in J} A_i$. Then we can choose some $j \in J$ such that $x \in A_j$. Let $X \in \mathcal{F}$ be arbitrary. Since $j \in J = \bigcap \mathcal{F}$ and $X \in \mathcal{F}$, $j \in X$. Since $j \in X$ and $x \in A_j$, $x \in \bigcup_{i\in X} A_i$. Since X was arbitrary, this shows that $x \in \bigcap_{X\in\mathcal{F}}(\bigcup_{i\in X} A_i)$.

   The two sets are not always equal. Here's an example in which they are not equal: $\mathcal{F} = \{\{1,2\},\{2,3\}\}$, $A_1 = \{a\}$, $A_2 = \{b\}$, $A_3 = \{a\}$.

   (d) $\bigcup_{X\in\mathcal{F}}(\bigcap_{i\in X} A_i) \subseteq \bigcap_{i\in J} A_i$. Proof: Suppose $x \in \bigcup_{X\in\mathcal{F}}(\bigcap_{i\in X} A_i)$. Then we can choose some $X_0 \in \mathcal{F}$ such that $x \in \bigcap_{i\in X_0} A_i$. Now let $j \in J$ be arbitrary. Since $J = \bigcap \mathcal{F}$ and $X_0 \in \mathcal{F}$, this implies that $j \in X_0$. Since $x \in \bigcap_{i\in X_0} A_i$, it follows that $x \in A_j$. Since j was arbitrary, we conclude that $x \in \bigcap_{i\in J} A_i$.

   The two sets need not be equal. The example from part (c) shows this.

7. Suppose $\epsilon > 0$. Let $\delta = \epsilon/3$, which is also clearly positive. Let x be an arbitrary real number, and suppose that $0 < |x-2| < \delta$. Since $|x-2| > 0$, $x \neq 2$, so $(3x^2-12)/(x-2)$ is defined, and

$$\left|\frac{3x^2-12}{x-2} - 12\right| = \left|\frac{3(x+2)(x-2)}{x-2} - 12\right| = |3(x+2)-12| = |3x-6| = 3|x-2| < 3\delta = 3\left(\frac{\epsilon}{3}\right) = \epsilon.$$

8. Suppose that $\lim_{x\to c} f(x) = L > 0$. Let $\epsilon = L$. Then by the definition of limit, we can choose some $\delta > 0$ such that for all x, if $0 < |x-c| < \delta$ then $|f(x)-L| < \epsilon = L$. Now let x be an arbitrary real number and suppose $0 < |x-c| < \delta$. Then $|f(x)-L| < L$, so $-L < f(x)-L < L$ and therefore $0 < f(x) < 2L$. Therefore, for every real number x, if $0 < |x-c| < \delta$ then $f(x) > 0$.

9. Suppose $\epsilon > 0$. Then $\epsilon/7 > 0$, so since $\lim_{x\to c} f(x) = L$, we can choose some $\delta > 0$ such that for all x, if $0 < |x-c| < \delta$ then $|f(x)-L| < \epsilon/7$. Now let x be an arbitrary real number and suppose $0 < |x-c| < \delta$. Then $|f(x)-L| < \epsilon/7$, so $|7f(x)-7L| = 7|f(x)-L| < 7(\epsilon/7) = \epsilon$.

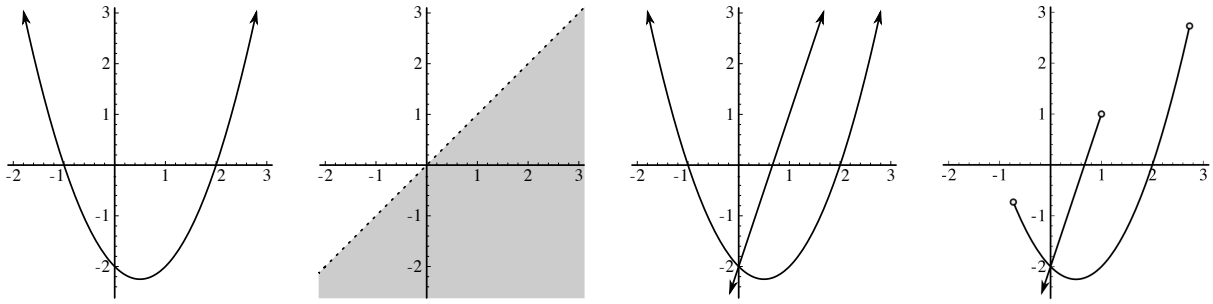
10. The proof is correct. The proof uses proof by cases. Within each case, the proof proves an existential statement by giving a specific instance of the statement that is true.

Chapter 4

Section 4.1

1. (a) $\{(x,y) \in P \times P \mid x \text{ is a parent of } y\} = \{(\text{Bill Clinton, Chelsea Clinton}), (\text{Goldie Hawn, Kate Hudson}), \dots\}$.

   (b) $\{(x,y) \in C \times U \mid \text{there is someone who lives in } x \text{ and attends } y\}$. If you are a university student, then let x be the city you live in, and let y be the university you attend; (x,y) will then be an element of this truth set.



(a) (b) (c) (d)

Figure 1: Truth sets for exercise 3.

2. (a) $\{(x, y) \in P \times C \mid x \text{ lives in } y\}$. For example, if you live in some city c, then (you, c) is an element of this truth set.
   (b) $\{(x, y) \in C \times \mathbb{N} \mid \text{the population of } x \text{ is } y\} = \{(\text{Tokyo, } 37{,}468{,}302), (\text{Paris, } 10{,}900{,}952), \ldots\}$. (Population data from `worldpopulationreview.com`.)

3. For pictures, see Figure 1. Here are a few elements of each truth set:
   (a) $(-1, 0)$, $(0, -2)$, $(1, -2)$, $(2, 0)$.
   (b) $(1, 0)$, $(3, 1)$, $(0, -37)$.
   (c) $(1, -2)$, $(1, 1)$, $(0, -2)$.
   (d) $(1, -2)$, $(0, -2)$, $(-1, -5)$.

4. $A \times (B \cap C) = (A \times B) \cap (A \times C) = \{(1, 4), (2, 4), (3, 4)\}$,
   $A \times (B \cup C) = (A \times B) \cup (A \times C) = \{(1, 1), (2, 1), (3, 1), (1, 3), (2, 3), (3, 3), (1, 4), (2, 4), (3, 4)\}$,
   $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D) = \varnothing$,
   $(A \times B) \cup (C \times D) = \{(1, 1), (2, 1), (3, 1), (1, 4), (2, 4), (3, 4), (3, 5), (4, 5)\}$,
   $(A \cup C) \times (B \cup D) = \{(1, 1), (2, 1), (3, 1), (4, 1), (1, 4), (2, 4), (3, 4), (4, 4), (1, 5), (2, 5), (3, 5), (4, 5)\}$.

5. Proof of 2: For any ordered pair (x, y),

$$\begin{aligned}
(x, y) \in A \times (B \cup C) &\text{ iff } x \in A \wedge (y \in B \vee y \in C) && \text{(definitions of } \times, \cup) \\
&\text{iff } (x \in A \wedge y \in B) \vee (x \in A \wedge y \in C) && \text{(distributive law)} \\
&\text{iff } (x, y) \in (A \times B) \cup (A \times C) && \text{(definitions of } \times, \cup).
\end{aligned}$$

   Proof of 3: For any ordered pair (x, y),

$$\begin{aligned}
(x, y) \in (A \times B) \cap (C \times D) &\text{ iff } (x \in A \wedge y \in B) \wedge (x \in C \wedge y \in D) && \text{(definitions of } \times, \cap) \\
&\text{iff } (x \in A \wedge x \in C) \wedge (y \in B \wedge y \in D) && \text{(commutative, associative laws)} \\
&\text{iff } (x, y) \in (A \cap C) \times (B \cap D) && \text{(definitions of } \cap, \times).
\end{aligned}$$

6. The cases are not exhaustive. For example, it is possible that $x \in A$ and $y \in D$.

7. mn. To see why, imagine writing the elements of $A \times B$ in a table with m rows and n columns.

8. Yes, it is true. Proof: Suppose $(x, y) \in A \times (B \setminus C)$. Then $x \in A$ and $y \in B \setminus C$, so $y \in B$ and $y \notin C$. Since $x \in A$ and $y \in B$, $(x, y) \in A \times B$. Since $y \notin C$, $(x, y) \notin A \times C$. Therefore $(x, y) \in (A \times B) \setminus (A \times C)$.
   Now suppose $(x, y) \in (A \times B) \setminus (A \times C)$. Then $(x, y) \in A \times B$, so $x \in A$ and $y \in B$, and also $(x, y) \notin A \times C$, so either $x \notin A$ or $y \notin C$. But we already know $x \in A$, so $y \notin C$. Since $y \in B$ and $y \notin C$, $y \in B \setminus C$, so $(x, y) \in A \times (B \setminus C)$.

9. $$\begin{aligned} A \times (B \triangle C) &= A \times ((B \setminus C) \cup (C \setminus B)) && \text{(definition of } \triangle) \\ &= (A \times (B \setminus C)) \cup (A \times (C \setminus B)) && \text{(Theorem 4.1.3, part 2)} \\ &= ((A \times B) \setminus (A \times C)) \cup ((A \times C) \setminus (A \times B)) && \text{(exercise 8)} \\ &= (A \times B) \triangle (A \times C) && \text{(definition of } \triangle). \end{aligned}$$

10. Suppose $(x, y) \in (A \setminus C) \times (B \setminus D)$. Then $x \in A \setminus C$ and $y \in B \setminus D$, which means $x \in A$, $x \notin C$, $y \in B$, and $y \notin D$. Since $x \in A$ and $y \in B$, $(x, y) \in A \times B$. And since $x \notin C$, $(x, y) \notin C \times D$. Therefore $(x, y) \in (A \times B) \setminus (C \times D)$.

11. Suppose $(x, y) \in (A \times B) \setminus (C \times D)$. Then $(x, y) \in A \times B$, so $x \in A$ and $y \in B$, and also $(x, y) \notin C \times D$, so either $x \notin C$ or $y \notin D$.

    Case 1. $x \notin C$. Then since $x \in A$ and $x \notin C$, $x \in A \setminus C$. Since we also have $y \in B$, $(x, y) \in (A \setminus C) \times B$, so $(x, y) \in [A \times (B \setminus D)] \cup [(A \setminus C) \times B]$.

    Case 2. $y \notin D$. Then since $y \in B$ and $y \notin D$, $y \in B \setminus D$. Since we also have $x \in A$, $(x, y) \in A \times (B \setminus D)$, so $(x, y) \in [A \times (B \setminus D)] \cup [(A \setminus C) \times B]$.

    Since these cases are exhaustive, $(x, y) \in [A \times (B \setminus D)] \cup [(A \setminus C) \times B]$.

    Now suppose $(x, y) \in [A \times (B \setminus D)] \cup [(A \setminus C) \times B]$. Then either $(x, y) \in A \times (B \setminus D)$ or $(x, y) \in (A \setminus C) \times B$.

    Case 1. $(x, y) \in A \times (B \setminus D)$. Then $x \in A$ and $y \in B \setminus D$, so $y \in B$ and $y \notin D$. Since $x \in A$ and $y \in B$, $(x, y) \in A \times B$, and since $y \notin D$, $(x, y) \notin C \times D$. Therefore $(x, y) \in (A \times B) \setminus (C \times D)$.

    Case 2. $(x, y) \in (A \setminus C) \times B$. Then $x \in A \setminus C$, so $x \in A$ and $x \notin C$, and also $y \in B$. Since $x \in A$ and $y \in B$, $(x, y) \in A \times B$, and since $x \notin C$, $(x, y) \notin C \times D$. Therefore $(x, y) \in (A \times B) \setminus (C \times D)$.

    Thus $(x, y) \in (A \times B) \setminus (C \times D)$.

12. Suppose $A \times B$ and $C \times D$ are disjoint. Suppose A and C are not disjoint, and also B and D are not disjoint. Then we can choose some $x \in A \cap C$ and $y \in B \cap D$. But then $(x, y) \in A \times B$ and also $(x, y) \in C \times D$, which contradicts the fact that $A \times B$ and $C \times D$ are disjoint. Therefore either A and C are disjoint or B and D are disjoint.

13. Let the indexed family $\{A_i \mid i \in I\}$ and the set B be arbitrary. Suppose $(x, y) \in (\bigcap_{i \in I} A_i) \times B$. Then $x \in \bigcap_{i \in I} A_i$ and $y \in B$. Now let $i \in I$ be arbitrary. Since $x \in \bigcap_{i \in I} A_i$ and $i \in I$, $x \in A_i$. Therefore $(x, y) \in A_i \times B$. Since i was arbitrary, $(x, y) \in \bigcap_{i \in I} (A_i \times B)$.

    Now suppose $(x, y) \in \bigcap_{i \in I} (A_i \times B)$. Since $I \neq \varnothing$, we can choose some $i_0 \in I$. Since $(x, y) \in \bigcap_{i \in I} (A_i \times B)$, $(x, y) \in A_{i_0} \times B$, so $y \in B$. Now let $i \in I$ be arbitrary. Then since $(x, y) \in \bigcap_{i \in I} (A_i \times B)$, $(x, y) \in A_i \times B$, so $x \in A_i$. Since i was arbitrary, $x \in \bigcap_{i \in I} A_i$. Since we also have $y \in B$, $(x, y) \in (\bigcap_{i \in I} A_i) \times B$.

14. (a) Suppose $(x, y) \in \bigcup_{i \in I} (A_i \times B_i)$. Then we can choose some $i_0 \in I$ such that $(x, y) \in A_{i_0} \times B_{i_0}$, so $x \in A_{i_0}$ and $y \in B_{i_0}$. Since $x \in A_{i_0}$ and $i_0 \in I$, $x \in \bigcup_{i \in I} A_i$, and similarly since $y \in B_{i_0}$, $y \in \bigcup_{i \in I} B_i$. Therefore $(x, y) \in (\bigcup_{i \in I} A_i) \times (\bigcup_{i \in I} B_i)$.

    (b) Suppose $(x, y) \in \bigcup_{p \in P} C_p$. Then we can choose some $(i_0, i_1) \in P = I \times I$ such that $(x, y) \in C_{(i_0, i_1)} = A_{i_0} \times B_{i_1}$. Therefore $x \in A_{i_0}$ and $y \in B_{i_1}$, so $x \in \bigcup_{i \in I} A_i$ and $y \in \bigcup_{i \in I} B_i$, and thus $(x, y) \in (\bigcup_{i \in I} A_i) \times (\bigcup_{i \in I} B_i)$.

    Now suppose $(x, y) \in (\bigcup_{i \in I} A_i) \times (\bigcup_{i \in I} B_i)$. Then $x \in \bigcup_{i \in I} A_i$ and $y \in \bigcup_{i \in I} B_i$, so we can choose i_0 and i_1 in I such that $x \in A_{i_0}$ and $y \in B_{i_1}$. Therefore $(x, y) \in A_{i_0} \times B_{i_1} = C_{(i_0, i_1)}$ and $(i_0, i_1) \in I \times I = P$, so $(x, y) \in \bigcup_{p \in P} C_p$.

15. The theorem is incorrect. Counterexample: $A = \{1\}$, $B = C = D = \varnothing$. To understand the mistake in the proof, it is helpful to discuss how the proof should have been structured. After we suppose that $A \times B \subseteq C \times D$, the goal is $(A \subseteq C) \wedge (B \subseteq D)$, so the rest of the proof should be structured as follows:

    Let a be an arbitrary element of A.
    [Proof that $a \in C$ goes here.]

Since a was arbitrary, $A \subseteq C$.
Let b be an arbitrary element of B.
[Proof that $b \in D$ goes here.]
Since b was arbitrary, $B \subseteq D$.
Therefore $A \subseteq C$ and $B \subseteq D$.

Notice that the proofs that $A \subseteq C$ and $B \subseteq D$ should be separate; each must stand on its own. The proof violates this by using the arbitrary object b in the proof that $A \subseteq C$ and using the arbitrary object a in the proof that $B \subseteq D$.

Section 4.2

1. (a) Domain $= \{p \in P \mid p$ has a living child$\}$; Range $= \{p \in P \mid p$ has a living parent$\}$.
   (b) Domain $= \mathbb{R}$; Range $= \mathbb{R}^+$.
2. (a) Domain $= \{p \in P \mid p$ is male and has a living sibling$\}$; Range $= \{p \in P \mid p$ has a male living sibling$\}$.
   (b) Domain $= \{x \in \mathbb{R} \mid x \geq 1$ or $x \leq -1\}$; Range $= \{x \in \mathbb{R} \mid -1 < x < 1\}$.
3. (a) $L^{-1} \circ L = \{(s,t) \in S \times S \mid \exists r \in R((s,r) \in L \wedge (r,t) \in L^{-1})\} = \{(s,t) \in S \times S \mid \exists r \in R((s,r) \in L \wedge (t,r) \in L)\} = \{(s,t) \in S \times S \mid$ the students s and t live in the same dorm room$\}$.
   (b) $E \circ (L^{-1} \circ L) = \{(s,c) \in S \times C \mid \exists t \in S((s,t) \in L^{-1} \circ L \wedge (t,c) \in E)\} = \{(s,c) \in S \times C \mid$ someone who lives in the same dorm room as the student s is taking the course $c\}$.
4. (a) $M \circ E = \{(s,d) \in S \times D \mid \exists c \in C((s,c) \in E \wedge (c,d) \in M)\} = \{(s,d) \in S \times D \mid$ the student s is enrolled in some course that meets on the day $d\}$.
   (b) $M \circ T^{-1} = \{(p,d) \in P \times D \mid \exists c \in C((p,c) \in T^{-1} \wedge (c,d) \in M)\} = \{(p,d) \in P \times D \mid$ the professor p is teaching some course that meets on the day $d\}$.
5. (a) $S \circ R = \{(1,4),(1,5),(1,6),(2,4),(3,6)\}$.
   (b) $S \circ S^{-1} = \{(4,4),(5,5),(5,6),(6,5),(6,6)\}$.
6. (a) $S^{-1} \circ R = \{(1,4),(3,4),(3,5)\}$.
   (b) $R^{-1} \circ S = \{(4,1),(4,3),(5,3)\}$.
7. (a) First note that $\text{Ran}(R^{-1})$ and $\text{Dom}(R)$ are both subsets of A. Now let a be an arbitrary element of A. Then

$$\begin{aligned} a \in \text{Ran}(R^{-1}) &\text{ iff } \exists b \in B((b,a) \in R^{-1}) \\ &\text{iff } \exists b \in B((a,b) \in R) \text{ iff } a \in \text{Dom}\, R. \end{aligned}$$

   (b)

$$\begin{aligned} \text{Ran}(R^{-1}) &= \text{Dom}((R^{-1})^{-1}) && \text{(part 2)} \\ &= \text{Dom}(R) && \text{(part 1)}. \end{aligned}$$

   (c) Suppose $(a,d) \in (T \circ S) \circ R$. Then we can choose some $b \in B$ such that $(a,b) \in R$ and $(b,d) \in T \circ S$. Since $(b,d) \in T \circ S$, we can choose some $c \in C$ such that $(b,c) \in S$ and $(c,d) \in T$. Since $(a,b) \in R$ and $(b,c) \in S$, $(a,c) \in S \circ R$. And since $(a,c) \in S \circ R$ and $(c,d) \in T$, $(a,d) \in T \circ (S \circ R)$.
   (d) First note that $(S \circ R)^{-1}$ and $R^{-1} \circ S^{-1}$ are both relations from C to A. Now consider an arbitrary $(c,a) \in C \times A$. Then

$$\begin{aligned} (c,a) \in (S \circ R)^{-1} &\text{ iff } (a,c) \in S \circ R \\ &\text{iff } \exists b \in B((a,b) \in R \wedge (b,c) \in S) \\ &\text{iff } \exists b \in B((c,b) \in S^{-1} \wedge (b,a) \in R^{-1}) \\ &\text{iff } (c,a) \in R^{-1} \circ S^{-1}. \end{aligned}$$

8. $E \circ E \subseteq F$.

9. (a) Suppose $a \in \text{Dom}(S \circ R)$. Then we can choose some $c \in C$ such that $(a, c) \in S \circ R$, which means that we can choose some $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S$. Since $(a, b) \in R$, $a \in \text{Dom}(R)$.

   (b) Suppose $\text{Ran}(R) \subseteq \text{Dom}(S)$. We already know that $\text{Dom}(S \circ R) \subseteq \text{Dom}(R)$, so all we have to prove is that $\text{Dom}(R) \subseteq \text{Dom}(S \circ R)$. To prove this, suppose $a \in \text{Dom}(R)$. Then we can choose some $b \in B$ such that $(a, b) \in R$. Since $(a, b) \in R$, $b \in \text{Ran}(R)$, and since $\text{Ran}(R) \subseteq \text{Dom}(S)$, it follows that $b \in \text{Dom}(S)$. Thus, we can choose some $c \in C$ such that $(b, c) \in S$. Since $(a, b) \in R$ and $(b, c) \in S$, $(a, c) \in S \circ R$, and therefore $a \in \text{Dom}(S \circ R)$.

   (c) $\text{Ran}(S \circ R) \subseteq \text{Ran}(S)$, and if $\text{Dom}(S) \subseteq \text{Ran}(R)$ then $\text{Ran}(S \circ R) = \text{Ran}(S)$. Proof: Suppose $c \in \text{Ran}(S \circ R)$. Then we can choose some $a \in A$ such that $(a, c) \in S \circ R$. Therefore we can choose some $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S$. Since $(b, c) \in S$, $c \in \text{Ran}(S)$.

   Now suppose $\text{Dom}(S) \subseteq \text{Ran}(R)$, and suppose that $c \in \text{Ran}(S)$. Then we can choose some $b \in B$ such that $(b, c) \in S$. Therefore $b \in \text{Dom}(S)$, so since $\text{Dom}(S) \subseteq \text{Ran}(R)$, $b \in \text{Ran}(R)$, and therefore we can choose some $a \in A$ such that $(a, b) \in R$. Since $(a, b) \in R$ and $(b, c) \in S$, $(a, c) \in S \circ R$, so $c \in \text{Ran}(S \circ R)$.

10. (a) True. Proof: Suppose $(a, b) \in R$. Then $a \in \text{Dom}(R)$ and $b \in \text{Ran}(R)$, so $(a, b) \in \text{Dom}(R) \times \text{Ran}(R)$.

    (b) True. Proof: Suppose $R \subseteq S$, and suppose $(b, a) \in R^{-1}$. Then $(a, b) \in R$, so since $R \subseteq S$, $(a, b) \in S$, and therefore $(b, a) \in S^{-1}$.

    (c) True. Proof: Let (b, a) be an arbitrary element of $B \times A$. Then

$$\begin{aligned}
(b, a) \in (R \cup S)^{-1} &\text{ iff } (a, b) \in R \cup S && \text{(definition of inverse)} \\
&\text{iff } (a, b) \in R \vee (a, b) \in S && \text{(definition of } \cup\text{)} \\
&\text{iff } (b, a) \in R^{-1} \vee (b, a) \in S^{-1} && \text{(definition of inverse)} \\
&\text{iff } (b, a) \in R^{-1} \cup S^{-1} && \text{(definition of } \cup\text{).}
\end{aligned}$$

11. We prove the contrapositives of both directions.

    ($\rightarrow$) Suppose $\text{Ran}(R)$ and $\text{Dom}(S)$ are not disjoint. Then we can choose some $b \in \text{Ran}(R) \cap \text{Dom}(S)$. Since $b \in \text{Ran}(R)$, we can choose some $a \in A$ such that $(a, b) \in R$. Similarly, since $b \in \text{Dom}(S)$, we can choose some $c \in C$ such that $(b, c) \in S$. But then $(a, c) \in S \circ R$, so $S \circ R \neq \varnothing$.

    ($\leftarrow$) Suppose $S \circ R \neq \varnothing$. Then we can choose some $(a, c) \in S \circ R$. By definition of $S \circ R$, this means that we can choose some $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S$. But then $b \in \text{Ran}(R)$ and $b \in \text{Dom}(S)$, so $\text{Ran}(R)$ and $\text{Dom}(S)$ are not disjoint.

12. (a) Suppose $(a, c) \in (S \circ R) \setminus (T \circ R)$. Then $(a, c) \in S \circ R$ and $(a, c) \notin T \circ R$. Since $(a, c) \in S \circ R$, we can choose some $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S$. If $(b, c) \in T$ then $(a, c) \in T \circ R$, which is a contradiction. Therefore $(b, c) \notin T$, so $(b, c) \in S \setminus T$. Since $(a, b) \in R$ and $(b, c) \in S \setminus T$, $(a, c) \in (S \setminus T) \circ R$.

    (b) The mistake is in the sentence "Similarly, since $(a, b) \in R$ and $(b, c) \notin T$, $(a, c) \notin T \circ R$." We can't be sure that $(a, c) \notin T \circ R$, because there could be some $b' \in B$ such that $(a, b') \in R$ and $(b', c) \in T$.

    (c) No, it need not be true. Counterexample: $A = \{1\}$, $B = \{2, 3\}$, $C = \{4\}$, $R = \{(1, 2), (1, 3)\}$, $S = \{(2, 4)\}$, $T = \{(3, 4)\}$.

13. (a) True. Proof: Suppose R and S and disjoint, but R^{-1} and S^{-1} are not. Then we can choose some $(b, a) \in B \times A$ such that $(b, a) \in R^{-1}$ and $(b, a) \in S^{-1}$. But then $(a, b) \in R$ and $(a, b) \in S$, which contradicts the fact that R and S are disjoint. Therefore if R and S are disjoint then so are R^{-1} and S^{-1}.

(b) Not necessarily true. Counterexample: $A = \{1\}$, $B = \{2, 3\}$, $C = \{4\}$, $R = \{(1, 2)\}$, $S = \{(1, 3)\}$, $T = \{(2, 4), (3, 4)\}$.

(c) Not necessarily true. Counterexample: $A = \{1\}$, $B = \{2, 3\}$, $C = \{4\}$, $R = S = \{(1, 2)\}$, $T = \{(3, 4)\}$.

14. (a) True. Proof: Suppose $S \subseteq T$, and suppose $(a, c) \in S \circ R$. Then we can choose $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S$. Since $(b, c) \in S$ and $S \subseteq T$, $(b, c) \in T$. Since $(a, b) \in R$ and $(b, c) \in T$, $(a, c) \in T \circ R$.

(b) True. Proof: Suppose $(a, c) \in (S \cap T) \circ R$. Then we can choose some $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S \cap T$. Since $(b, c) \in S \cap T$, $(b, c) \in S$ and $(b, c) \in T$. Since $(a, b) \in R$ and $(b, c) \in S$, $(a, c) \in S \circ R$. Similarly, since $(a, b) \in R$ and $(b, c) \in T$, $(a, c) \in T \circ R$. Therefore $(a, c) \in (S \circ R) \cap (T \circ R)$.

(c) Not necessarily true. Counterexample: $A = \{1\}$, $B = \{2, 3\}$, $C = \{4\}$, $R = \{(1, 2), (1, 3)\}$, $S = \{(2, 4)\}$, $T = \{(3, 4)\}$.

(d) True. Proof: Suppose $(a, c) \in (S \cup T) \circ R$. Then we can choose some $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S \cup T$, which means either $(b, c) \in S$ or $(b, c) \in T$.

Case 1. $(b, c) \in S$. Since $(a, b) \in R$ and $(b, c) \in S$, $(a, c) \in S \circ R$, so $(a, c) \in (S \circ R) \cup (T \circ R)$.

Case 2. $(b, c) \in T$. Since $(a, b) \in R$ and $(b, c) \in T$, $(a, c) \in T \circ R$, so $(a, c) \in (S \circ R) \cup (T \circ R)$.

Therefore $(a, c) \in (S \circ R) \cup (T \circ R)$.

Now suppose $(a, c) \in (S \circ R) \cup (T \circ R)$. Then either $(a, c) \in S \circ R$ or $(a, c) \in T \circ R$.

Case 1. $(a, c) \in S \circ R$. Then we can choose some $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S$. Since $(b, c) \in S$, $(b, c) \in S \cup T$. Since $(a, b) \in R$ and $(b, c) \in S \cup T$, $(a, c) \in (S \cup T) \circ R$.

Case 2. $(a, c) \in T \circ R$. Then we can choose some $b \in B$ such that $(a, b) \in R$ and $(b, c) \in T$. Since $(b, c) \in T$, $(b, c) \in S \cup T$. Since $(a, b) \in R$ and $(b, c) \in S \cup T$, $(a, c) \in (S \cup T) \circ R$.

Therefore $(a, c) \in (S \cup T) \circ R$.

15. Let $E = B \cup C$. Then $B \subseteq E$ and $C \subseteq E$, so $R \subseteq A \times B \subseteq A \times E$ and $S \subseteq C \times D \subseteq E \times D$.

Now suppose E_1 and E_2 are two sets such that $R \subseteq A \times E_1$, $S \subseteq E_1 \times D$, $R \subseteq A \times E_2$, and $S \subseteq E_2 \times D$. Let

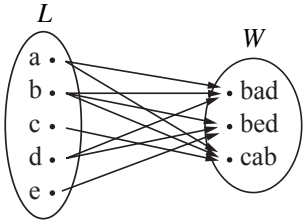
$$T_1 = \{(a, d) \in A \times D \mid \exists e \in E_1((a, e) \in R \wedge (e, d) \in S)\},$$
$$T_2 = \{(a, d) \in A \times D \mid \exists e \in E_2((a, e) \in R \wedge (e, d) \in S)\}.$$

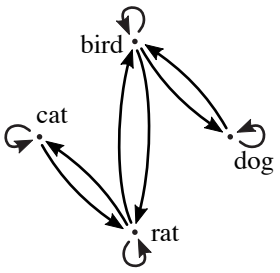
We must prove that $T_1 = T_2$.

Suppose $(a, d) \in T_1$. Then we can choose some $e \in E_1$ such that $(a, e) \in R$ and $(e, d) \in S$. Since $(a, e) \in R$ and $R \subseteq A \times E_2$, $(a, e) \in A \times E_2$, and therefore $e \in E_2$. Since $e \in E_2$, $(a, e) \in R$, and $(e, d) \in S$, $(a, d) \in T_2$. A similar argument shows that if $(a, d) \in T_2$ then $(a, d) \in T_1$, so $T_1 = T_2$.

Section 4.3

1.



2. 

R is reflexive and symmetric, but not transitive.

3. 

4. (a) $\{(a,c),(b,d),(c,c),(d,a),(d,b)\}$. Not reflexive, symmetric, or transitive.
   (b) $\{(a,b),(a,d),(b,a),(b,d)\}$. Not reflexive, symmetric, or transitive.
   (c) $\{(a,a),(b,b),(b,d),(c,c),(d,b),(d,d)\}$. Reflexive, symmetric, and transitive.
   (d) $\{(a,b),(a,c),(a,d),(b,d),(c,d)\}$. Not reflexive or symmetric, but transitive.

5. $S \circ R = \{(a,y),(a,z),(b,x),(c,y),(c,z)\}$.

6. $D_r \circ D_s = D_{r+s}$. Proof: Suppose $(x,y) \in D_r \circ D_s$. Then we can choose some real number z such that $(x,z) \in D_s$ and $(z,y) \in D_r$. This means that $|x-z| < s$ and $|z-y| < r$. Therefore by the triangle inequality,
$$|x-y| = |(x-z)+(z-y)| \leq |x-z| + |z-y| < r+s,$$
so $(x,y) \in D_{r+s}$.
   Now suppose $(x,y) \in D_{r+s}$. Then $|x-y| < r+s$. Let $z = (rx+sy)/(r+s)$. Then
$$|x-z| = \left|x - \frac{rx+sy}{r+s}\right| = \left|\frac{sx-sy}{r+s}\right| = \frac{s}{r+s}|x-y| < \frac{s}{r+s}\cdot(r+s) = s,$$
so $(x,z) \in D_s$, and also
$$|z-y| = \left|\frac{rx+sy}{r+s} - y\right| = \left|\frac{rx-ry}{r+s}\right| = \frac{r}{r+s}|x-y| < \frac{r}{r+s}\cdot(r+s) = r,$$
so $(z,y) \in D_r$. Therefore $(x,y) \in D_r \circ D_s$.

7. ($\rightarrow$) Suppose R is reflexive. Let (x,y) be an arbitrary element of i_A. Then by the definition of i_A, $x = y \in A$. Since R is reflexive, $(x,y) = (x,x) \in R$. Since (x,y) was arbitrary, this shows that $i_A \subseteq R$.
   ($\leftarrow$) Suppose $i_A \subseteq R$. Let $x \in A$ be arbitrary. Then $(x,x) \in i_A$, so since $i_A \subseteq R$, $(x,x) \in R$. Since x was arbitrary, this shows that R is reflexive.

8. ($\rightarrow$) Suppose R is transitive. Let (x,y) be an arbitrary element of $R \circ R$. Then we can choose some $z \in A$ such that $(x,z) \in R$ and $(z,y) \in R$. Since R is transitive, it follows that $(x,y) \in R$. Since (x,y) was arbitrary, this shows that $R \circ R \subseteq R$.
   ($\leftarrow$) Suppose $R \circ R \subseteq R$. Suppose $(x,y) \in R$ and $(y,z) \in R$. Then $(x,z) \in R \circ R$, and since $R \circ R \subseteq R$ it follows that $(x,z) \in R$. Since x, y, and z were arbitrary, this shows that R is transitive.

9. (a) Suppose R is a relation from A to B. Let (a,b) be an arbitrary element of $A \times B$. Suppose $(a,b) \in R \circ i_A$. Then we can choose some $x \in A$ such that $(a,x) \in i_A$ and $(x,b) \in R$. Since $(a,x) \in i_A$, $a = x$, and therefore $(a,b) = (x,b) \in R$.
   Now suppose $(a,b) \in R$. Since $(a,a) \in i_A$, $(a,b) \in R \circ i_A$. Thus, $R \circ i_a = R$.

(b) Suppose R is a relation from A to B. Let (a, b) be an arbitrary element of $A \times B$. Suppose $(a, b) \in i_B \circ R$. Then we can choose some $x \in B$ such that $(a, x) \in R$ and $(x, b) \in i_B$. Since $(x, b) \in i_B$, $b = x$, and therefore $(a, b) = (a, x) \in R$.

Now suppose $(a, b) \in R$. Since $(b, b) \in i_B$, $(a, b) \in i_B \circ R$. Thus, $i_B \circ R = R$.

10. Suppose $(x, y) \in i_D$. Then $x = y \in D = \text{Dom}(S)$, so there is some $z \in A$ such that $(x, z) \in S$. Therefore $(z, x) \in S^{-1}$, so $(x, y) = (x, x) \in S^{-1} \circ S$. Thus, $i_D \subseteq S^{-1} \circ S$. The proof of the other statement is similar.

11. Suppose R is a relation on A and R is reflexive. Suppose $(x, y) \in R$. Since R is reflexive, $(x, x) \in R$. Since $(x, x) \in R$ and $(x, y) \in R$, $(x, y) \in R \circ R$. Thus, $R \subseteq R \circ R$.

12. (a) Suppose R is reflexive. Let $x \in A$ be arbitrary. Since R is reflexive, $(x, x) \in R$, so $(x, x) \in R^{-1}$. Thus, R^{-1} is reflexive.

    (b) Suppose R is symmetric. Let $x, y \in A$ be arbitrary, and suppose $(x, y) \in R^{-1}$. Then $(y, x) \in R$. Since R is symmetric, $(x, y) \in R$, so $(y, x) \in R^{-1}$. Thus, R^{-1} is symmetric.

    (c) Suppose R is transitive. Let $x, y, z \in A$ be arbitrary, and suppose $(x, y) \in R^{-1}$ and $(y, z) \in R^{-1}$. Then $(z, y) \in R$ and $(y, x) \in R$. Since R is transitive, it follows that $(z, x) \in R$, so $(x, z) \in R^{-1}$. Thus, R^{-1} is transitive.

13. (a) Yes. Proof: Suppose R_1 and R_2 are reflexive, and suppose $a \in A$. Since R_1 is reflexive, $(a, a) \in R_1$, so $(a, a) \in R_1 \cup R_2$.

    (b) Yes. Proof: Suppose R_1 and R_2 are symmetric, and suppose $(x, y) \in R_1 \cup R_2$. Then either $(x, y) \in R_1$ or $(x, y) \in R_2$. If $(x, y) \in R_1$ then since R_1 is symmetric, $(y, x) \in R_1$, so $(y, x) \in R_1 \cup R_2$. Similar reasoning shows that if $(x, y) \in R_2$ then $(y, x) \in R_1 \cup R_2$.

    (c) No. Counterexample: $A = \{1, 2, 3\}$, $R_1 = \{(1, 2)\}$, $R_2 = \{(2, 3)\}$.

14. (a) Yes. Proof: Suppose R_1 and R_2 are reflexive, and suppose $a \in A$. Since R_1 and R_2 are reflexive, $(a, a) \in R_1$ and $(a, a) \in R_2$, so $(a, a) \in R_1 \cap R_2$.

    (b) Yes. Proof: Suppose R_1 and R_2 are symmetric, and suppose $(x, y) \in R_1 \cap R_2$. Then $(x, y) \in R_1$ and $(x, y) \in R_2$. Since R_1 and R_2 are symmetric, it follows that $(y, x) \in R_1$ and $(y, x) \in R_2$, so $(y, x) \in R_1 \cap R_2$.

    (c) Yes. Proof: Suppose R_1 and R_2 are transitive, and suppose $(x, y) \in R_1 \cap R_2$ and $(y, z) \in R_1 \cap R_2$. Then $(x, y) \in R_1$ and $(y, z) \in R_1$, so since R_1 is transitive, $(x, z) \in R_1$. Similarly, $(x, y) \in R_2$ and $(y, z) \in R_2$, so since R_2 is transitive, $(x, z) \in R_2$. Therefore $(x, z) \in R_1 \cap R_2$.

15. (a) No. Counterexample: $A = \{1\}$, $R_1 = R_2 = \{(1, 1)\}$.

    (b) Yes. Proof: Suppose R_1 and R_2 are symmetric, and suppose $(x, y) \in R_1 \setminus R_2$. Then $(x, y) \in R_1$ and $(x, y) \notin R_2$. Since $(x, y) \in R_1$ and R_1 is symmetric, $(y, x) \in R_1$. Now suppose $(y, x) \in R_2$. Then since R_2 is symmetric, $(x, y) \in R_2$, which is a contradiction. Therefore $(y, x) \notin R_2$. Since $(y, x) \in R_1$ and $(y, x) \notin R_2$, $(y, x) \in R_1 \setminus R_2$.

    (c) No. Counterexample: $A = \{1, 2, 3\}$, $R_1 = \{(1, 2), (2, 3), (1, 3)\}$, $R_2 = \{(1, 3)\}$.

16. Suppose $a \in A$. Since R and S are reflexive, $(a, a) \in R$ and $(a, a) \in S$, so $(a, a) \in R \circ S$.

17. First note that by part 2 of Theorem 4.3.4, since R and S are symmetric, $R = R^{-1}$ and $S = S^{-1}$. Therefore

$$\begin{aligned} R \circ S \text{ is symmetric iff } & R \circ S = (R \circ S)^{-1} && \text{(Theorem 4.3.4, part 2)} \\ \text{iff } & R \circ S = S^{-1} \circ R^{-1} && \text{(Theorem 4.2.5, part 5)} \\ \text{iff } & R \circ S = S \circ R. \end{aligned}$$

18. Suppose $S \circ R \subseteq R \circ S$. Suppose $(x, y) \in R \circ S$ and $(y, z) \in R \circ S$. Then we can choose $u, v \in A$ such that $(x, u) \in S$, $(u, y) \in R$, $(y, v) \in S$, and $(v, z) \in R$. Since $(u, y) \in R$ and $(y, v) \in S$, $(u, v) \in S \circ R$,

so since $S \circ R \subseteq R \circ S$, $(u, v) \in R \circ S$. This means that we can choose some $w \in A$ such that $(u, w) \in S$ and $(w, v) \in R$. Since $(x, u) \in S$, $(u, w) \in S$, and S is transitive, $(x, w) \in S$. And since $(w, v) \in R$, $(v, z) \in R$, and R is transitive, $(w, z) \in R$. Since $(x, w) \in S$ and $(w, z) \in R$, $(x, z) \in R \circ S$.

19. (a) The mistake is in the sentence "Then by the definition of S, xRy and yRz, where $x \in X$, $y \in Y$, and $z \in Z$." The correct sentence would be "Then by the definition of S, xRy_1 and y_2Rz for some $x \in X$, $y_1, y_2 \in Y$, and $z \in Z$."

    (b) The theorem is incorrect. Counterexample: $A = \{1, 2, 3, 4\}$, $R = \{(1, 2), (3, 4)\}$. Let $X = \{1\}$, $Y = \{2, 3\}$, and $Z = \{4\}$. Then $(X, Y) \in S$ and $(Y, Z) \in S$, but $(X, Z) \notin S$.

20. Suppose R is transitive, and suppose $(X, Y) \in S$ and $(Y, Z) \in S$. To prove that $(X, Z) \in S$ we must show that $\forall x \in X \forall z \in Z(xRz)$, so let $x \in X$ and $z \in Z$ be arbitrary. Since $Y \in B$, $Y \neq \varnothing$, so we can choose $y \in Y$. Since $(X, Y) \in S$ and $(Y, Z) \in S$, by the definition of S we have xRy and yRz. But then since R is transitive, xRz, as required. The empty set had to be excluded from B so that we could come up with $y \in Y$ in this proof.

21. (a) Yes. Proof: Suppose R is reflexive. Let $X \in \mathscr{P}(A)$ be arbitrary. Let $x \in X$ be arbitrary. Since R is reflexive, xRx, so $\exists y \in X(xRy)$. Since x was arbitrary, $\forall x \in X \exists y \in X(xRy)$, so $(X, X) \in S$.

    (b) No. Counterexample: $A = \{1, 2, 3\}$, $R = \{(1, 2), (2, 1)\}$, which is symmetric. Let $X = \{1\}$ and $Y = \{2, 3\}$. Then $(X, Y) \in S$ but $(Y, X) \notin S$, so S is not symmetric.

    (c) Yes. Proof: Suppose R is transitive, and suppose $(X, Y) \in S$ and $(Y, Z) \in S$. Let $x \in X$ be arbitrary. Then since $(X, Y) \in S$, we can choose some $y \in Y$ such that xRy. Since $(Y, Z) \in S$, we can choose some $z \in Z$ such that yRz. By transitivity of R, since xRy and yRz, xRz. Since x was arbitrary, we conclude that $\forall x \in X \exists z \in Z(xRz)\}$, so $(X, Z) \in S$.

22. The proof is incorrect. The mistake is in the sentence "Let y be any element of A such that xRy." We don't know that such a y exists. The theorem is incorrect. Counterexample: $A = \{1\}$, $R = \varnothing$.

23. Suppose aRb and bRc. To prove aRc, suppose that $X \subseteq A \setminus \{a, c\}$ and $X \cup \{a\} \in \mathcal{F}$. We must prove that $X \cup \{c\} \in \mathcal{F}$. If $c = a$ then $X \cup \{c\} = X \cup \{a\} \in \mathcal{F}$, as required. Now suppose $c \neq a$. We consider two cases.

    Case 1. $b \notin X$. Then $X \subseteq A \setminus \{a, b\}$. Since aRb and $X \cup \{a\} \in \mathcal{F}$, $X \cup \{b\} \in \mathcal{F}$. But also bRc and $X \subseteq A \setminus \{b, c\}$, so since $X \cup \{b\} \in \mathcal{F}$, $X \cup \{c\} \in \mathcal{F}$.

    Case 2. $b \in X$. Since $a \notin X$ and $c \notin X$, $b \neq a$ and $b \neq c$. Let $X_1 = X \cup \{a\} \setminus \{b\}$. Then $X_1 \subseteq A \setminus \{b, c\}$ and $X_1 \cup \{b\} = X \cup \{a\} \in \mathcal{F}$, so since bRc, $X_1 \cup \{c\} \in \mathcal{F}$. Note that $X_1 \cup \{c\} = X \cup \{a, c\} \setminus \{b\}$. Let $X_2 = X \cup \{c\} \setminus \{b\}$. Then $X_2 \subseteq A \setminus \{a, b\}$ and $X_2 \cup \{a\} = X \cup \{a, c\} \setminus \{b\} = X_1 \cup \{c\} \in \mathcal{F}$, so since aRb, $X_2 \cup \{b\} \in \mathcal{F}$. But $X_2 \cup \{b\} = X \cup \{c\}$, so $X \cup \{c\} \in \mathcal{F}$.

    Therefore $X \cup \{c\} \in \mathcal{F}$. Since X was arbitrary, this proves that aRc.

24. (a) Yes, because for every $n \in \mathbb{N}$, $|n - n| = 0 \leq 1$, so $(n, n) \in R$.

    (b) No, because, for example, $(-1, -1) \notin R$.

Section 4.4

1. (a) Partial order, but not total order since $(a, c) \notin R$ and $(c, a) \notin R$.

    (b) Not a partial order, since $(-1, 1) \in R$ and $(1, -1) \in R$, but $1 \neq -1$.

    (c) Partial order, but not total order since $(-1, 1) \notin R$ and $(1, -1) \notin R$.

2. (a) Total order. (This is the order in which words appear in a dictionary.)

    (b) Not a partial order, because $(\text{bat}, \text{bed}) \in R$ and $(\text{bed}, \text{bat}) \in R$, but of course bed $\neq$ bat.

    (c) Probably a total order. If there were two different countries C_1 and C_2 with exactly the same population, then we would have $(C_1, C_2) \in R$ and $(C_2, C_1) \in R$ but $C_1 \neq C_2$, so R would fail to be antisymmetric. But this seems unlikely.

3. (a) 2 is the smallest element of B and also a minimal element. 3 and 4 are maximal elements, but there is no largest element. 2 is the greatest lower bound. There are no upper bounds, so no least upper bound.

   (b) 1 is the smallest element of B, and also a minimal element. There are no maximal or largest elements. 1 is the greatest lower bound, and 2 is the least upper bound.

   (c) $\varnothing$ is the smallest element and also a minimal element. Every 5-element set is a maximal element, but there is no largest element. $\varnothing$ is the greatest lower bound and $\mathbb{N}$ is the least upper bound.

4. ($\rightarrow$) Suppose that R is both antisymmetric and symmetric. Suppose that $(x, y) \in R$. Then since R is symmetric, $(y, x) \in R$, and since R is antisymmetric, it follows that $x = y$. Therefore $(x, y) \in i_A$. Since (x, y) was arbitrary, this shows that $R \subseteq i_A$.

   ($\leftarrow$) Suppose that $R \subseteq i_A$. Suppose $(x, y) \in R$. Then $(x, y) \in i_A$, so $x = y$, and therefore $(y, x) = (x, y) \in R$. This shows that R is symmetric. To see that R is antisymmetric, suppose that $(x, y) \in R$ and $(y, x) \in R$ Then $(x, y) \in i_A$, so $x = y$.

5. Suppose $x \in B$. Then since $B \subseteq A$, $x \in A$. Since R is reflexive on A, $(x, x) \in R$. Also, $(x, x) \in B \times B$, so $(x, x) \in R \cap (B \times B)$. Since x was an arbitrary element of B, this shows that $R \cap (B \times B)$ is reflexive on B.

   Suppose $(x, y) \in R \cap (B \times B)$ and $(y, z) \in R \cap (B \times B)$. Then $(x, y) \in R$ and $(y, z) \in R$, so since R is transitive, $(x, z) \in R$. Also, $(x, y) \in B \times B$ and $(y, z) \in B \times B$, so $x \in B$ and $z \in B$, and therefore $(x, z) \in B \times B$. Thus $(x, z) \in R \cap (B \times B)$, so $R \cap (B \times B)$ is transitive.

   Finally, suppose $(x, y) \in R \cap (B \times B)$ and $(y, x) \in R \cap (B \times B)$. Then $(x, y) \in R$ and $(y, x) \in R$, so since R is antisymmetric, $x = y$. Therefore $R \cap (B \times B)$ is antisymmetric.

6. (a) Yes. By parts (a) and (c) of exercise 14 in Section 4.3, $R_1 \cap R_2$ is reflexive and transitive. To prove that it is antisymmetric, suppose $(x, y) \in R_1 \cap R_2$ and $(y, x) \in R_1 \cap R_2$. Then $(x, y) \in R_1$ and $(y, x) \in R_1$, so since R_1 is antisymmetric, $x = y$.

   (b) No. Counterexample: $A = \mathbb{R}$, $R_1 = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$, $R_2 = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \geq y\}$.

7. (a) Suppose $x \in A_1 \cup A_2$. Then either $x \in A_1$ or $x \in A_2$.

   Case 1. $x \in A_1$. Then since R_1 is reflexive on A_1, $(x, x) \in R_1$, so $(x, x) \in R_1 \cup R_2$.

   Case 2. $x \in A_2$. Then since R_2 is reflexive on A_2, $(x, x) \in R_2$, so $(x, x) \in R_1 \cup R_2$.

   Thus $(x, x) \in R_1 \cup R_2$, so $R_1 \cup R_2$ is reflexive on $A_1 \cup A_2$.

   Now suppose $(x, y) \in R_1 \cup R_2$ and $(y, z) \in R_1 \cup R_2$. Then either $(x, y) \in R_1$ or $(x, y) \in R_2$.

   Case 1. $(x, y) \in R_1$. Then since $R_1 \subseteq A_1 \times A_1$, $y \in A_1$. Since A_1 and A_2 are disjoint, $y \notin A_2$. Since $R_2 \subseteq A_2 \times A_2$, it follows that $(y, z) \notin R_2$, so since $(y, z) \in R_1 \cup R_2$, we must have $(y, z) \in R_1$. Since $(x, y) \in R_1$, $(y, z) \in R_1$, and R_1 is transitive, $(x, z) \in R_1$, so $(x, z) \in R_1 \cup R_2$.

   Case 2. $(x, y) \in R_2$. Then a similar argument shows that $(y, z) \in R_2$, so by transitivity of R_2, $(x, z) \in R_2$, so $(x, z) \in R_1 \cup R_2$.

   Thus $(x, z) \in R_1 \cup R_2$, so $R_1 \cup R_2$ is transitive.

   Finally, suppose $(x, y) \in R_1 \cup R_2$ and $(y, x) \in R_1 \cup R_2$. Then either $(x, y) \in R_1$ or $(x, y) \in R_2$.

   Case 1. $(x, y) \in R_1$. As in the proof of transitivity, it follows that $(y, x) \notin R_2$, so $(y, x) \in R_1$. Therefore, since R_1 is antisymmetric, $x = y$.

   Case 2. $(x, y) \in R_2$. Similar to case 1.

   Thus, $x = y$, so $R_1 \cup R_2$ is antisymmetric.

   (b) The proof that $R_1 \cup R_2 \cup (A_1 \times A_2)$ is reflexive is the same as in part (a). For transitivity, suppose $(x, y) \in R_1 \cup R_2 \cup (A_1 \times A_2)$ and $(y, z) \in R_1 \cup R_2 \cup (A_1 \times A_2)$.

   Case 1. $(x, y) \in R_1$. Then $y \in A_1$, so since A_1 and A_2 are disjoint, $y \notin A_2$, and therefore $(y, z) \notin R_2$. Thus either $(y, z) \in R_1$ or $(y, z) \in A_1 \times A_2$.

   Case 1a. $(y, z) \in R_1$. Then since R_1 is transitive, $(x, z) \in R_1$, so $(x, z) \in R_1 \cup R_2 \cup (A_1 \times A_2)$.

   Case 1b. $(y, z) \in A_1 \times A_2$. Then $z \in A_2$. Since $(x, y) \in R_1$, $x \in A_1$, so $(x, z) \in A_1 \times A_2$, and therefore $(x, z) \in R_1 \cup R_2 \cup (A_1 \times A_2)$.

Case 2. $(x, y) \in R_2$. Then $y \in A_2$, so since A_1 and A_2 are disjoint, $y \notin A_1$, and therefore $(y, z) \notin R_1$ and $(y, z) \notin A_1 \times A_2$. Thus $(y, z) \in R_2$. By transitivity of R_2, $(x, z) \in R_2$, so $(x, z) \in R_1 \cup R_2 \cup (A_1 \times A_2)$.

Case 3. $(x, y) \in A_1 \times A_2$. Then $x \in A_1$ and $y \in A_2$. As in case 2, $(y, z) \in R_2$, and therefore $z \in A_2$. Thus $(x, z) \in A_1 \times A_2$, so $(x, z) \in R_1 \cup R_2 \cup (A_1 \times A_2)$.

Thus $(x, z) \in R_1 \cup R_2 \cup (A_1 \times A_2)$, so $R_1 \cup R_2 \cup (A_1 \times A_2)$ is transitive.

Finally, suppose $(x, y) \in R_1 \cup R_2 \cup (A_1 \times A_2)$ and $(y, x) \in R_1 \cup R_2 \cup (A_1 \times A_2)$. If $(x, y) \in A_1 \times A_2$ then $x \in A_1$ and $y \in A_2$, so $(y, x) \notin R_1 \cup R_2 \cup (A_1 \times A_2)$, which is a contradiction. Therefore either $(x, y) \in R_1$ or $(x, y) \in R_2$.

Case 1. $(x, y) \in R_1$. Then $x \in A_1$, so $(y, x) \notin A_1 \times A_2$ and $(y, x) \notin R_2$. Therefore $(y, x) \in R_1$, so by antisymmetry of R_1, $x = y$.

Case 2. $(x, y) \in R_2$. Then $y \in A_2$, so $(y, x) \notin A_1 \times A_2$ and $(y, x) \notin R_1$. Therefore $(y, x) \in R_2$, so by antisymmetry of R_2, $x = y$.

Thus $x = y$, so $R_1 \cup R_2 \cup (A_1 \times A_2)$ is antisymmetric.

(c) If $a_1 \in A_1$ and $a_2 \in A_2$ then $(a_1, a_2) \notin R_1 \cup R_2$ and $(a_2, a_1) \notin R_1 \cup R_2$. Therefore as long as $A_1 \neq \varnothing$ and $A_2 \neq \varnothing$, $R_1 \cup R_2$ is not a total order. However, $R_1 \cup R_2 \cup (A_1 \times A_2)$ is a total order. To prove this, suppose $x, y \in A_1 \cup A_2$.

Case 1. $x \in A_1$ and $y \in A_1$. Then since R_1 is a total order on A_1, either $(x, y) \in R_1$ or $(y, x) \in R_1$, so either $(x, y) \in R_1 \cup R_2 \cup (A_1 \times A_2)$ or $(y, x) \in R_1 \cup R_2 \cup (A_1 \times A_2)$.

Case 2. $x \in A_2$ and $y \in A_2$. Similar to case 1, using R_2 instead of R_1.

Case 3. $x \in A_1$ and $y \in A_2$. Then $(x, y) \in A_1 \times A_2$, so $(x, y) \in R_1 \cup R_2 \cup (A_1 \times A_2)$.

Case 4. $x \in A_2$ and $y \in A_1$. Similar to case 3, using (y, x) instead of (x, y).

8. To see that T is reflexive, consider an arbitrary $(a, b) \in A \times B$. Since R and S are both reflexive, we have aRa and bSb. By the definition of T, it follows that $(a, b)T(a, b)$. To see that T is antisymmetric, suppose that $(a, b)T(a', b')$ and $(a', b')T(a, b)$. Then aRa' and $a'Ra$, so since R is antisymmetric, $a = a'$. Similarly, bSb' and $b'Sb$, so since S is antisymmetric, we also have $b = b'$. Thus $(a, b) = (a', b')$, as required. Finally, to see that T is transitive, suppose that $(a, b)T(a', b')$ and $(a', b')T(a'', b'')$. Then aRa' and $a'Ra''$, so since R is transitive, aRa''. Similarly, bSb' and $b'Sb''$, so bSb'', and therefore $(a, b)T(a'', b'')$.

Even if both R and S are total orders, T need not be a total order. For example, let $A = B = \mathbb{R}$ and $R = S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$. Then $((1, 2), (2, 1)) \notin T$ and $((2, 1), (1, 2)) \notin T$.

9. Suppose $(a, b) \in A \times B$. Since R is reflexive on A and S is reflexive on B, aRa and bSb. Therefore $((a, b), (a, b)) \in L$.

Now suppose $((a, b), (a', b')) \in L$ and $((a', b'), (a'', b'')) \in L$. Then aRa' and $a'Ra''$, so by transitivity of R, aRa''. Now suppose $a = a''$. Then since $a'Ra''$, $a'Ra$. Since aRa', $a'Ra$, and R is antisymmetric, $a' = a = a''$. So since $((a, b), (a', b')) \in L$ and $((a', b'), (a'', b'')) \in L$, bSb' and $b'Sb''$. By transitivity of S, bSb''. Thus $((a, b), (a'', b'')) \in L$, which proves that L is transitive.

Next, suppose that $((a, b), (a', b')) \in L$ and $((a', b'), (a, b)) \in L$. Then aRa' and $a'Ra$, so by the antisymmetry of R, $a = a'$. But then we also have bSb' and $b'Sb$, so by antisymmetry of S, $b = b'$, and therefore $(a, b) = (a', b')$. Thus L is antisymmetric.

If R and S are total orders, then L is also total. To see why, suppose $(a, b), (a', b') \in A \times B$.

Case 1. $a \neq a'$. Since R is a total order, either aRa' or $a'Ra$. Since $a \neq a'$, it follows that either $((a, b), (a', b')) \in L$ or $((a', b'), (a, b)) \in L$.

Case 2. $a = a'$. Since R is reflexive, aRa' and $a'Ra$. Since S is a total order, either bSb' or $b'Sb$. Therefore either $((a, b), (a', b')) \in L$ or $((a', b'), (a, b)) \in L$.

10. Let x and y be arbitrary elements of A.

($\rightarrow$) Suppose xRy. Suppose $a \in P_x$. Then aRx. Since aRx, xRy, and R is transitive, aRy, so $a \in P_y$. Since a was arbitrary, $P_x \subseteq P_y$.

($\leftarrow$) Suppose $P_x \subseteq P_y$. Since R is reflexive, xRx, so $x \in P_x$. Since $P_x \subseteq P_y$, $x \in P_y$, so xRy.

11. The minimal elements of B are the prime numbers. B has no smallest element.

12. Let $\mathcal{F} = \{X \subseteq \mathbb{R} \mid X \neq \varnothing \text{ and } \forall x \forall y((x \in X \wedge x < y) \to y \in X)\}$. Suppose X is a minimal element of $\mathcal{F}$. Then $X \neq \varnothing$, so we can choose some $x \in X$. Also, $\forall y(x < y \to y \in X)$, so $\{y \in \mathbb{R} \mid y \geq x\} \subseteq X$. Let $X' = \{y \in \mathbb{R} \mid y \geq x + 1\}$. Then $X' \in \mathcal{F}$, $X' \subseteq X$, and $X' \neq X$. This contradicts the assumption that X is minimal. Therefore $\mathcal{F}$ has no minimal element.

13. By exercise 12 of Section 4.3, R^{-1} is reflexive and transitive. Now suppose $(x, y) \in R^{-1}$ and $(y, x) \in R^{-1}$. Then $(y, x) \in R$ and $(x, y) \in R$, so since R is antisymmetric, $x = y$. Therefore R^{-1} is antisymmetric. If R is a total order, then $\forall x \in A \forall y \in A((x, y) \in R \vee (y, x) \in R)$, so $\forall x \in A \forall y \in A((y, x) \in R^{-1} \vee (x, y) \in R^{-1})$ and therefore R^{-1} is also a total order.

14. (a) b is the R-largest element of B
$$\begin{aligned} &\text{iff } b \in B \text{ and } \forall x \in B(xRb) \\ &\text{iff } b \in B \text{ and } \forall x \in B(bR^{-1}x) \\ &\text{iff } b \text{ is the } R^{-1}\text{-smallest element of } B. \end{aligned}$$

    (b) b is an R-maximal element of B
$$\begin{aligned} &\text{iff } b \in B \text{ and } \neg\exists x \in B(bRx \wedge x \neq b) \\ &\text{iff } b \in B \text{ and } \neg\exists x \in B(xR^{-1}b \wedge x \neq b) \\ &\text{iff } b \text{ is an } R^{-1}\text{-minimal element of } B. \end{aligned}$$

15. (a) Suppose b is the R_1-smallest element of B. Let $x \in B$ be arbitrary. Then $(b, x) \in R_1$, so since $R_1 \subseteq R_2$, $(b, x) \in R_2$. Since x was arbitrary, $\forall x \in B((b, x) \in R_2)$, so b is the R_2-smallest element of B.

    (b) Suppose b is an R_2-minimal element of B. Suppose $x \in B$, $(x, b) \in R_1$, and $x \neq b$. Then since $R_1 \subseteq R_2$, $(x, b) \in R_2$, which contradicts the fact that b is R_2-minimal. Therefore $\neg\exists x \in B((x, b) \in R_1 \wedge x \neq b)$, so b is an R_1-minimal element of B.

16. Suppose b is the largest element of B. Let x be an arbitrary element of B and suppose that bRx. Since b is the largest element of B, we must have xRb, and now by antisymmetry it follows that $x = b$. Thus, there can be no $x \in B$ such that bRx and $x \neq b$, so b is a maximal element.

    To see that it is the only one, suppose c is also a maximal element. Since b is the largest element of B, cRb. But then since c is maximal we must have $b = c$. Thus b is the only maximal element of B.

17. No. Let $A = \mathbb{R} \times \mathbb{R}$, and let $R = \{((x, y), (x', y')) \in A \times A \mid x \leq x' \text{ and } y \leq y'\}$. By exercise 8, R is a partial order on A. Let $B = \{(0, 0)\} \cup (\{1\} \times \mathbb{R})$. $(0, 0)$ is a minimal element of B because for every real number x, $((1, x), (0, 0)) \notin R$. But it is not smallest since, for example, $((0, 0), (1, -1)) \notin R$. For every real number x, $(1, x - 1)R(1, x)$, so $(1, x)$ is not a minimal element of B, and therefore $(0, 0)$ is the only minimal element.

18. (a) Let $x \in A$ be arbitrary.

    ($\to$) Suppose x is an upper bound for B_1. Suppose $b \in B_2$. Then since $\forall x \in B_2 \exists y \in B_1(xRy)$, we can choose some $y \in B_1$ such that bRy. Since $y \in B_1$ and x is an upper bound for B_1, yRx. Since bRy and yRx, by transitivity of R it follows that bRx. Since b was arbitrary, this shows that x is an upper bound for B_2.

    ($\leftarrow$) Similar to ($\to$).

    (b) Suppose B_1 and B_2 are disjoint. Suppose $b \in B_1$. Then since $\forall x \in B_1 \exists y \in B_2(xRy)$, we can choose some $c \in B_2$ such that bRc. And then since $\forall x \in B_2 \exists y \in B_1(xRy)$, we can choose some $d \in B_1$ such that cRd. Since bRc and cRd, by transitivity of R, bRd. If $b = d$ then bRc and cRb, so by antisymmetry of R, $b = c$. But $b \in B_1$ and $c \in B_2$, so this would contradict the fact that B_1 and B_2 are disjoint. Thus $b \neq d$. Since bRd and $b \neq d$, b is not maximal. Since b was arbitrary,

this shows that B_1 does not have a maximal element. A similar argument shows that B_2 does not have a maximal element.

19. (a) In case 1, we cannot conclude that for all $x \in B$, bRx; all we can say is that for all $x \in B$ *that fall under case 1*, bRx. Similarly, the conclusion in case 2 is also not justified. (The mistake here is essentially the same as the one in exercise 31 of Section 3.5.)

    (b) The theorem is incorrect. Counterexample: $A = \mathbb{R}$, $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$, $B = \mathbb{R}$.

20. (a) Suppose b is the smallest element of B. Then $\forall x \in B(bRx)$, so b is a lower bound for B. Now suppose c is a lower bound. Then since $b \in B$, cRb. Thus b is the greatest lower bound.

    (b) Similar to (a).

21. (a) Suppose that $x \in U$ and xRy. To prove that $y \in U$, we must show that y is an upper bound for B, so suppose that $b \in B$. Since $x \in U$, x is an upper bound for B, so bRx. But we also have xRy, so by transitivity of R we can conclude that bRy. Since b was arbitrary, this shows that y is an upper bound for B.

    (b) Suppose $b \in B$. To prove that b is a lower bound for U, let x be an arbitrary element of U. Then by definition of U, x is an upper bound for B, so bRx. Since x was arbitrary, this shows that b is a lower bound for U.

    (c) Suppose x is the greatest lower bound of U. Suppose $b \in B$. Then by part (b), b is a lower bound for U. Since x is the greatest lower bound, bRx. Since b was arbitrary, this shows that x is an upper bound for B. Now suppose c is an upper bound for B. Then $c \in U$. Since x is a lower bound for U, xRc. Since c was arbitrary, this shows that x is the least upper bound of B.

22. Suppose $B_1 \subseteq B_2$. We first show that x_2 is an upper bound for B_1. To prove this, let $b \in B_1$ be arbitrary. Since $B_1 \subseteq B_2$, $b \in B_2$, and since x_2 is an upper bound for B_2, bRx_2. Since b was arbitrary, this shows that x_2 is an upper bound for B_1. But x_1 is the least upper bound of B_1, so x_1Rx_2.

23. By exercise 8 in Section 3.3, for every $X \in \mathcal{F}$, $X \subseteq \bigcup \mathcal{F}$. This shows that $\bigcup \mathcal{F}$ is an upper bound for $\mathcal{F}$. Now suppose B is an upper bound. Then for all $X \in \mathcal{F}$, $X \subseteq B$, so $X \in \mathscr{P}(B)$. Therefore $\mathcal{F} \subseteq \mathscr{P}(B)$, so by exercise 16 in Section 3.3, $\bigcup \mathcal{F} \subseteq B$. Thus, $\bigcup \mathcal{F}$ is the least upper bound of $\mathcal{F}$.

    By exercise 9 in Section 3.3, for all $X \in \mathcal{F}$, $\bigcap \mathcal{F} \subseteq X$. This shows that $\bigcap \mathcal{F}$ is a lower bound for $\mathcal{F}$. Now suppose B is a lower bound. Then for all $X \in \mathcal{F}$, $B \subseteq X$, so by exercise 10 in Section 3.3, $B \subseteq \bigcap \mathcal{F}$. Thus, $\bigcap \mathcal{F}$ is the greatest lower bound of $\mathcal{F}$.

24. (a) Suppose $(x, y) \in S$. Then either $(x, y) \in R$ or $(x, y) \in R^{-1}$. If $(x, y) \in R$, then $(y, x) \in R^{-1}$, so $(y, x) \in S$. If $(x, y) \in R^{-1}$, then $(y, x) \in R$, so $(y, x) \in S$. Therefore S is symmetric. Since $S = R \cup R^{-1}$, it is clear that $R \subseteq S$.

    (b) Suppose T is a symmetric relation on A and $R \subseteq T$. To show that $S \subseteq T$, let (x, y) be an arbitrary element of S. Then either $(x, y) \in R$ or $(x, y) \in R^{-1}$. If $(x, y) \in R$, then since $R \subseteq T$, $(x, y) \in T$. If $(x, y) \in R^{-1}$, then $(y, x) \in R$, so since $R \subseteq T$, $(y, x) \in T$. But T is symmetric, so it follows that $(x, y) \in T$.

25. (a) $A \times A \in \mathcal{F}$, so $\mathcal{F} \neq \varnothing$.

    (b) Since $A \times A \in \mathcal{F}$, by exercise 9 in Section 3.3, $\bigcap \mathcal{F} \subseteq A \times A$. To see that $\bigcap \mathcal{F}$ is transitive, suppose $(x, y) \in \bigcap \mathcal{F}$ and $(y, z) \in \bigcap \mathcal{F}$. Let $T \in \mathcal{F}$ be arbitrary. Since $(x, y) \in \bigcap \mathcal{F}$, $(x, y) \in T$. Similarly, $(y, z) \in T$. Since $T \in \mathcal{F}$, T is transitive, so $(x, z) \in T$. Since T was arbitrary, $(x, z) \in \bigcap \mathcal{F}$. Finally, for all $T \in \mathcal{F}$, $R \subseteq T$, so by exercise 10 in Section 3.3, $R \subseteq \bigcap \mathcal{F}$.

    (c) Suppose T is a transitive relation on A that contains R as a subset. Then $T \in \mathcal{F}$, so by exercise 9 in Section 3.3, $\bigcap \mathcal{F} \subseteq T$. Thus, $\bigcap \mathcal{F}$ is the smallest transitive relation on A that contains R.

26. (a) S_2 is a symmetric relation on A and $R_2 \subseteq S_2$. Since $R_1 \subseteq R_2$, $R_1 \subseteq S_2$. Since S_1 is the *smallest* symmetric relation on A that contains R_1 as a subset, $S_1 \subseteq S_2$.

(b) T_2 is a transitive relation on A and $R_2 \subseteq T_2$. Since $R_1 \subseteq R_2$, $R_1 \subseteq T_2$. Since T_1 is the *smallest* transitive relation on A that contains R_1 as a subset, $T_1 \subseteq T_2$.

27. (a) First, note that $R_1 \subseteq R$ and $R_2 \subseteq R$. It follows, by exercise 26, that $S_1 \subseteq S$ and $S_2 \subseteq S$, so $S_1 \cup S_2 \subseteq S$. For the other direction, note that $R = R_1 \cup R_2 \subseteq S_1 \cup S_2$, and by exercise 13(b) of Section 4.3, $S_1 \cup S_2$ is symmetric. Therefore, since S is the *smallest* symmetric relation on A that contains R, $S \subseteq S_1 \cup S_2$.

(b) Imitating the first half of the proof in part (a), we can use exercise 26 to show that $T_1 \cup T_2 \subseteq T$. However, the answer to exercise 13(c) of Section 4.3 was no, so we can't imitate the second half of the proof. In fact, the example given in the solution to exercise 13(c) works as an example for which $T_1 \cup T_2 \neq T$.

28. (a) Let a and b be distinct elements of A. Suppose R is the largest antisymmetric relation on A. Let $S_1 = \{(a, b)\}$. Then S_1 is antisymmetric, so since R is the largest antisymmetric relation, $S_1 \subseteq R$ and therefore $(a, b) \in R$. Similarly, if we let $S_2 = \{(b, a)\}$ then S_2 is antisymmetric, so $S_2 \subseteq R$ and therefore $(b, a) \in R$. But now we have $(a, b) \in R$, $(b, a) \in R$, and $a \neq b$, so this contradicts the fact that R is antisymmetric. Therefore there is no largest antisymmetric relation on A.

(b) Suppose S is an antisymmetric relation on A such that $R \subseteq S$ and $R \neq S$. Then there must be some ordered pair $(a, b) \in A \times A$ such that $(a, b) \in S$ and $(a, b) \notin R$. Since R is a total order on A, either $(a, b) \in R$ or $(b, a) \in R$, so since $(a, b) \notin R$, $(b, a) \in R$. But $R \subseteq S$, so it follows that $(b, a) \in S$. Since $(a, b) \in S$, $(b, a) \in S$, and S is antisymmetric, $a = b$. But then since R is reflexive, $(a, b) \in R$, which is a contradiction. Therefore there is no antisymmetric relation S on A such that $R \subseteq S$ and $R \neq S$.

29. (a) L is irreflexive because for all $x \in \mathbb{R}$, $x \not< x$, so $(x, x) \notin L$. L is transitive because for all $x, y, z \in \mathbb{R}$, if $x < y$ and $y < z$ then $x < z$. L is a strict total order because for all $x, y \in \mathbb{R}$, either $x < y$, $y < x$, or $y = x$.

(b) Suppose R is a partial order on A. Let $x \in A$ be arbitrary. Then $(x, x) \in i_A$, so $(x, x) \notin R \setminus i_A$. Therefore $R \setminus i_A$ is irreflexive. Now suppose $(x, y) \in R \setminus i_A$ and $(y, z) \in R \setminus i_A$. Then $(x, y) \in R$ and $(y, z) \in R$, so since R is transitive, $(x, z) \in R$. Also, $(x, y) \notin i_A$ and $(y, z) \notin i_A$, so $x \neq y$ and $y \neq z$. If $x = z$ then $(x, y) \in R$ and $(y, x) = (y, z) \in R$, which contradicts the fact that R is antisymmetric. Therefore $x \neq z$, so $(x, z) \notin i_A$. Since $(x, z) \in R$ and $(x, z) \notin i_A$, $(x, z) \in R \setminus i_A$. This prove that $R \setminus i_A$ is transitive, so it is a strict partial order. Finally, suppose R is a total order. Let $x, y \in A$ be arbitrary. Then since R is a total order, either $(x, y) \in R$ or $(y, x) \in R$. If $x \neq y$ then $(x, y) \notin i_A$, so either $(x, y) \in R \setminus i_A$ or $(y, x) \in R \setminus i_A$. Thus either either $(x, y) \in R \setminus i_A$, or $(y, x) \in R \setminus i_A$, or $x = y$, so $R \setminus i_A$ is a strict total order.

(c) Suppose R is a strict partial order on A. Since $i_A \subseteq R \cup i_A$, by part 1 of Theorem 4.3.4, $R \cup i_A$ is reflexive. To prove that $R \cup i_A$ is transitive, suppose $(x, y) \in R \cup i_A$ and $(y, z) \in R \cup i_A$. Since $(x, y) \in R \cup i_A$, either $(x, y) \in R$ or $(x, y) \in i_A$.

Case 1. $(x, y) \in R$. Since $(y, z) \in R \cup i_A$, either $(y, z) \in R$ or $(y, z) \in i_A$.

Case 1a. $(y, z) \in R$. By transitivity of R, $(x, z) \in R$, so $(x, z) \in R \cup i_A$.

Case 1b. $(y, z) \in i_A$. Then $y = z$, so $(x, z) = (x, y) \in R \cup i_A$.

Case 2. $(x, y) \in i_A$. Then $x = y$, so $(x, z) = (y, z) \in R \cup i_A$.

Thus $(x, z) \in R \cup i_A$. This proves that $R \cup i_A$ is transitive.

To prove that $R \cup i_A$ is antisymmetric, suppose $(x, y) \in R \cup i_A$ and $(y, x) \in R \cup i_A$, but $x \neq y$. Then $(x, y) \notin i_A$ and $(y, x) \notin i_A$, so $(x, y) \in R$ and $(y, x) \in R$. By transitivity of R, $(x, x) \in R$. But this contradicts the fact that R is irreflexive. Therefore R is antisymmetric, so it is a partial order.

Finally, suppose that R is a strict total order on A. Let $x, y \in A$ be arbitrary. Since R is a strict total order, either $(x, y) \in R$, $(y, x) \in R$, or $x = y$. But if $x = y$ then $(x, y) \in i_A$, so either $(x, y) \in R \cup i_A$ or $(y, x) \in R \cup i_A$. Therefore R is a total order on A.

30. Since T is the transitive closure of R, $R \subseteq T$. Suppose R is symmetric. Let $(x, y) \in R$ be arbitrary. Then since R is symmetric, $(y, x) \in R$, and since $R \subseteq T$, it follows that $(y, x) \in T$. Thus $(x, y) \in T^{-1}$. Since (x, y) was arbitrary, this shows that $R \subseteq T^{-1}$. Next, suppose $(x, y) \in T^{-1}$ and $(y, z) \in T^{-1}$. Then $(z, y) \in T$ and $(y, x) \in T$, so by transitivity of T, $(z, x) \in T$, and therefore $(x, z) \in T^{-1}$. Thus T^{-1} is transitive. Since T is the smallest transitive relation on A that contains R, we conclude that $T \subseteq T^{-1}$. Finally, to prove that T is symmetric, suppose $(x, y) \in T$. Then since $T \subseteq T^{-1}$, $(x, y) \in T^{-1}$, so $(y, x) \in T$.

Section 4.5

1. Here is a list of all partitions:

$$\{\{1, 2, 3\}\}$$
$$\{\{1, 2\}, \{3\}\}$$
$$\{\{1, 3\}, \{2\}\}$$
$$\{\{2, 3\}, \{1\}\}$$
$$\{\{1\}, \{2\}, \{3\}\}$$

2. Each equivalence relation corresponds to one of the partitions listed in exercise 1:

$$\{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$$
$$\{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$$
$$\{(1, 1), (1, 3), (3, 1), (3, 3), (2, 2)\}$$
$$\{(2, 2), (2, 3), (3, 2), (3, 3), (1, 1)\}$$
$$\{(1, 1), (2, 2), (3, 3)\}$$

3. (a) R is an equivalence relation. There are 26 equivalence classes – one for each letter of the alphabet. The equivalence classes are: the set of all words that start with a, the set of all words that start with b, ..., the set of all words that start with z.
   (b) S is not an equivalence relation, because it is not transitive.
   (c) T is an equivalence relation. The equivalence classes are: the set of all one-letter words, the set of all two-letter words, and so on. For every positive integer n, if there is at least one English word of length n, then the set of all words of length n is an equivalence class.

4. (a) R is not an equivalence relation: $(2, 1) \in R$ but $(1, 2) \notin R$, so R is not symmetric.
   (b) S is an equivalence relation. For any $x \in \mathbb{R}$, $[x]_S = \{x + q \mid q \in \mathbb{Q}\}$.
   (c) T is an equivalence relation. For any $x \in \mathbb{R}$, $[x]_T$ is the set of numbers that have the same digits as x, but perhaps with the decimal point in a different location. For example,

$$[\pi]_T = \{3.14159\ldots, 31.4159\ldots, 314.159\ldots, \ldots, 0.314159\ldots, 0.0314159\ldots, \ldots\}$$

5. (a) R is an equivalence relation. The equivalence classes are families of parallel lines.
   (b) S is not an equivalence relation, because it is not reflexive and it is not transitive.
   (c) T is an equivalence relation. The set of all lines passing through the origin that are neither horizontal nor vertical is one equivalence class. Every other equivalence class contains just a single line.

6. Suppose $X \in P/B$. Then we can choose some $x \in P$ such that $X = [x]$. Let d be x's birthday. Then for every $y \in P$, $y \in [x]$ iff yBx iff $y \in P_d$, and therefore $X = [x] = P_d$. Since X was arbitrary, this shows that $P/B \subseteq \{P_d \mid d \in D\}$.

   Now suppose $d \in D$. At this point, we must make the very reasonable assumption that some person x was born on the day d. As before, it follows that $P_d = [x] \in P/B$. Since d was arbitrary, we conclude that $\{P_d \mid d \in D\} \subseteq P/B$.

7. Every triangle is similar to itself, if s is similar to t then t is similar to s, and if r is similar to s and s is similar to t then r is similar to t.

8. To see that R is symmetric, suppose $(x, y) \in R$. Since $R = \bigcup_{X \in \mathcal{F}}(X \times X)$, this means that there is some $X \in \mathcal{F}$ such that $(x, y) \in X \times X$, so $x \in X$ and $y \in X$. Therefore $(y, x) \in X \times X$, so $(y, x) \in \bigcup_{X \in \mathcal{F}}(X \times X) = R$.

   To prove that R is transitive, suppose $(x, y) \in R$ and $(y, z) \in R$. Then we can choose sets $X, Y \in \mathcal{F}$ such that $(x, y) \in X \times X$ and $(y, z) \in Y \times Y$. Therefore $x \in X$, $y \in X$, $y \in Y$, and $z \in Y$. Since $y \in X$ and $y \in Y$, $X \cap Y \neq \varnothing$. Since $\mathcal{F}$ is pairwise disjoint, it follows that $X = Y$. Thus $x \in X$ and $z \in Y = X$, so $(x, z) \in X \times X$ and therefore $(x, z) \in \bigcup_{X \in \mathcal{F}}(X \times X) = R$.

9. We first claim that $\forall x \in A([x]_R = [x]_S)$. To prove this, let $x \in A$ be arbitrary. Then $[x]_R \in A/R = A/S$, so there is some $y \in A$ such that $[x]_R = [y]_S$. By part 1 of Lemma 4.5.5, $x \in [x]_R$, so $x \in [y]_S$, and therefore by part 2 of Lemma 4.5.5, $[x]_S = [y]_S = [x]_R$. Since x was arbitrary, this proves our claim.

   Now, to prove that $R = S$, let $(x, y) \in A \times A$ be arbitrary. Then $(x, y) \in R$ iff $x \in [y]_R$ iff $x \in [y]_S$ iff $(x, y) \in S$.

10. Since S is the equivalence relation determined by $\mathcal{F}$, the proof of Theorem 4.5.6 shows that $A/S = \mathcal{F} = A/R$. The desired conclusion now follows from exercise 9.

11. (a) Let $x \in \mathbb{Z}$ be arbitrary. Since $x - x = 0 = 0 \cdot m$, $x \equiv_m x$, so $\equiv_m$ is reflexive. Now suppose $x \equiv_m y$. Then $m \mid (x - y)$, so we can choose some integer k such that $x - y = km$. Therefore $y - x = (-k)m$, so $m \mid (y - x)$ and $y \equiv_m x$. This shows that $\equiv_m$ is symmetric.

    (b) Equivalence classes for $\equiv_2$: $[0]_{\equiv_2} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$, $[1]_{\equiv_2} = \{\ldots, -3, -1, 1, 3, \ldots\}$.
    Equivalence classes for $\equiv_3$: $[0]_{\equiv_3} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$, $[1]_{\equiv_3} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$, $[2]_{\equiv_3} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$.
    There are m equivalence classes for $\equiv_m$. For more on this, see Section 7.3.

12. Let n be an arbitrary integer. Then n is either even or odd.

    Case 1. n is even. Then we can choose an integer k such that $n = 2k$. Therefore $n^2 - 0 = 4k^2$, so $4 \mid (n^2 - 0)$, which means that $n^2 \equiv 0 \pmod 4$.

    Case 2. n is odd. Then we can choose some integer k such that $n = 2k + 1$. Therefore $n^2 - 1 = (4k^2 + 4k + 1) - 1 = 4(k^2 + k)$, so $4 \mid (n^2 - 1)$, which means that $n^2 \equiv 1 \pmod 4$.

    Thus, either $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

13. See Lemma 7.3.4.

14. (a) Suppose $x \in B$. Then $x \in A$, so $(x, x) \in R$, since R is reflexive on A, and also $(x, x) \in B \times B$. Therefore $(x, x) \in R \cap (B \times B) = S$, so S is reflexive on B. Suppose $(x, y) \in S$. Then $(x, y) \in R$, so since R is symmetric, $(y, x) \in R$. Also, $(x, y) \in B \times B$, so $x \in B$ and $y \in B$, and therefore $(y, x) \in B \times B$. Thus $(y, x) \in R \cap (B \times B) = S$. Finally, suppose $(x, y) \in S$ and $(y, z) \in S$. Then $(x, y) \in R$ and $(y, z) \in R$, so by transitivity of R, $(x, z) \in R$. Also, $x \in B$ and $z \in B$, so $(x, z) \in B \times B$. Therefore $(x, z) \in S$.

    (b) Suppose $x \in B$. Then for every y,

$$y \in [x]_S \text{ iff } (y, x) \in R \cap (B \times B) \text{ iff } (y, x) \in R \wedge y \in B \text{ iff } y \in [x]_R \wedge y \in B \text{ iff } y \in [x]_R \cap B.$$

15. (a) For every $X \in \mathscr{P}(A)$, $X \triangle X = \varnothing \subseteq B$, so $(X, X) \in R$. Suppose $(X, Y) \in R$. Then $X \triangle Y \subseteq B$. But $Y \triangle X = X \triangle Y$, so $Y \triangle X \subseteq B$ and therefore $(Y, X) \in R$. Finally, suppose $(X, Y) \in R$ and $(Y, Z) \in R$. Then $X \triangle Y \subseteq B$ and $Y \triangle Z \subseteq B$. Therefore

$$(X \triangle Y) \triangle (Y \triangle Z) \subseteq (X \triangle Y) \cup (Y \triangle Z) \subseteq B.$$

    But

$$(X \triangle Y) \triangle (Y \triangle Z) = (X \triangle (Y \triangle Y)) \triangle Z = (X \triangle \varnothing) \triangle Z = X \triangle Z.$$

Therefore $X \triangle Z \subseteq B$, so $(X, Z) \in R$.

(b) Suppose $X \in \mathscr{P}(A)$. Let $Y = X \setminus B$. Then $Y \subseteq X$, so $Y \setminus X = \varnothing$, and by exercise 8(c) of Section 1.4, $X \setminus Y = X \setminus (X \setminus B) = X \cap B$. Therefore $Y \triangle X = (Y \setminus X) \cup (X \setminus Y) = \varnothing \cup (X \cap B) = X \cap B \subseteq B$, so $(Y, X) \in R$ and $Y \in [X]_R$. Also, $Y \cap B = (X \setminus B) \cap B = \varnothing$. Finally, to see that Y is unique, suppose that $Y' \in [X]_R$ and $Y' \cap B = \varnothing$. Then $(Y', X) \in R$, so since $(Y, X) \in R$, by symmetry and transitivity of R, $(Y', Y) \in R$, so $Y' \triangle Y \subseteq B$. Suppose $y \in Y$. If $y \notin Y'$ then $y \in Y \setminus Y' \subseteq Y' \triangle Y \subseteq B$. But this contradicts the fact that Y and B are disjoint. Therefore $y \in Y'$. Since y was arbitrary, this proves that $Y \subseteq Y'$. A similar argument shows that $Y' \subseteq Y$, so $Y' = Y$.

16. By exercise 16(a) of Section 3.5, $\bigcup(\mathcal{F} \cup \mathcal{G}) = (\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G}) = A \cup B$. To see that $\mathcal{F} \cup \mathcal{G}$ is pairwise disjoint, suppose that $X \in \mathcal{F} \cup \mathcal{G}$, $Y \in \mathcal{F} \cup \mathcal{G}$, and $X \cap Y \neq \varnothing$. If $X \in \mathcal{F}$ and $Y \in \mathcal{G}$ then $X \subseteq A$ and $Y \subseteq B$, and since A and B are disjoint it follows that X and Y are disjoint, which is a contradiction. Thus it cannot be the case that $X \in \mathcal{F}$ and $Y \in \mathcal{G}$, and a similar argument can be used to rule out the possibility that $X \in \mathcal{G}$ and $Y \in \mathcal{F}$. Thus, X and Y are either both elements of $\mathcal{F}$ or both elements of $\mathcal{G}$. If they are both in $\mathcal{F}$, then since $\mathcal{F}$ is pairwise disjoint, $X = Y$. A similar argument applies if they are both in $\mathcal{G}$. Finally, we have $\forall X \in \mathcal{F}(X \neq \varnothing)$ and $\forall X \in \mathcal{G}(X \neq \varnothing)$, and it follows by exercise 8 of Section 2.2 that $\forall X \in \mathcal{F} \cup \mathcal{G}(X \neq \varnothing)$.

17. (a) Suppose $x \in A \cup B$. Then either $x \in A$ or $x \in B$. If $x \in A$ then, since R is reflexive on A, $(x, x) \in R$, and if $x \in B$ then, since S is reflexive on B, $(x, x) \in S$. Therefore either $(x, x) \in R$ or $(x, x) \in S$, so $(x, x) \in R \cup S$. This proves that $R \cup S$ is reflexive on $A \cup B$. Now suppose $(x, y) \in R \cup S$. Then either $(x, y) \in R$ or $(x, y) \in S$. If $(x, y) \in R$ then, by symmetry of R. $(y, x) \in R$, and if $(x, y) \in S$ then, by symmetry of S, $(y, x) \in S$. Therefore $(y, x) \in R \cup S$, so $R \cup S$ is symmetric. Finally, suppose $(x, y) \in R \cup S$ and $(y, z) \in R \cup S$. Then either $(x, y) \in R$ or $(x, y) \in S$.

Case 1. $(x, y) \in R$. Since $R \subseteq A \times A$, $y \in A$, and since A and B are disjoint, $y \notin B$. Since $S \subseteq B \times B$, it follows that $(y, z) \notin S$, so since $(y, z) \in R \cup S$, $(y, z) \in R$. Since $(x, y) \in R$, $(y, z) \in R$, and R is transitive, $(x, z) \in R$, so $(x, z) \in R \cup S$.

Case 2. $(x, y) \in S$. A similar argument shows that $(y, z) \in S$, so by transitivity of S, $(x, z) \in S$, and therefore $(x, z) \in R \cup S$.

Thus $(x, z) \in R \cup S$, so $R \cup S$ is transitive.

(b) Suppose $x \in A$. Suppose $y \in [x]_{R \cup S}$. Then $(y, x) \in R \cup S$, so either $(y, x) \in R$ or $(y, x) \in S$. But since $x \in A$ and A and B are disjoint, $x \notin B$, so since $S \subseteq B \times B$, $(y, x) \notin S$. Therefore $(y, x) \in R$, so $y \in [x]_R$. Now suppose $y \in [x]_R$. Then $(y, x) \in R$, so $(y, x) \in R \cup S$, and therefore $y \in [x]_{R \cup S}$. Thus $[x]_{R \cup S} = [x]_R$. A similar proof shows that if $x \in B$ then $[x]_{R \cup S} = [x]_S$.

(c) Suppose $X \in (A \cup B)/(R \cup S)$. Then for some $x \in A \cup B$, $X = [x]_{R \cup S}$. Since $x \in A \cup B$, either $x \in A$ or $x \in B$. By part (b), if $x \in A$ then $[x]_{R \cup S} = [x]_R$ and if $x \in B$ then $[x]_{R \cup S} = [x]_S$. Thus either $X = [x]_R \in A/R$ or $X = [x]_S \in B/S$, so $X \in (A/R) \cup (B/S)$.

Now suppose $X \in (A/R) \cup (B/S)$. Then either $X \in A/R$ or $X \in B/S$. If $X \in A/R$ then for some $x \in A$, $X = [x]_R$, and by part (b) it follows that $X = [x]_{R \cup S} \in (A \cup B)/(R \cup S)$. Similarly if $X \in B/S$ then for some $x \in B$, $X = [x]_{R \cup S} \in (A \cup B)/(R \cup S)$. Thus $(A \cup B)/(R \cup S) = (A/R) \cup (B/S)$.

18. Clearly $\mathcal{F} \cdot \mathcal{G} \subseteq \mathscr{P}(A)$, so $\bigcup(\mathcal{F} \cdot \mathcal{G}) \subseteq A$. Now suppose $x \in A$. Since $\mathcal{F}$ and $\mathcal{G}$ are both partitions of A, there are sets $X \in \mathcal{F}$ and $Y \in \mathcal{G}$ such that $x \in X$ and $x \in Y$. Therefore $x \in X \cap Y \in \mathcal{F} \cdot \mathcal{G}$, so $x \in \bigcup(\mathcal{F} \cdot \mathcal{G})$. This proves that $\bigcup(\mathcal{F} \cdot \mathcal{G}) = A$.

To prove that $\mathcal{F} \cdot \mathcal{G}$ is pairwise disjoint, suppose that $Z_1, Z_2 \in \mathcal{F} \cdot \mathcal{G}$ and $Z_1 \cap Z_2 \neq \varnothing$. Since $Z_1 \in \mathcal{F} \cdot \mathcal{G}$, we can choose sets $X_1 \in \mathcal{F}$ and $Y_1 \in \mathcal{G}$ such that $Z_1 = X_1 \cap Y_1$. Similarly, since $Z_2 \in \mathcal{F} \cdot \mathcal{G}$ we can choose $X_2 \in \mathcal{F}$ and $Y_2 \in \mathcal{G}$ such that $Z_2 = X_2 \cap Y_2$. Since $Z_1 \cap Z_2 \neq \varnothing$, we can choose some $z \in Z_1 \cap Z_2$. Thus $z \in Z_1 = X_1 \cap Y_1$ and $z \in Z_2 = X_2 \cap Y_2$, so $z \in X_1$, $z \in Y_1$, $z \in X_2$, and $z \in Y_2$.

Since $z \in X_1$ and $z \in X_2$, X_1 and X_2 are not disjoint. Since $\mathcal{F}$ is pairwise disjoint, it follows that $X_1 = X_2$. Similarly, Y_1 and Y_2 are not disjoint, so since $\mathcal{G}$ is pairwise disjoint, $Y_1 = Y_2$. Therefore $Z_1 = X_1 \cap Y_1 = X_2 \cap Y_2 = Z_2$. This proves that $\mathcal{F} \cdot \mathcal{G}$ is pairwise disjoint.

Finally, it follows directly from the definition of $\mathcal{F} \cdot \mathcal{G}$ that $\forall Z \in \mathcal{F} \cdot \mathcal{G}(Z \neq \varnothing)$. Thus, $\mathcal{F} \cdot \mathcal{G}$ is a partition of A.

19. $\mathcal{F} \cdot \mathcal{G} = \{\mathbb{Z}^-, \mathbb{R}^- \setminus \mathbb{Z}^-, \mathbb{Z}^+, \mathbb{R}^+ \setminus \mathbb{Z}^+, \{0\}\}$.

20. (a) Suppose $x \in A$. Since R is an equivalence relation on A, R is reflexive on A, so $(x, x) \in R$. Similarly, S is reflexive, so $(x, x) \in S$. Therefore $(x, x) \in R \cap S = T$, so T is reflexive on A.

Next, suppose $(x, y) \in T = R \cap S$. Then $(x, y) \in R$ and $(x, y) \in S$, so since R and S are symmetric, $(y, x) \in R$ and $(y, x) \in S$. Therefore $(y, x) \in R \cap S = T$, so T is symmetric.

Finally, to prove that T is transitive, suppose $(x, y) \in T$ and $(y, z) \in T$. Then since $T = R \cap S$, $(x, y) \in R$ and $(y, z) \in R$, so since R is transitive, $(x, z) \in R$. Similarly, $(x, z) \in S$, so $(x, z) \in R \cap S = T$.

(b) Suppose $x \in A$. Then for all $y \in A$,

$$\begin{aligned} y \in [x]_T \text{ iff } (y, x) \in T &\text{ iff } (y, x) \in R \wedge (y, x) \in S \\ &\text{iff } y \in [x]_R \wedge y \in [x]_S \text{ iff } y \in [x]_R \cap [x]_S. \end{aligned}$$

(c) Suppose $X \in A/T$. Then since A/T is a partition, $X \neq \varnothing$. Also, for some $x \in A$, $X = [x]_T = [x]_R \cap [x]_S$, so since $[x]_R \in A/R$ and $[x]_S \in A/S$, $X \in (A/R) \cdot (A/S)$.

Now suppose $X \in (A/R) \cdot (A/S)$. Then for some y and z in A, $X = [y]_R \cap [z]_S$. Also, $X \neq \varnothing$, so we can choose some $x \in X$. Therefore $x \in [y]_R$ and $x \in [z]_S$, and by part 2 of Lemma 4.5.5 it follows that $[x]_R = [y]_R$ and $[x]_S = [z]_S$. Therefore $X = [x]_R \cap [x]_S = [x]_T \in A/T$.

21. Since $\mathcal{F} \otimes \mathcal{G} \subseteq \mathscr{P}(A \times B)$, $\bigcup(\mathcal{F} \otimes \mathcal{G}) \subseteq A \times B$. Now suppose $(a, b) \in A \times B$. Then $a \in A$, so since $\mathcal{F}$ is a partition of A, we can choose some $X \in \mathcal{F}$ such that $a \in X$. Similarly, $b \in B$, so we can choose some $Y \in \mathcal{G}$ such that $b \in Y$. Therefore $(a, b) \in X \times Y \in \mathcal{F} \otimes \mathcal{G}$, so $(a, b) \in \bigcup(\mathcal{F} \otimes \mathcal{G})$. This proves that $\bigcup(\mathcal{F} \otimes \mathcal{G}) = A \times B$.

To prove that $\mathcal{F} \otimes \mathcal{G}$ is pairwise disjoint, suppose $Z_1, Z_2 \in \mathcal{F} \otimes \mathcal{G}$ and $Z_1 \cap Z_2 \neq \varnothing$. Since $Z_1 \in \mathcal{F} \otimes \mathcal{G}$, we can choose $X_1 \in \mathcal{F}$ and $Y_1 \in \mathcal{G}$ such that $Z_1 = X_1 \times Y_1$. Similarly, since $Z_2 \in \mathcal{F} \otimes \mathcal{G}$, we can choose $X_2 \in \mathcal{F}$ and $Y_2 \in \mathcal{G}$ such that $Z_2 = X_2 \times Y_2$. Since $Z_1 \cap Z_2 \neq \varnothing$, we can choose some $(a, b) \in A \times B$ such that $(a, b) \in Z_1 \cap Z_2$. Thus $(a, b) \in Z_1 = X_1 \times Y_1$ and $(a, b) \in Z_2 = X_2 \times Y_2$, so $a \in X_1$, $b \in Y_1$, $a \in X_2$, and $b \in Y_2$. Since $a \in X_1$ and $a \in X_2$, X_1 and X_2 are not disjoint, so since $\mathcal{F}$ is pairwise disjoint, $X_1 = X_2$. Similarly, Y_1 and Y_2 are not disjoint, so since $\mathcal{G}$ is pairwise disjoint, $Y_1 = Y_2$. Therefore $Z_1 = X_1 \times Y_1 = X_2 \times Y_2 = Z_2$, so $\mathcal{F} \otimes \mathcal{G}$ is pairwise disjoint.

Finally, suppose $Z \in \mathcal{F} \otimes \mathcal{G}$. Then we can choose $X \in \mathcal{F}$ and $Y \in \mathcal{G}$ such that $Z = X \times Y$. Since $\mathcal{F}$ and $\mathcal{G}$ are partitions, X and Y are nonempty, so we can choose $a \in X$ and $b \in Y$. Therefore $(a, b) \in X \times Y = Z$, so $Z \neq \varnothing$.

22. $\mathcal{F} \otimes \mathcal{F} = \{\mathbb{R}^+ \times \mathbb{R}^+, \mathbb{R}^- \times \mathbb{R}^+, \mathbb{R}^- \times \mathbb{R}^-, \mathbb{R}^+ \times \mathbb{R}^-, \mathbb{R}^+ \times \{0\}, \mathbb{R}^- \times \{0\}, \{0\} \times \mathbb{R}^+, \{0\} \times \mathbb{R}^-, \{(0, 0)\}\}$. In geometric terms these are the four quadrants of the plane, the positive and negative x-axes, the positive and negative y-axes, and the origin.

23. (a) Suppose $(a, b) \in A \times B$. Then $a \in A$ and $b \in B$, so since R is reflexive on A and S is reflexive on B, aRa and bRb. Thus $((a, b), (a, b)) \in T$, so T is reflexive on $A \times B$.

Next, suppose that $((a, b), (a', b')) \in T$. Then aRa' and bSb'. Since R and S are symmetric, $a'Ra$ and $b'Sb$, so $((a', b'), (a, b)) \in T$. Therefore T is symmetric.

Finally, suppose $((a, b), (a', b')) \in T$ and $((a', b'), (a'', b'')) \in T$. Then aRa', bSb', $a'Ra''$, and $b'Sb''$. Since R and S are transitive, aRa'' and bSb'', so $((a, b), (a'', b'')) \in T$. Therefore T is transitive.

(b) Suppose $a \in A$ and $b \in B$. Then for all $(x, y) \in A \times B$,

$$(x, y) \in [(a, b)]_T \text{ iff } ((x, y), (a, b)) \in T \text{ iff } xRa \wedge ySb$$
$$\text{iff } x \in [a]_R \wedge y \in [b]_S \text{ iff } (x, y) \in [a]_R \times [b]_S.$$

(c) Suppose $Z \in (A \times B)/T$. Then there is some $(a, b) \in A \times B$ such that $Z = [(a, b)]_T = [a]_R \times [b]_S \in (A/R) \otimes (B/S)$. Now suppose $Z \in (A/R) \otimes (B/S)$. Then we can choose $X \in A/R$ and $Y \in B/S$ such that $Z = X \times Y$. Since $X \in A/R$ and $Y \in B/S$, we can choose $a \in A$ and $b \in B$ such that $X = [a]_R$ and $Y = [b]_S$. Therefore $Z = X \times Y = [a]_R \times [b]_S = [(a, b)]_T \in (A \times B)/T$. Thus $(A \times B)/T = (A/R) \otimes (B/S)$.

24. (a) Suppose R is compatible with S. Let $T = \{(X, Y) \in A/S \times A/S \mid \exists x \in X \exists y \in Y(xRy)\}$. Let x and y be arbitrary elements of A. Suppose $[x]_S T [y]_S$. Then by the definition of T, there are $x' \in [x]_S$ and $y' \in [y]_S$ such that $x'Ry'$. Since $x' \in [x]_S$ and $y' \in [y]_S$, $x'Sx$ and $y'Sy$, so since R is compatible with S, xRy. Now suppose xRy. Since $x \in [x]_S$ and $y \in [y]_S$, it follows that $[x]_S T [y]_S$.

To see that T is unique, suppose T' is another relation with the required properties. Let X and Y be arbitrary elements of A/S. Then we can choose $x, y \in A$ such that $X = [x]_S$ and $Y = [y]_S$. Therefore

$$(X, Y) \in T' \text{ iff } [x]_S T' [y]_S \text{ iff } xRy \text{ iff } [x]_S T [y]_S \text{ iff } (X, Y) \in T,$$

so $T' = T$.

(b) Suppose $x, y, x', y' \in A$, xSx', and ySy'. Then $[x]_S = [x']_S$ and $[y]_S = [y']_S$, so xRy iff $[x]_S T [y]_S$ iff $[x']_S T [y']_S$ iff $x'Ry'$.

25. (a) By exercises 12 and 14 in Section 4.3, S is reflexive and transitive. To see that S is symmetric, suppose $(x, y) \in S = R \cap R^{-1}$. Then $(x, y) \in R$ and $(x, y) \in R^{-1}$, so $(y, x) \in R^{-1}$ and $(y, x) \in R$, and therefore $(y, x) \in R \cap R^{-1} = S$.

(b) Let x, y, x', and y' be arbitrary elements of A, and suppose that xSx' and ySy'. Then $(x, x') \in S = R \cap R^{-1}$ and $(y, y') \in S = R \cap R^{-1}$, so xRx', $x'Rx$, yRy', and $y'Ry$. Now suppose xRy. By transitivity of R, since $x'Rx$ and xRy, $x'Ry$. But then since yRy', by another application of transitivity, $x'Ry'$. A similar argument shows that if $x'Ry'$ then xRy. Therefore R is compatible with S, so the required conclusion follows from exercise 24.

(c) Suppose $X \in A/S$. Then we can choose some $x \in A$ such that $X = [x]_S$. Since R is reflexive, xRx, so $[x]_S T [x]_S$, which means XTX. Thus T is reflexive. Next, suppose $X, Y, Z \in A/S$, XTY, and YTZ. Choose $x, y, z \in A$ such that $X = [x]_S$, $Y = [y]_S$, and $Z = [z]_S$. Then $[x]_S T [y]_S$ and $[y]_S T [z]_S$, so xRy and yRz. Since R is transitive, xRz. Therefore $[x]_S T [z]_S$, which means XTZ. This proves that T is transitive. Finally, to see that T is antisymmetric, suppose $X, Y \in A/S$, XTY, and YTX. Choose $x, y \in A$ such that $X = [x]_S$ and $Y = [y]_S$. Then $[x]_S T [y]_S$ and $[y]_S T [x]_S$, so xRy and yRx. Therefore $(x, y) \in R \cap R^{-1} = S$, so $[x]_S = [y]_S$, which means that $X = Y$.

26. (a) For every $X \in A$, X has at least as many elements as X, so R is reflexive. For all $X, Y, Z \in A$, if Y has at least as many elements as X and Z has at least as many elements as Y then Z has at least as many elements as X, so R is transitive.

(b) For all X and Y in A, $(X, Y) \in S$ iff X and Y have the same number of elements. Let $J = \{0, 1, \ldots, 100\}$, and for each $j \in J$ let $P_j = \{X \in \mathscr{P}(I) \mid X \text{ has exactly } j \text{ elements}\}$. Then $A/S = \{P_0, P_1, \ldots, P_{100}\} = \{P_j \mid j \in J\}$, so A/S has 101 elements. $T = \{(P_j, P_k) \mid j \in J, k \in J, \text{ and } j \leq k\}$. T is a total order.

27. (a) Suppose $\mathcal{F} \in P$. Then for every $X \in \mathcal{F}$, $X \subseteq X$, so $\forall X \in \mathcal{F} \exists Y \in \mathcal{F}(X \subseteq Y)$ and therefore $(\mathcal{F}, \mathcal{F}) \in R$. Thus R is reflexive. Suppose $(\mathcal{F}, \mathcal{G}) \in R$ and $(\mathcal{G}, \mathcal{H}) \in R$. Then $\mathcal{F}$ refines $\mathcal{G}$ and $\mathcal{G}$

refines $\mathcal{H}$. Let $X \in \mathcal{F}$ be arbitrary. Then since $\mathcal{F}$ refines $\mathcal{G}$, we can choose some $Y \in \mathcal{G}$ such that $X \subseteq Y$. Since $\mathcal{G}$ refines $\mathcal{H}$, we can choose some $Z \in \mathcal{H}$ such that $Y \subseteq Z$. Since $X \subseteq Y$ and $Y \subseteq Z$, $X \subseteq Z$. Therefore $\forall X \in \mathcal{F} \exists Z \in \mathcal{H}(X \subseteq Z)$, so $\mathcal{F}$ refines $\mathcal{H}$ and therefore $(\mathcal{F}, \mathcal{H}) \in R$. Thus, R is transitive. Finally, suppose $(\mathcal{F}, \mathcal{G}) \in R$ and $(\mathcal{G}, \mathcal{F}) \in R$. Then $\mathcal{F}$ refines $\mathcal{G}$ and $\mathcal{G}$ refines $\mathcal{F}$. Let $X \in \mathcal{F}$ be arbitrary. Then since $\mathcal{F}$ refines $\mathcal{G}$, there is some $Y \in \mathcal{G}$ such that $X \subseteq Y$. Since $\mathcal{G}$ refines $\mathcal{F}$, there is some $X' \in \mathcal{F}$ such that $Y \subseteq X'$. Since $X \subseteq Y$ and $Y \subseteq X'$, $X \subseteq X'$. But then $X \cap X' = X \neq \varnothing$, so since $\mathcal{F}$ is pairwise disjoint, $X' = X$. Therefore $X \subseteq Y$ and $Y \subseteq X' = X$, so $X = Y \in \mathcal{G}$. Since X was an arbitrary element of $\mathcal{F}$, this shows that $\mathcal{F} \subseteq \mathcal{G}$. A similar argument shows that $\mathcal{G} \subseteq \mathcal{F}$, so $\mathcal{F} = \mathcal{G}$, and therefore R is antisymmetric.

(b) ($\rightarrow$) Suppose $S \subseteq T$. Suppose $X \in \mathcal{F} = A/S$. Then we can choose some $x \in A$ such that $X = [x]_S$. Let $Y = [x]_T \in A/T = \mathcal{G}$. Let a be an arbitrary element of X. Then $a \in [x]_S$, so $(a, x) \in S$. Since $S \subseteq T$, $(a, x) \in T$, so $a \in [x]_T = Y$. Since a was arbitrary, $X \subseteq Y$. Since X was arbitrary, this shows that $\mathcal{F}$ refines $\mathcal{G}$.

($\leftarrow$) Suppose $\mathcal{F}$ refines $\mathcal{G}$. Suppose $(x, y) \in S$. Let $Y = [y]_S \in A/S = \mathcal{F}$. Since $\mathcal{F}$ refines $\mathcal{G}$, there is some $Z \in \mathcal{G} = A/T$ such that $Y \subseteq Z$. Since $Z \in A/T$, we can choose some $z \in A$ such that $Z = [z]_T$. By Lemma 4.5.5, $y \in [y]_S = Y \subseteq Z = [z]_T$, so $[y]_T = [z]_T$. Since $(x, y) \in S$, $x \in [y]_S \subseteq [z]_T = [y]_T$, so $(x, y) \in T$. Since (x, y) was arbitrary, $S \subseteq T$.

(c) Suppose $Z \in \mathcal{F} \cdot \mathcal{G}$. Then we can choose $X \in \mathcal{F}$ and $Y \in \mathcal{G}$ such that $Z = X \cap Y$. Therefore $Z \subseteq X$ and $Z \subseteq Y$. Since Z was arbitrary, this shows that $\mathcal{F} \cdot \mathcal{G}$ refines both $\mathcal{F}$ and $\mathcal{G}$, so $\mathcal{F} \cdot \mathcal{G}$ is a lower bound for $\{\mathcal{F}, \mathcal{G}\}$ in the partial order R. To see that it is the greatest lower bound, suppose $\mathcal{H}$ is a lower bound. Then $\mathcal{H}$ refines both $\mathcal{F}$ and $\mathcal{G}$. Let $Z \in \mathcal{H}$ be arbitrary. Since $\mathcal{H}$ refines both $\mathcal{F}$ and $\mathcal{G}$, we can choose $X \in \mathcal{F}$ and $Y \in \mathcal{G}$ such that $Z \subseteq X$ and $Z \subseteq Y$. Therefore $Z \subseteq X \cap Y$. Since $\mathcal{H}$ is a partition and $Z \in \mathcal{H}$, $Z \neq \varnothing$, so $X \cap Y \neq \varnothing$ and therefore $X \cap Y \in \mathcal{F} \cdot \mathcal{G}$. Since Z was arbitrary, this shows that $\mathcal{H}$ refines $\mathcal{F} \cdot \mathcal{G}$, so $(\mathcal{H}, \mathcal{F} \cdot \mathcal{G}) \in R$. Since $\mathcal{H}$ was arbitrary, this shows that $\mathcal{F} \cdot \mathcal{G}$ is the greatest lower bound of $\{\mathcal{F}, \mathcal{G}\}$ in the partial order R.

Chapter 5

Section 5.1

1. (a) Yes.
   (b) No, because 1 appears as the first coordinate of multiple ordered pairs in f.
   (c) Yes.
2. (a) No, because d is not paired with anything.
   (b) f is not a function, because many words are paired with multiple letters, but g is a function.
   (c) Yes.
3. (a) $f(a) = b$, $f(b) = b$, $f(c) = a$.
   (b) $f(2) = 0$.
   (c) $f(\pi) = 3$ and $f(-\pi) = -4$.
4. (a) $H(\text{Italy}) = \text{Rome}$.
   (b) $F(\{1, 3\}) = \{2\}$.
   (c) $f(2) = (3, 1)$.
5. $L \circ H : N \to N$, and for every $n \in N$, $(L \circ H)(n) = n$. Thus, $L \circ H = i_N$.
   $H \circ L : C \to C$, and for every $c \in C$, $(H \circ L)(c) =$ the capital of the country in which c is located.
6. $$(f \circ g)(x) = f(g(x)) = f(2x - 1) = \frac{1}{(2x-1)^2 + 2} = \frac{1}{4x^2 - 4x + 3},$$

$$(g \circ f)(x) = g(f(x)) = g\left(\frac{1}{x^2+2}\right) = 2 \cdot \frac{1}{x^2+2} - 1 = -\frac{x^2}{x^2+2}.$$

7. (a) Suppose that $c \in C$. We must prove that there is a unique $b \in B$ such that $(c, b) \in f \restriction C$.

   Existence: Let $b = f(c) \in B$. Then $(c, b) \in f$ and $(c, b) \in C \times B$, and therefore $(c, b) \in f \cap (C \times B) = f \restriction C$.

   Uniqueness: Suppose that $(c, b_1) \in f \restriction C$ and $(c, b_2) \in f \restriction C$. Then $(c, b_1) \in f$ and $(c, b_2) \in f$, so since f is a function, $b_1 = b_2$.

   This proves that $f \restriction C$ is a function from C to B. Finally, to derive the formula for $(f \restriction C)(c)$, suppose that $c \in C$, and let $b = f(c)$. We showed in the existence half of the proof that $(c, b) \in f \restriction C$. It follows that

   $$f(c) = b = (f \restriction C)(c).$$

   (b) ($\rightarrow$) Suppose $g = f \restriction C$. Then $g = f \cap (C \times B)$, so clearly $g \subseteq f$.

   ($\leftarrow$) Suppose $g \subseteq f$. Suppose $c \in C$, and let $b = g(c)$. Then $(c, b) \in g$, so $(c, b) \in f$, and therefore $f(c) = b$. But then by part (a), $(f \restriction C)(c) = f(c) = b = g(c)$. Since c was arbitrary, it follows by Theorem 5.1.4 that $g = f \restriction C$.

   (c) $h \restriction \mathbb{Z} = h \cap (\mathbb{Z} \times \mathbb{R}) = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = 2x + 3\} \cap (\mathbb{Z} \times \mathbb{R}) = \{(x, y) \in \mathbb{Z} \times \mathbb{R} \mid y = 2x + 3\} = g$.

8. Let $A' = \text{Dom}(g)$. Let $(a, b) \in g$ be arbitrary. Then $(a, b) \in f \subseteq A \times B$, so $b \in B$, and also $a \in \text{Dom}(g) = A'$. Therefore $(a, b) \in A' \times B$. Since (a, b) was arbitrary, $g \subseteq A' \times B$. Now let $a \in A'$ be arbitrary. Then $a \in \text{Dom}(g)$, so there is some $b \in B$ such that $(a, b) \in g$. Now suppose $(a, b_1) \in g$ and $(a, b_2) \in g$. Then $(a, b_1) \in f$ and $(a, b_2) \in f$, so since f is a function, $b_1 = b_2$. Therefore g is a function from A' to B.

9. Since $B \neq \varnothing$, we can choose some $b_0 \in B$. Let $g = f \cup ((A' \setminus A) \times \{b_0\})$. Clearly $f \subseteq g$. To prove that $g : A' \rightarrow B$, suppose $a \in A'$.

   Case 1. $a \in A$. Then $(a, f(a)) \in f \subseteq g$. Now suppose $(a, b_1) \in g$ and $(a, b_2) \in g$. Then since $a \in A$, $a \notin A' \setminus A$, so $(a, b_1) \notin (A' \setminus A) \times \{b_0\}$ and $(a, b_2) \notin (A' \setminus A) \times \{b_0\}$. Therefore $(a, b_1) \in f$ and $(a, b_2) \in f$, so since f is a function, $b_1 = b_2$.

   Case 2. $a \notin A$. Then $a \in A' \setminus A$, so $(a, b_0) \in (A' \setminus A) \times \{b_0\} \subseteq g$. Now suppose $(a, b_1) \in g$ and $(a, b_2) \in g$. Then since $a \notin A$, $(a, b_1) \notin f$ and $(a, b_2) \notin f$. Therefore $(a, b_1) \in (A' \setminus A) \times \{b_0\}$ and $(a, b_2) \in (A' \setminus A) \times \{b_0\}$, so $b_1 = b_0 = b_2$.

10. Since $f \neq g$, by Theorem 5.1.4 we can choose some $a \in A$ such that $f(a) \neq g(a)$. Therefore $(a, f(a)) \in f$ and $(a, f(a)) \notin g$, so by the definition of symmetric difference, $(a, f(a)) \in f \triangle g$, and similarly $(a, g(a)) \in f \triangle g$. Since $f(a) \neq g(a)$, it follows that $f \triangle g$ is not a function.

11. We already know that i_A is both an equivalence relation on A and also a function from A to A. Now suppose R is an equivalence relation on A and also a function from A to A. Then R is reflexive on A, so by Theorem 4.3.4, $i_A \subseteq R$. Now suppose $(x, y) \in R$. Since R is reflexive, $(x, x) \in R$. Since R is a function, it follows that $y = x$, so $(x, y) = (x, x) \in i_A$. Since (x, y) was arbitrary, this shows that $R \subseteq i_A$. Since $i_A \subseteq R$ and $R \subseteq i_A$, $R = i_A$.

12. We solve part (b) first.

    (b) ($\rightarrow$) Suppose $f \cup g : A \cup B \rightarrow C$. We already know from exercise 7 that $f \restriction (A \cap B)$ and $g \restriction (A \cap B)$ are functions from $A \cap B$ to C. Let $x \in A \cap B$ be arbitrary. Let $c_1 = (f \restriction (A \cap B))(x)$ and $c_2 = (g \restriction (A \cap B))(x)$. Then $(x, c_1) \in f \restriction (A \cap B) \subseteq f$, so $(x, c_1) \in f \cup g$, and similarly $(x, c_2) \in f \cup g$. Since $f \cup g$ is a function, $c_1 = c_2$, so $(f \restriction (A \cap B))(x) = (g \restriction (A \cap B))(x)$. Since x was arbitrary, it follows by Theorem 5.1.4 that $f \restriction (A \cap B) = g \restriction (A \cap B)$.

    ($\leftarrow$) Suppose $f \restriction (A \cap B) = g \restriction (A \cap B)$. It is clear that $f \cup g \subseteq (A \times C) \cup (B \times C) = (A \cup B) \times C$. Now suppose $x \in A \cup B$. Then either $x \in A$ or $x \in B$. If $x \in A$ then $(x, f(x)) \in f \subseteq f \cup g$, and if $x \in B$ then $(x, g(x)) \in g \subseteq f \cup g$. Thus, there exists some $c \in C$ such that $(x, c) \in f \cup g$. Now suppose $(x, c_1) \in f \cup g$ and $(x, c_2) \in f \cup g$.

Case 1. $(x, c_1) \in f$ and $(x, c_2) \in f$. Then since f is a function, $c_1 = c_2$.
Case 2. $(x, c_1) \in g$ and $(x, c_2) \in g$. Then since g is a function, $c_1 = c_2$.
Case 3. $(x, c_1) \in f$ and $(x, c_2) \in g$. Since $(x, c_1) \in f$, $x \in A$, and since $(x, c_2) \in g$, $x \in B$. Therefore $x \in A \cap B$. It follows that $c_1 = (f \upharpoonright (A \cap B))(x) = (g \upharpoonright (A \cap B))(x) = c_2$.
Case 4. $(x, c_1) \in g$ and $(x, c_2) \in f$. Similar to case 3.
Thus, $c_1 = c_2$, so $f \cup g : A \cup B \to C$.

(a) Suppose A and B are disjoint. Then $A \cap B = \varnothing$, so $f \upharpoonright (A \cap B) = \varnothing = g \upharpoonright (A \cap B)$, and therefore by part (b), $f \cup g : A \cup B \to C$.

13. (a) Suppose $b \in B$. Since $\mathrm{Dom}(S) = B$, we know that there is some $c \in C$ such that $(b, c) \in S$. To see that it is unique, suppose that $c' \in C$ and $(b, c') \in S$. Since $\mathrm{Ran}(R) = B$, we can choose some $a \in A$ such that $(a, b) \in R$. But then $(a, c) \in S \circ R$ and $(a, c') \in S \circ R$, and since $S \circ R$ is a function, it follows that $c = c'$.

(b) $A = \{1\}$, $B = \{2, 3\}$, $C = \{4\}$, $R = \{(1, 2), (1, 3)\}$, $S = \{(2, 4), (3, 4)\}$.

14. (a) Suppose S is reflexive. Suppose $x \in A$. Then since S is reflexive, $(f(x), f(x)) \in S$, so $(x, x) \in R$. Therefore R is reflexive.

(b) Suppose S is symmetric. Suppose $(x, y) \in R$. Then $(f(x), f(y)) \in S$, so since S is symmetric, $(f(y), f(x)) \in S$, and therefore $(y, x) \in R$. Thus R is symmetric.

(c) Suppose S is transitive. Suppose $(x, y) \in R$ and $(y, z) \in R$. Then $(f(x), f(y)) \in S$ and $(f(y), f(z)) \in S$, so since S is transitive, $(f(x), f(z)) \in S$. Therefore $(x, z) \in R$, so R is transitive.

15. (a) No. Example: $A = \{1\}$, $B = \{2, 3\}$, $f = \{(1, 2)\}$, $R = \{(1, 1)\}$.

(b) Yes. Proof: Suppose R is symmetric. Suppose $(x, y) \in S$. Then we can choose some u and v in A such that $f(u) = x$, $f(v) = y$, and $(u, v) \in R$. Since R is symmetric, $(v, u) \in R$, and therefore $(y, x) \in S$.

(c) No. Example: $A = \{1, 2, 3, 4\}$, $B = \{5, 6, 7\}$, $f = \{(1, 5), (2, 6), (3, 6), (4, 7)\}$, $R = \{(1, 2), (3, 4)\}$.

16. (a) Yes. Proof: Suppose R is reflexive. Let $f \in \mathcal{F}$ be arbitrary. Let $x \in A$ be arbitrary. Since R is reflexive, $(f(x), f(x)) \in R$. Since x was arbitrary, $\forall x \in A((f(x), f(x)) \in R)$, so $(f, f) \in S$. Since f was arbitrary, this shows that S is reflexive.

(b) Yes. Proof: Suppose R is symmetric. Suppose $(f, g) \in S$. Let $x \in A$ be arbitrary. Then $(f(x), g(x)) \in R$, so since R is symmetric, $(g(x), f(x)) \in R$. Since x was arbitrary, $(g, f) \in S$. Thus, S is symmetric.

(c) Yes. Proof: Suppose R is transitive. Suppose $(f, g) \in S$ and $(g, h) \in S$. Let $x \in A$ be arbitrary. Then $(f(x), g(x)) \in R$ and $(g(x), h(x)) \in R$, so since R is transitive, $(f(x), h(x)) \in R$. Since x was arbitrary, $(f, h) \in S$. Therefore S is transitive.

17. (a) Suppose $g : A \to A$. Let $x \in A$ be arbitrary. Then $(f \circ g)(x) = f(g(x)) = a = f(x)$. Since x was arbitrary, this shows that $f \circ g = f$.

(b) Since A is nonempty, we can choose some $a_0 \in A$. Let $a = f(a_0)$. Define $g : A \to A$ by the formula $g(x) = a_0$. By assumption, $f \circ g = f$, so for every $x \in A$, $f(x) = (f \circ g)(x) = f(g(x)) = f(a_0) = a$. Thus, f is a constant function.

18. (a) Clearly for all $x > 0$, $f(x) = |x| = x = g(x)$, so $(f, g) \in R$.

(b) Suppose $f \in \mathcal{F}$. Then for all $x > 0$, $f(x) = f(x)$, so $(f, f) \in R$. Therefore R is reflexive. Next, suppose $(f, g) \in R$. Then we can choose some $a \in \mathbb{R}$ such that $\forall x > a(f(x) = g(x))$. Then $\forall x > a(g(x) = f(x))$, so $(g, f) \in R$. Thus R is symmetric. Finally, suppose $(f, g) \in R$ and $(g, h) \in R$. Then we can choose $a_1 \in \mathbb{R}$ and $a_2 \in \mathbb{R}$ such that $\forall x > a_1(f(x) = g(x))$ and $\forall x > a_2(g(x) = h(x))$. Let a be the larger of a_1 and a_2. Then for every $x > a$, $x > a_1$ and $x > a_2$, so $f(x) = g(x)$ and $g(x) = h(x)$, and therefore $f(x) = h(x)$. Thus $(f, h) \in R$, so R is transitive.

19. (a) Let $a = 3$ and $c = 8$. Then for any $x > a = 3$,

$$|f(x)| = |7x + 3| = 7x + 3 < 7x + x = 8x < 8x^2 = c|g(x)|.$$

This shows that $f \in O(g)$.

Now suppose that $g \in O(f)$. Then we can choose $a \in \mathbb{Z}^+$ and $c \in \mathbb{R}^+$ such that $\forall x > a(|g(x)| \leq c|f(x)|)$, or in other words, $\forall x > a(x^2 \leq c(7x+3))$. Let x be any positive integer larger than both a and $10c$. Multiplying both sides of the inequality $x > 10c$ by x, we can conclude that $x^2 > 10cx$. But since $x > a$, we also have $x^2 \leq c(7x+3) \leq c(7x+3x) = 10cx$, so we have reached a contradiction. Therefore $g \notin O(f)$.

(b) Clearly for any function $f \in \mathcal{F}$ we have $\forall x \in \mathbb{Z}^+(|f(x)| \leq 1 \cdot |f(x)|)$, so $f \in O(f)$, and therefore $(f, f) \in S$. Thus, S is reflexive. To see that it is also transitive, suppose $(f, g) \in S$ and $(g, h) \in S$. Then there are positive integers a_1 and a_2 and positive real numbers c_1 and c_2 such that $\forall x > a_1(|f(x)| \leq c_1|g(x)|)$ and $\forall x > a_2(|g(x)| \leq c_2|h(x)|)$. Let a be the maximum of a_1 and a_2, and let $c = c_1c_2$. Then for all $x > a$,

$$|f(x)| \leq c_1|g(x)| \leq c_1c_2|h(x)| = c|h(x)|.$$

Thus, $(f, h) \in S$, so S is transitive. Finally, to see that S is not a partial order, we show that it is not antisymmetric. Let f and g be the functions from $\mathbb{Z}^+$ to $\mathbb{R}$ defined by the formulas $f(x) = x$ and $g(x) = 2x$. Then for all $x \in \mathbb{Z}^+, |f(x)| \leq |g(x)|$ and $|g(x)| \leq 2|f(x)|$, so $f \in O(g)$ and also $g \in O(f)$. Therefore $(f, g) \in S$ and $(g, f) \in S$, but $f \neq g$.

(c) Since $f_1 \in O(g)$, we can choose $a_1 \in \mathbb{Z}^+$ and $c_1 \in \mathbb{R}^+$ such that $\forall x > a_1(|f_1(x)| \leq c_1|g(x)|)$. Similarly, since $f_2 \in O(g)$ we can choose $a_2 \in \mathbb{Z}^+$ and $c_2 \in \mathbb{R}^+$ such that $\forall x > a_2(|f_2(x)| \leq c_2|g(x)|)$. Let a be the maximum of a_1 and a_2, and let $c = |s|c_1 + |t|c_2 + 1$. (We have added 1 here just to make sure that c is positive, as required in the definition of O.) Then for all $x > a$,

$$\begin{aligned} |f(x)| &= |sf_1(x) + tf_2(x)| \leq |s||f_1(x)| + |t||f_2(x)| \\ &\leq |s|c_1|g(x)| + |t|c_2|g(x)| = (|s|c_1 + |t|c_2)|g(x)| \leq c|g(x)|. \end{aligned}$$

Therefore $f \in O(g)$.

20. (a) Suppose $x \in A$. Since $g(x) = g(x)$, $(x, x) \in R$, so R is reflexive. Suppose $(x, y) \in R$. Then $g(x) = g(y)$. Therefore $g(y) = g(x)$, so $(y, x) \in R$. This proves that R is symmetric. Finally, suppose $(x, y) \in R$ and $(y, z) \in R$. Then $g(x) = g(y)$ and $g(y) = g(z)$, and therefore $g(x) = g(z)$. Thus $(x, z) \in R$, so R is transitive.

(b) Let $(x, y) \in A \times A$ be arbitrary. Then by part 2 of Lemma 4.5.5, $(x, y) \in R$ iff $x \in [y]_R$ iff $[x]_R = [y]_R$ iff $g(x) = g(y)$.

21. (a) Let $h = \{(X, y) \in A/R \times B \mid \exists x \in X(f(x) = y)\}$. We first show that $h : A/R \to B$. Suppose $X \in A/R$. Then we can choose some $x \in A$ such that $X = [x]_R$. Let $y = f(x)$. Since $x \in [x]_R = X$ and $f(x) = y$, we have $(X, y) \in h$. To see that y is unique, suppose $(X, y') \in h$. Then we can choose some $x' \in X$ such that $f(x') = y'$. Since $x' \in X = [x]_R$, $x'Rx$, so since f is compatible with R, $y' = f(x') = f(x) = y$.

To see that h is unique, suppose that $h' : A/R \to B$ and for all $x \in A$, $h'([x]_R) = f(x)$. Let $X \in A/R$ be arbitrary. Then we can choose some $x \in A$ such that $X = [x]_R$. Therefore $h'(X) = h'([x]_R) = f(x) = h([x]_R) = h(X)$. Since X was arbitrary, $h' = h$.

(b) Suppose $x, x' \in R$ and xRx'. Then $x \in [x']_R$, so by Lemma 4.5.5, $[x]_R = [x']_R$. Therefore $f(x) = h([x]_R) = h([x']_R) = f(x')$. Since x and x' were arbitrary, this shows that f is compatible with R.

22. (a) Define $f : \mathbb{N} \to \mathbb{N}/R$ by the formula $f(x) = [x^2]_R$. We first show that f is compatible with R (see exercise 21 for the definition). Suppose $x, y \in \mathbb{N}$ and xRy. Then $x \equiv y \pmod 5$, so $5 \mid (x-y)$ and we can choose an integer k such that $x - y = 5k$. Therefore $x^2 - y^2 = (x-y)(x+y) = 5k(x+y)$, so $5 \mid (x^2 - y^2)$, which means that $x^2 \equiv y^2 \pmod 5$. Thus $f(x) = [x^2]_R = [y^2]_R = f(y)$, and since x and y were arbitrary, this shows that f is compatible with R. Finally, the existence and uniqueness of the function h follow from exercise 21(a).

    (b) Suppose there is such a function. Define $f : \mathbb{N} \to \mathbb{N}/R$ by the formula $f(x) = [2^x]_R$. By exercise 21(b), f must be compatible with R. But $(0, 5) \in R$, since $0 \equiv 5 \pmod 5$, and $2^0 - 2^5 = -31$, which is not divisible by 5, so $2^0 \not\equiv 2^5 \pmod 5$, and therefore $f(0) = [2^0]_R \neq [2^5]_R = f(5)$. This contradicts the compatibility of f with R.

Section 5.2

1. (a) f is not one-to-one, but it is onto.
   (b) f is not a function.
   (c) f is one-to-one, but it is not onto.
2. (a) f is not a function from A to B.
   (b) f is not a function. g is a function that is onto, but not one-to-one.
   (c) R is one-to-one and onto.
3. (a) f is not one-to-one, but it is onto.
   (b) f is neither one-to-one nor onto.
   (c) f is not one-to-one, but it is onto.
4. (a) H is one-to-one, but it is not onto.
   (b) F is one-to-one and onto.
   (c) f is one-to-one, but it is not onto.
5. (a) Suppose that $x_1 \in A$, $x_2 \in A$, and $f(x_1) = f(x_2)$. Then we can perform the following algebraic steps:

$$\begin{aligned} \frac{x_1 + 1}{x_1 - 1} &= \frac{x_2 + 1}{x_2 - 1}, \\ (x_1 + 1)(x_2 - 1) &= (x_2 + 1)(x_1 - 1), \\ x_1x_2 - x_1 + x_2 - 1 &= x_1x_2 - x_2 + x_1 - 1, \\ 2x_2 &= 2x_1, \\ x_2 &= x_1. \end{aligned}$$

   This shows that f is one-to-one.

   To show that f is onto, suppose that $y \in A$. Let

$$x = \frac{y+1}{y-1}.$$

   Notice that this is defined, since $y \neq 1$, and also clearly $x \neq 1$, so $x \in A$. Then

$$f(x) = \frac{x+1}{x-1} = \frac{\frac{y+1}{y-1} + 1}{\frac{y+1}{y-1} - 1} = \frac{\frac{2y}{y-1}}{\frac{2}{y-1}} = y.$$

   (b) For any $x \in A$,

$$(f \circ f)(x) = \frac{\frac{x+1}{x-1} + 1}{\frac{x+1}{x-1} - 1} = \frac{\frac{2x}{x-1}}{\frac{2}{x-1}} = x = i_A(x).$$

6. Suppose $x_1, x_2 \in \mathbb{R}$ and $f(x_1) = f(x_2)$. This means $ax_1 + b = ax_2 + b$, so $ax_1 = ax_2$. Since $a \neq 0$, we can divide by a to conclude that $x_1 = x_2$. This proves that f is one-to-one. To prove that it is onto, suppose $y \in \mathbb{R}$. Let $x = (y-b)/a$. Then $f(x) = a((y-b)/a) + b = y - b + b = y$. Since y was arbitrary, this shows that f is onto.

7. (a) Following the hint, we first prove that if $0 < a < b$ then $f(a) > f(b)$. Suppose $0 < a < b$. Then by exercise 6 in Section 3.1, $1/a > 1/b$, and also $-a > -b$. Adding these inequalities, we conclude that $f(a) = 1/a - a > 1/b - b = f(b)$.

   Now suppose f is not one-to-one. Then there are positive real numbers x_1 and x_2 such that $x_1 \neq x_2$ and $f(x_1) = f(x_2)$. Since $x_1 \neq x_2$, either $x_1 < x_2$ or $x_2 < x_1$. But then by the previous paragraph, either $f(x_1) > f(x_2)$ or $f(x_1) < f(x_2)$, which is a contradiction.

   (b) Suppose $y \in \mathbb{R}$. Let $x = (\sqrt{y^2+4} - y)/2$. Note that $\sqrt{y^2+4} > \sqrt{y^2} = |y| \geq y$, so $x \in \mathbb{R}^+$. Also,

$$f(x) = \frac{2}{\sqrt{y^2+4} - y} - \frac{\sqrt{y^2+4} - y}{2} = \frac{\sqrt{y^2+4} + y}{2} - \frac{\sqrt{y^2+4} - y}{2} = \frac{2y}{2} = y.$$

   (c) $g(2) = 5/2 = g(1/2)$, so g is not one-to-one. For every $x \in \mathbb{R}^+$, $g(x) = 1/x + x > 0$, so $-1 \notin \text{Ran}(g)$. Therefore g is not onto.

8. (a) $f(2) = \{y \in \mathbb{R} \mid y^2 < 2\} = \{y \in \mathbb{R} \mid -\sqrt{2} < y < \sqrt{2}\}$.

   (b) $f(0) = f(-1) = \varnothing$, so f is not one-to-one. And $\{y \in \mathbb{R} \mid -1 < y < 2\}$ is not in $\text{Ran}(f)$, so f is not onto.

9. (a) $f(\{\{1,2\},\{3,4\}\}) = \bigcup\{\{1,2\},\{3,4\}\} = \{1,2\} \cup \{3,4\} = \{1,2,3,4\}$.

   (b) $f(\{\{1\},\{2,3,4\}\}) = \{1\} \cup \{2,3,4\} = \{1,2,3,4\} = f(\{\{1,2\},\{3,4\}\})$, so f is not one-to-one. For every set $X \in \mathscr{P}(\mathbb{R})$, $f(\{X\}) = \bigcup\{X\} = X$, so f is onto.

10. (a) Suppose $g \circ f$ is onto. Let $c \in C$ be arbitrary. Since $g \circ f$ is onto, we can choose some $a \in A$ such that $(g \circ f)(a) = c$. Let $b = f(a) \in B$. Then $g(b) = g(f(a)) = (g \circ f)(a) = c$. Therefore g is onto.

    (b) Suppose $g \circ f$ is one-to-one. Suppose $a_1, a_2 \in A$ and $f(a_1) = f(a_2)$. Then $(g \circ f)(a_1) = g(f(a_1)) = g(f(a_2)) = (g \circ f)(a_2)$, so since $g \circ f$ is one-to-one, $a_1 = a_2$. Therefore f is one-to-one.

11. (a) Suppose f is onto and g is not one-to-one. Since g is not one-to-one, we can choose $b_1, b_2 \in B$ such that $b_1 \neq b_2$ and $g(b_1) = g(b_2)$. Since f is onto, we can choose $a_1, a_2 \in A$ such that $f(a_1) = b_1$ and $f(a_2) = b_2$. If $a_1 = a_2$ then $b_1 = f(a_1) = f(a_2) = b_2$, which is a contradiction, so $a_1 \neq a_2$. But $(g \circ f)(a_1) = g(f(a_1)) = g(b_1) = g(b_2) = g(f(a_2)) = (g \circ f)(a_2)$. Therefore $g \circ f$ is not one-to-one.

    (b) Suppose f is not onto and g is one-to-one. Since f is not onto, we can choose some $b \in B$ such that $b \notin \text{Ran}(f)$. Let $c = g(b) \in C$. Suppose $g \circ f$ is onto. Then we can choose some $a \in A$ such that $g(f(a)) = (g \circ f)(a) = c = g(b)$. Since g is one-to-one, it follows that $f(a) = b$, which contradicts the fact that $b \notin \text{Ran}(f)$. Therefore $g \circ f$ is not onto.

12. Suppose f is onto. Suppose $b_1, b_2 \in B$ and $g(b_1) = g(b_2)$. Since f is onto, we can choose some $a \in A$ such that $f(a) = b_1$. Then $a \in g(b_1) = g(b_2)$, so $f(a) = b_2$. Therefore $b_1 = b_2$, so g is one-to-one.

    If f is not onto, then g may fail to be one-to-one. Example: $A = \{1\}$, $B = \{2,3,4\}$, $f = \{(1,2)\}$. Then $g(3) = g(4) = \varnothing$.

13. (a) Suppose that f is one-to-one. Suppose that $c_1 \in C$, $c_2 \in C$, and $(f \restriction C)(c_1) = (f \restriction C)(c_2)$. By exercise 7(a) of Section 5.1, it follows that $f(c_1) = f(c_2)$, so since f is one-to-one, $c_1 = c_2$.

    (b) Suppose that $f \restriction C$ is onto. Suppose $b \in B$. Then since $f \restriction C$ is onto, we can choose some $c \in C$ such that $(f \restriction C)(c) = b$. But then $c \in A$, and by exercise 7(a) of Section 5.1, $f(c) = b$.

    (c) Let $A = B = \mathbb{R}$ and $C = \mathbb{R}^+$. For (a), use $f(x) = |x|$, and for (b), use $f(x) = x$.

14. (a) Suppose A has more than one element. Let a_1 and a_2 be two distinct elements of A. Then $f(a_1) = b = f(a_2)$, so f is not one-to-one.

(b) Suppose B has more than one element. Then we can choose $b' \in B$ such that $b' \neq b$. Then for all $a \in A$, $f(a) = b \neq b'$, so f is not onto.

15. ($\rightarrow$) Suppose $f \cup g$ is one-to-one. Suppose $\text{Ran}(f) \cap \text{Ran}(g) \neq \varnothing$. Then we can choose some $c \in \text{Ran}(f) \cap \text{Ran}(g)$. Since $c \in \text{Ran}(f)$, we can choose some $a \in A$ such that $f(a) = c$. Similarly, since $c \in \text{Ran}(g)$, we can choose some $b \in B$ such that $g(b) = c$. Therefore $(a, c) \in f \cup g$ and $(b, c) \in f \cup g$, so $(f \cup g)(a) = c = (f \cup g)(b)$. But since A and B are disjoint, $a \neq b$. This contradicts the fact that $f \cup g$ is one-to-one. Therefore $\text{Ran}(f)$ and $\text{Ran}(g)$ are disjoint.

($\leftarrow$) Suppose $\text{Ran}(f)$ and $\text{Ran}(g)$ are disjoint. Suppose $x_1, x_2 \in A \cup B$ and $(f \cup g)(x_1) = (f \cup g)(x_2)$. Let $c = (f \cup g)(x_1) = (f \cup g)(x_2) \in C$.

Case 1. $x_1 \in A$. Then $(x_1, f(x_1)) \in f \subseteq f \cup g$, so $f(x_1) = (f \cup g)(x_1) = c$. Suppose $x_2 \in B$. Then $(x_2, g(x_2)) \in g \subseteq f \cup g$, so $g(x_2) = (f \cup g)(x_2) = c$. But then $c \in \text{Ran}(f) \cap \text{Ran}(g)$, which contradicts the fact that $\text{Ran}(f)$ and $\text{Ran}(g)$ are disjoint. Therefore $x_2 \notin B$, so $x_2 \in A$. Thus $(x_2, f(x_2)) \in f \subseteq f \cup g$, so $f(x_2) = (f \cup g)(x_2) = c = f(x_1)$. Since f is one-to-one, $x_1 = x_2$.

Case 2. $x_1 \in B$. Then a similar argument shows that $x_2 \in B$ and $g(x_1) = c = g(x_2)$, so since g is one-to-one, $x_1 = x_2$.

Thus $x_1 = x_2$. Since x_1 and x_2 were arbitrary, $f \cup g$ is one-to-one.

16. Suppose S is one-to-one. Suppose $a \in A$. Let $c = (S \circ R)(a) \in C$. Then $(a, c) \in S \circ R$, so we can choose some $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S$. Now suppose $b' \in B$ and $(a, b') \in R$. Since $S : B \rightarrow C$, we can let $c' = S(b')$. Then $(a, b') \in R$ and $(b', c') \in S$, and therefore $(a, c') \in S \circ R$. Since $(a, c) \in S \circ R$, $(a, c') \in S \circ R$, and $S \circ R$ is a function, $c = c'$. Therefore $S(b') = c' = c = S(b)$, so since S is one-to-one, $b' = b$. Thus b is the only element of B such that $(a, b) \in R$. Since a was arbitrary, we conclude that $R : A \rightarrow B$.

17. (a) Suppose R is reflexive and f is onto. Let $x \in B$ be arbitrary. Since f is onto, we can choose some $u \in A$ such that $f(u) = x$. Since R is reflexive, $(u, u) \in R$. Therefore $(x, x) \in S$.

(b) Suppose R is transitive and f is one-to-one. Suppose that $(x, y) \in S$ and $(y, z) \in S$. Since $(x, y) \in S$, we can choose some u and v in A such that $f(u) = x$, $f(v) = y$, and $(u, v) \in R$. Similarly, since $(y, z) \in S$ we can choose p and q in A such that $f(p) = y$, $f(q) = z$, and $(p, q) \in R$. Since $f(v) = y = f(p)$ and f is one-to-one, $v = p$. Therefore $(v, q) = (p, q) \in R$. Since we also have $(u, v) \in R$, by transitivity of R it follows that $(u, q) \in R$, so $(x, z) \in S$.

18. (a) Suppose $X \in A/R$. Then we can choose some $x \in A$ such that $X = [x]_R$. Therefore $g(x) = [x]_R = X$, so g is onto.

(b) ($\rightarrow$) Suppose g is one-to-one. Since R is reflexive, by Theorem 4.3.4, $i_A \subseteq R$. Now suppose $(x, y) \in R$. Then $g(x) = [x]_R = [y]_R = g(y)$, so since g is one-to-one, $x = y$, and therefore $(x, y) \in i_A$. Thus $R \subseteq i_A$. Since $i_A \subseteq R$ and $R \subseteq i_A$, $R = i_A$.

($\leftarrow$) Suppose $R = i_A$. Suppose $a_1, a_2 \in A$ and $g(a_1) = g(a_2)$. Then $[a_1]_R = [a_2]_R$. Since $a_1 \in [a_1]_R$, it follows that $a_1 \in [a_2]_R$, so $(a_1, a_2) \in R = i_A$, and therefore $a_1 = a_2$. Since a_1 and a_2 were arbitrary, g is one-to-one.

19. ($\rightarrow$) Suppose h is one-to-one. Suppose $x, y \in A$ and $f(x) = f(y)$. Then $h([x]_R) = f(x) = f(y) = h([y]_R)$, so since h is one-to-one, $[x]_R = [y]_R$. Since $x \in [x]_R$, $x \in [y]_R$, so xRy. Since x and y were arbitrary, this shows that $\forall x \in A \forall y \in A(f(x) = f(y) \rightarrow xRy)$.

($\leftarrow$) Suppose $\forall x \in A \forall y \in A(f(x) = f(y) \rightarrow xRy)$. Suppose $X, Y \in A/R$ and $h(X) = h(Y)$. By definition of A/R, we can choose $x, y \in A$ such that $X = [x]_R$ and $Y = [y]_R$. Then $f(x) = h([x]_R) = h(X) = h(Y) = h([y]_R) = f(y)$, so by our assumption xRy. Therefore $x \in [y]_R$, so by Lemma 4.5.5, $X = [x]_R = [y]_R = Y$. Since X and Y were arbitrary, this shows that h is one-to-one.

20. (a) Suppose that f is onto, $g : B \rightarrow C$, $h : B \rightarrow C$, and $g \circ f = h \circ f$. Let $b \in B$ be arbitrary. Since f is onto, we can choose some $a \in A$ such that $f(a) = b$. Therefore $g(b) = g(f(a)) = (g \circ f)(a) = (h \circ f)(a) = h(f(a)) = h(b)$. Since b was arbitrary, this shows that $\forall b \in B(g(b) = h(b))$, so $g = h$.

(b) Suppose that C has at least two elements, and for all functions g and h from B to C, if $g \circ f = h \circ f$ then $g = h$. Let c_1 and c_2 be two distinct elements of C. Suppose $b \in B$. Let g and h be functions from B to C such that $\forall x \in B(g(x) = c_1)$, $\forall x \in B \setminus \{b\}(h(x) = c_1)$, and $h(b) = c_2$. (Formally, $g = B \times \{c_1\}$ and $h = [(B \setminus \{b\}) \times \{c_1\}] \cup \{(b, c_2)\}$.) Then $g \neq h$, so by assumption $g \circ f \neq h \circ f$, and therefore we can choose some $a \in A$ such that $g(f(a)) \neq h(f(a))$. But by the way g and h were defined, the only $x \in B$ for which $g(x) \neq h(x)$ is $x = b$, so it follows that $f(a) = b$. Since b was arbitrary, this shows that f is onto.

21. (a) Suppose that f is one-to-one, $g : A \to B$, $h : A \to B$, and $f \circ g = f \circ h$. Let $a \in A$ be arbitrary. Then $f(g(a)) = (f \circ g)(a) = (f \circ h)(a) = f(h(a))$, and since f is one-to-one it follows that $g(a) = h(a)$. Since a was arbitrary, we conclude that $g = h$.

(b) Suppose that $A \neq \varnothing$, and for all functions g and h from A to B, if $f \circ g = f \circ h$ then $g = h$. Suppose $b_1, b_2 \in B$ and $f(b_1) = f(b_2)$. Let g and h be functions from A to B such that $\forall a \in A(g(a) = b_1)$ and $\forall a \in A(h(a) = b_2)$. (Formally, $g = A \times \{b_1\}$ and $h = A \times \{b_2\}$.) Then for all $a \in A$, $(f \circ g)(a) = f(g(a)) = f(b_1) = f(b_2) = f(h(a)) = (f \circ h)(a)$, so $f \circ g = f \circ h$, and therefore by assumption $g = h$. Since $A \neq \varnothing$, we can choose some $a_0 \in A$. Then $b_1 = g(a_0) = h(a_0) = b_2$. Since b_1 and b_2 were arbitrary, f is one-to-one.

22. (a) Let $j : \mathbb{R} \to \mathbb{R}$ be defined by the formula $j(x) = (x-1)^2 + 1$. Then for all $x \in \mathbb{R}$, $(j \circ f)(x) = j(f(x)) = j(x^2+1) = (x^2+1-1)^2 + 1 = x^4 + 1 = h(x)$. Therefore $h = j \circ f$, so hRf.

Now suppose gRf. Then we can choose some function $k : \mathbb{R} \to \mathbb{R}$ such that $g = k \circ f$. But then $2 = g(1) = (k \circ f)(1) = k(f(1)) = k(2) = k(f(-1)) = (k \circ f)(-1) = g(-1) = 0$, which is a contradiction. Therefore it is not the case that gRf.

(b) For every function $f \in \mathcal{F}$, $f = i_{\mathbb{R}} \circ f$, so fRf. Therefore R is reflexive. Now suppose $f, g, h \in \mathcal{F}$, fRg, and gRh. Then we can choose functions j and k from $\mathbb{R}$ to $\mathbb{R}$ such that $f = j \circ g$ and $g = k \circ h$. Therefore $f = j \circ (k \circ h) = (j \circ k) \circ h$, so fRh. Thus f is transitive.

(c) For every $f \in \mathcal{F}$, $f = f \circ i_{\mathbb{R}}$, so $fRi_{\mathbb{R}}$.

(d) Let $f \in \mathcal{F}$ be arbitrary.

($\rightarrow$) Suppose $i_{\mathbb{R}}Rf$. Then there is some function $g : \mathbb{R} \to \mathbb{R}$ such that $g \circ f = i_{\mathbb{R}}$. See part 1 of Theorem 5.3.3 for a proof that f is one-to-one.

($\leftarrow$) Suppose f is one-to-one. Let $A = \text{Ran}(f)$ and let $h = f^{-1} \cup ((\mathbb{R} \setminus A) \times \{0\})$. To see that $h : \mathbb{R} \to \mathbb{R}$, suppose $x \in \mathbb{R}$.

Case 1. $x \in A$. Then $x \in \text{Ran}(f)$, so we can choose some $y \in \mathbb{R}$ such that $(y, x) \in f$, and therefore $(x, y) \in f^{-1} \subseteq h$. Now suppose that for some $y' \in \mathbb{R}$, $(x, y') \in h$. Clearly $(x, y') \notin (\mathbb{R} \setminus A) \times \{0\}$, since $x \in A$, so $(x, y') \in f^{-1}$. Therefore $(y', x) \in f$, so $f(y') = x = f(y)$. Since f is one-to-one, $y' = y$.

Case 2. $x \notin A$. Then $(x, 0) \in (\mathbb{R} \setminus A) \times \{0\} \subseteq h$. Also, if $(x, y) \in h$ then $(x, y) \notin f^{-1}$, since $x \notin A = \text{Ran}(f)$, so $(x, y) \in (\mathbb{R} \setminus A) \times \{0\}$, and therefore $y = 0$.

Thus $\forall x \in \mathbb{R} \exists! y \in \mathbb{R}((x, y) \in h)$, so $h : \mathbb{R} \to \mathbb{R}$. Finally, for any $x \in \mathbb{R}$ we have $(f(x), x) \in f^{-1} \subseteq h$, so $(h \circ f)(x) = h(f(x)) = x = i_{\mathbb{R}}(x)$. Therefore $i_{\mathbb{R}} = h \circ f$, so $i_{\mathbb{R}}Rf$.

(e) By part 1 of exercise 17 in Section 5.1, for all $f \in \mathbb{R}$, $g = g \circ f$, so gRf.

(f) ($\rightarrow$) Suppose fRg. Then we can choose some function $h : \mathbb{R} \to \mathbb{R}$ such that $f = h \circ g$. Since g is a constant function, we can choose some $a \in \mathbb{R}$ such that $\forall x \in \mathbb{R}(g(x) = a)$. Therefore for every $x \in \mathbb{R}$, $f(x) = (h \circ g)(x) = h(g(x)) = h(a)$, so f is a constant function (with constant value $h(a)$).

($\leftarrow$) Suppose f is a constant function. Then by part (e), fRg.

(g) We first show that $[i_{\mathbb{R}}]_S = \{f \in \mathcal{F} \mid f \text{ is one-to-one}\}$. Suppose $f \in [i_{\mathbb{R}}]_S$. Then $(f, i_{\mathbb{R}}) \in S = R \cap R^{-1}$, so $i_{\mathbb{R}}Rf$, and therefore, by part (d), f is one-to-one. Now suppose $f \in \mathcal{F}$ and f is one-to-one. Then by part (d), $i_{\mathbb{R}}Rf$, and by part (c), $fRi_{\mathbb{R}}$. Therefore $(f, i_{\mathbb{R}}) \in R \cap R^{-1} = S$, so $f \in [i_{\mathbb{R}}]_S$. This completes the proof that $\{f \in \mathcal{F} \mid f \text{ is one-to-one}\} = [i_{\mathbb{R}}]_S \in \mathcal{F}/S$. To see that it is the largest element of $\mathcal{F}/S$, let $X \in \mathcal{F}/S$ be arbitrary. Then we can choose some $f \in \mathcal{F}$ such

that $X = [f]_S$. By part (c), $fRi_{\mathbb{R}}$, so $[f]_S T [i_{\mathbb{R}}]_S$, which means $XR[i_{\mathbb{R}}]_S$. Since X was arbitrary, this shows that $[i_{\mathbb{R}}]_S$ is the largest element of $\mathcal{F}/S$.

The second half of the problem is very similar. Let $g = \mathbb{R} \times \{0\}$. Then g is the constant function whose constant value is 0. We first show that $[g]_S = \{f \in \mathcal{F} \mid f \text{ is a constant function}\}$. To prove this, suppose $f \in [g]_S$. Then $(f, g) \in S = R \cap R^{-1}$, so fRg, and therefore, by part (f), f is a constant function. Now suppose $f \in \mathcal{F}$ and f is a constant function. Then by part (f), fRg, and by part (e), gRf. Therefore $(f, g) \in R \cap R^{-1} = S$, so $f \in [g]_S$. This completes the proof that $\{f \in \mathcal{F} \mid f \text{ is a constant function}\} = [g]_S \in \mathcal{F}/S$. To see that it is the smallest element of $\mathcal{F}/S$, let $X \in \mathcal{F}/S$ be arbitrary. Then we can choose some $f \in \mathcal{F}$ such that $X = [f]_S$. By part (e), gRf, so $[g]_S T [f]_S$, which means $[g]_S TX$. Since X was arbitrary, this shows that $[g]_S$ is the smallest element of $\mathcal{F}/S$.

23. (a) Yes, because for every $n \in \mathbb{N}$, $f(n) = n$, so $n \in \text{Ran}(f)$.
    (b) No, because, for example, $-1 \in \mathbb{Z}$ but $-1 \notin \text{Ran}(f)$.

Section 5.3

1. $R^{-1}(p) =$ the person sitting immediately to the right of p.
2. $F^{-1}(X) = A \setminus X$. Thus, $F^{-1} = F$.
3. Let $g(x) = (3x - 5)/2$. Then for any $x \in \mathbb{R}$,

$$f(g(x)) = \frac{2(3x-5)/2 + 5}{3} = \frac{3x - 5 + 5}{3} = \frac{3x}{3} = x$$

and

$$g(f(x)) = \frac{3(2x+5)/3 - 5}{2} = \frac{2x + 5 - 5}{2} = \frac{2x}{2} = x.$$

Therefore $f \circ g = i_{\mathbb{R}}$ and $g \circ f = i_{\mathbb{R}}$, and by Theorems 5.3.4 and 5.3.5 it follows that f is one-to-one and onto and $f^{-1} = g$, so $f^{-1}(x) = g(x) = (3x - 5)/2$.

4. Let $g(x) = \sqrt[3]{(x+3)/2}$. Then for any $x \in \mathbb{R}$,

$$f(g(x)) = 2\left(\sqrt[3]{\frac{x+3}{2}}\right)^3 - 3 = 2 \cdot \frac{x+3}{2} - 3 = x + 3 - 3 = x$$

and

$$g(f(x)) = \sqrt[3]{\frac{2x^3 - 3 + 3}{2}} = \sqrt[3]{\frac{2x^3}{2}} = \sqrt[3]{x^3} = x.$$

Therefore $f \circ g = i_{\mathbb{R}}$ and $g \circ f = i_{\mathbb{R}}$, and as in the previous exercise it follows that f is one-to-one and onto and $f^{-1} = g$, so $f^{-1}(x) = g(x) = \sqrt[3]{(x+3)/2}$.

5. Let $g : \mathbb{R}^+ \to \mathbb{R}$ be defined by the formula $g(x) = 2 - \log x$. Then for all $x \in \mathbb{R}^+$,

$$f(g(x)) = 10^{2-(2-\log x)} = 10^{\log x} = x,$$

and for all $x \in \mathbb{R}$,

$$g(f(x)) = 2 - \log(10^{2-x}) = 2 - (2 - x) = x.$$

Therefore $f \circ g = i_{\mathbb{R}^+}$ and $g \circ f = i_{\mathbb{R}}$, and it follows that f is one-to-one and onto and $f^{-1} = g$, so $f^{-1}(x) = g(x) = 2 - \log x$.

6. (a) Let $B = \mathbb{R} \setminus \{3\}$. Notice that for all $x \in A$,

$$f(x) = \frac{3x}{x-2} \neq \frac{3x-6}{x-2} = 3,$$

so $f(x) \in B$. Therefore $f : A \to B$.

Define $g : B \to A$ by the formula $g(x) = 2x/(x-3)$. Then for all $x \in B$,

$$f(g(x)) = \frac{3 \cdot \frac{2x}{x-3}}{\frac{2x}{x-3} - 2} = \frac{\frac{6x}{x-3}}{\frac{6}{x-3}} = \frac{6x}{6} = x,$$

and for all $x \in A$,

$$g(f(x)) = \frac{2 \cdot \frac{3x}{x-2}}{\frac{3x}{x-2} - 3} = \frac{\frac{6x}{x-2}}{\frac{6}{x-2}} = \frac{6x}{6} = x.$$

Therefore $f \circ g = i_B$ and $g \circ f = i_A$, so f is one-to-one and maps onto B.

(b) It follows from part (a) that $f^{-1} = g$, so $f^{-1}(x) = g(x) = 2x/(x-3)$.

7. (a) For all $x \in \mathbb{R}$, $(f_2 \circ f_1)(x) = f_2(f_1(x)) = f_2(x+7) = (x+7)/5 = f(x)$.

(b) It is easy to verify that $f_1^{-1}(x) = x - 7$ and $f_2^{-1}(x) = 5x$. Therefore $(f_1^{-1} \circ f_2^{-1})(x) = f_1^{-1}(f_2^{-1}(x)) = f_1^{-1}(5x) = 5x - 7 = f^{-1}(x)$.

8. (a) Let b be an arbitrary element of B. Let $a = f^{-1}(b) \in A$. Then $(b, a) \in f^{-1}$, so $(a, b) \in f$ and therefore $f(a) = b$. Thus,

$$(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b = i_B(b).$$

Since b was arbitrary, we have shown that $\forall b \in B((f \circ f^{-1})(b) = i_B(b))$, so $f \circ f^{-1} = i_B$.

(b) Since $f^{-1} : B \to A$ and $(f^{-1})^{-1} = f : A \to B$, by the first half of Theorem 5.3.2, $i_B = (f^{-1})^{-1} \circ f^{-1} = f \circ f^{-1}$.

9. Suppose that $f : A \to B$, $g : B \to A$, and $f \circ g = i_B$. Let b be an arbitrary element of B. Let $a = g(b) \in A$. Then $f(a) = f(g(b)) = (f \circ g)(b) = i_B(b) = b$. Since b was arbitrary, this shows that f is onto.

10. Let (b, a) be an arbitrary element of $B \times A$. Suppose $(b, a) \in g$. Then $g(b) = a$, so $f(a) = f(g(b)) = (f \circ g)(b) = i_B(b) = b$. Therefore $(a, b) \in f$, so $(b, a) \in f^{-1}$. Now suppose $(b, a) \in f^{-1}$. Then $(a, b) \in f$, so $f(a) = b$. Therefore $g(b) = g(f(a)) = (g \circ f)(a) = i_A(a) = a$, so $(b, a) \in g$.

11. (a) Suppose that f is one-to-one and $f \circ g = i_B$. By part 2 of Theorem 5.3.3, f is also onto, so $f^{-1} : B \to A$ and $f^{-1} \circ f = i_A$. This gives us enough information to imitate the reasoning in the proof of Theorem 5.3.5:

$$g = i_A \circ g = (f^{-1} \circ f) \circ g = f^{-1} \circ (f \circ g) = f^{-1} \circ i_B = f^{-1}.$$

(b) Suppose f is onto and $g \circ f = i_A$. By part 1 of Theorem 5.3.3, f is also one-to-one, so $f^{-1} : B \to A$ and $f \circ f^{-1} = i_B$. Therefore

$$g = g \circ i_B = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1} = i_A \circ f^{-1} = f^{-1}.$$

(c) Suppose $f \circ g = i_B$ and $g \circ f \neq i_A$. By part 2 of Theorem 5.3.3, f is onto. If f is one-to-one, then by part (a), $g = f^{-1}$, so $f^{-1} : B \to A$. But then by Theorem 5.3.2, $g \circ f = f^{-1} \circ f = i_A$, which is a contradiction. Therefore f is not one-to-one. Similarly, by part 1 of Theorem 5.3.3, g is one-to-one. If g is onto, then by part (b), $f = g^{-1}$, so $g^{-1} : A \to B$. But then by Theorem 5.3.2, $g \circ f = g \circ g^{-1} = i_A$, which is a contradiction. Therefore g is not onto.

12. Let $B' = \text{Ran}(f) \subseteq B$. Then $f : A \to B'$, f is one-to-one, and f maps onto B'. Therefore by Theorem 5.3.1, $f^{-1} : B' \to A$.

13. (a) It is clear from the definition of R that $\forall x \in A \forall y \in A(xRy \to f(x) = f(y))$, so in the terminology of exercise 21 in Section 5.1, f is compatible with R. Therefore, by part (a) of that exercise, there is a function $h : A/R \to B$ such that for all $x \in A$, $h([x]_R) = f(x)$.

    (b) It is clear from the definition of R that $\forall x \in A \forall y \in A(f(x) = f(y) \to xRy)$. Therefore, by exercise 19 in Section 5.2, h is one-to-one. To prove that h is onto, suppose $b \in B$. Since f is onto, there is some $x \in A$ such that $f(x) = b$. Therefore $h([x]_R) = f(x) = b$. Since b was arbitrary, this proves that h is onto.

    (c) Suppose $b \in B$. Since f is onto, we can choose some $y \in A$ such that $f(y) = b$. Therefore $h([y]_R) = f(y) = b$, so

$$h^{-1}(b) = [y]_R = \{x \in A \mid xRy\} = \{x \in A \mid f(x) = f(y)\} = \{x \in A \mid f(x) = b\}.$$

    (d) By part (c),

$$f \circ g = i_B \text{ iff } \forall b \in B(f(g(b)) = b) \text{ iff } \forall b \in B(g(b) \in \{x \in A \mid f(x) = b\}) \text{ iff } \forall b \in B(g(b) \in h^{-1}(b)).$$

14. (a) Suppose $x \in A' = \text{Ran}(g)$. Then we can choose some $b \in B$ such that $g(b) = x$. Therefore $(g \circ f)(x) = g(f(g(b))) = g((f \circ g)(b)) = g(i_B(b)) = g(b) = x$.

    (b) By the given information, $(f \upharpoonright A') \circ g = i_B$, and by part (a), $g \circ (f \upharpoonright A') = i_{A'}$. Therefore by Theorem 5.3.4, $f \upharpoonright A'$ is a one-to-one, onto function from A' to B, and by Theorem 5.3.5, $g = (f \upharpoonright A')^{-1}$.

15. Note that $\text{Ran}(g) = \{x \in \mathbb{R} \mid x \geq 0\} = B$. Also, for all $x \in B$, $(f \circ g)(x) = f(g(x)) = (\sqrt{x})^2 = x$, so $f \circ g = i_B$. Therefore by exercise 14, $g = (f \upharpoonright B)^{-1}$.

16. (a) $B = \{x \in \mathbb{R} \mid x \leq 4\}$. To prove this, suppose first that $y \in B = \text{Ran}(f)$. Then we can choose some $x \in \mathbb{R}$ such that $y = f(x) = 4x - x^2$. Therefore $4 - y = x^2 - 4x + 4 = (x-2)^2 \geq 0$, so $y \leq 4$, and therefore $y \in \{x \in \mathbb{R} \mid x \leq 4\}$. Now suppose $y \in \{x \in \mathbb{R} \mid x \leq 4\}$. Then $y \in \mathbb{R}$ and $y \leq 4$. Let $x = 2 + \sqrt{4-y}$, which is defined since $4 - y \geq 0$. Then

$$f(x) = 4(2 + \sqrt{4-y}) - (2 + \sqrt{4-y})^2 = 8 + 4\sqrt{4-y} - (4 + 4\sqrt{4-y} + 4 - y) = y,$$

    so $y \in \text{Ran}(f) = B$.

    (b) Since $B = \text{Ran}(f)$, $f : \mathbb{R} \to B$. Define $g : B \to \mathbb{R}$ by the formula $g(x) = 2 + \sqrt{4-x}$. The calculation in part (a) shows that for all $y \in B$, $f(g(y)) = y$, which shows that $f \circ g = i_B$. By exercise 14, if we let $A = \text{Ran}(g)$ then $f \upharpoonright A$ is a one-to-one, onto function from A to B, and $(f \upharpoonright A)^{-1}(x) = g(x) = 2 + \sqrt{4-x}$.

    We now prove that $A = \{x \in \mathbb{R} \mid x \geq 2\}$. To prove this, suppose first that $y \in A = \text{Ran}(g)$. Then we can choose some $x \in \mathbb{R}$ such that $y = g(x) = 2 + \sqrt{4-x}$. Since $\sqrt{4-x} \geq 0$, $y \geq 2$, so $y \in \{x \in \mathbb{R} \mid x \geq 2\}$. Now suppose $y \in \{x \in \mathbb{R} \mid x \geq 2\}$. Then $y \in \mathbb{R}$ and $y \geq 2$. Let $x = 4y - y^2$. Then $4 - x = y^2 - 4y + 4 = (y-2)^2$, and since $y \geq 2$, $y - 2 \geq 0$. Therefore $\sqrt{4-x} = y - 2$, so $g(x) = 2 + \sqrt{4-x} = 2 + y - 2 = y$. This proves that $y \in \text{Ran}(g) = A$.

17. (a) Suppose $f \in \mathcal{F}$. As we saw in Example 5.2.2, i_A is one-to-one and onto, so $i_A \in \mathcal{P}$. Also, $i_A^{-1} \circ f \circ i_A = i_A \circ f \circ i_A = f$, so $(f, f) \in R$. Therefore R is reflexive. Next, suppose $(f, g) \in R$. Then we can choose some $h \in \mathcal{P}$ such that $f = h^{-1} \circ g \circ h$. Since $(h^{-1})^{-1} = h : A \to A$, by Theorem 5.3.4, h^{-1} is one-to-one and onto, so $h^{-1} \in \mathcal{P}$. Also,

$$(h^{-1})^{-1} \circ f \circ h^{-1} = h \circ (h^{-1} \circ g \circ h) \circ h^{-1} = (h \circ h^{-1}) \circ g \circ (h \circ h^{-1}) = i_A \circ g \circ i_A = g,$$

so $(g, f) \in R$. Therefore R is symmetric. Finally, suppose $(f, g) \in R$ and $(g, h) \in R$. Then we can choose functions $j, k \in \mathcal{P}$ such that $f = j^{-1} \circ g \circ j$ and $g = k^{-1} \circ h \circ k$. By Theorem 5.2.5, $k \circ j$ is one-to-one and onto, so $k \circ j \in \mathcal{P}$. Also, applying part 5 of Theorem 4.2.5,

$$f = j^{-1} \circ g \circ j = j^{-1} \circ (k^{-1} \circ h \circ k) \circ j = (j^{-1} \circ k^{-1}) \circ h \circ (k \circ j) = (k \circ j)^{-1} \circ h \circ (k \circ j),$$

so $(f, h) \in R$. Therefore R is transitive.

(b) Suppose fRg. Then we can choose some $h \in \mathcal{P}$ such that $f = h^{-1} \circ g \circ h$. Therefore

$$f \circ f = (h^{-1} \circ g \circ h) \circ (h^{-1} \circ g \circ h) = h^{-1} \circ g \circ (h \circ h^{-1}) \circ g \circ h = h^{-1} \circ g \circ i_A \circ g \circ h = h^{-1} \circ (g \circ g) \circ h,$$

so $(f \circ f)R(g \circ g)$.

(c) Suppose f has a fixed point and fRg. Then we can choose some $a \in A$ such that $f(a) = a$, and we can also choose some $h \in \mathcal{P}$ such that $f = h^{-1} \circ g \circ h$. Therefore $a = f(a) = h^{-1}(g(h(a)))$, so $h(a) = g(h(a))$. This means that $h(a)$ is a fixed point of g.

18. Since g is one-to-one and onto, $g^{-1} : C \to B$. Let $h = g^{-1} \circ f$. Then $h : A \to B$ and $g \circ h = g \circ (g^{-1} \circ f) = (g \circ g^{-1}) \circ f = i_C \circ f = f$.

Section 5.4

1. (a) No: $f(0) = 1/2 \notin \mathbb{Z}$.
   (b) Yes.
   (c) Yes.
   (d) No: $f(2) = 3/2 \notin \{x \in \mathbb{R} \mid 2 \leq x < 4\}$.
2. (a) Yes.
   (b) Yes.
   (c) No: $f(\{100, 101, 102, \ldots, 199\}) = \{17, 100, 101, 102, \ldots, 199\}$, which has 101 elements.
   (d) Yes.
3. $f(-1) = 2$ and $f(1) = 0$, so we need to add those values to the set. It is easy to check that $\{-1, 0, 1, 2\}$ is closed under f, so it is the closre.
4. By exercise 12 of Section 4.3, all three sets sets are closed under f.
5. Yes: the statement $\forall x \in \varnothing(f(x) \in \varnothing)$ is vacuously true.
6. (a) Suppose $\text{Ran}(f) \subseteq C \subseteq A$. Suppose $x \in C$. Then $f(x) \in \text{Ran}(f)$, so $f(x) \in C$. Therefore C is closed under f.
   (b) Clearly $B \subseteq B \cup \text{Ran}(f) \subseteq A$, and by part (a), $B \cup \text{Ran}(f)$ is closed under f. Since the closure of B under f is the *smallest* subset of A that contains B and is closed under f, the closure is a subset of $B \cup \text{Ran}(f)$.
7. Suppose $C \subseteq A$ and C is closed under f. Suppose $x \in A \setminus C$, so $x \in A$ and $x \notin C$. Then $f^{-1}(x) \in A$. Suppose $f^{-1}(x) \in C$. Then since C is closed under f, $x = f(f^{-1}(x)) \in C$, which is a contradiction. Therefore $f^{-1}(x) \notin C$, so $f^{-1}(x) \in A \setminus C$. Since x was an arbitrary element of $A \setminus C$, this shows that $A \setminus C$ is closed under f^{-1}.
8. Let D be the closure of C under f.
   ($\rightarrow$) Suppose C is closed under f. Since D is the *smallest* subset of A that contains C and is closed under f, $D \subseteq C$. But also by definition of closure, $C \subseteq D$, so $D = C$.
   ($\leftarrow$) Suppose $D = C$. By definition, D is closed under f, so C is closed under f.

9. (a) Suppose $x \in C_1 \cup C_2$. Then either $x \in C_1$ or $x \in C_2$.
   Case 1. $x \in C_1$. Then since C_1 is closed under f, $f(x) \in C_1$, so $f(x) \in C_1 \cup C_2$.
   Case 2. $x \in C_2$. Then since C_2 is closed under f, $f(x) \in C_2$, so $f(x) \in C_1 \cup C_2$.
   Therefore $f(x) \in C_1 \cup C_2$. Since x was arbitrary, $C_1 \cup C_2$ is closed under f.

   (b) Yes. Proof: Suppose $x \in C_1 \cap C_2$. Then $x \in C_1$ and $x \in C_2$. Since $x \in C_1$ and C_1 is closed under f, $f(x) \in C_1$. Similarly, $f(x) \in C_2$. Therefore $f(x) \in C_1 \cap C_2$, so since x was arbitrary, $C_1 \cap C_2$ is closed under f.

   (c) No. Here is a counterexample: $A = \{1, 2\}$, $f = \{(1, 2), (2, 2)\}$, $C_1 = \{1, 2\}$, $C_2 = \{2\}$.

10. (a) Suppose $B_1 \subseteq B_2$. Then $B_1 \subseteq B_2 \subseteq C_2 \subseteq A$ and C_2 is closed under f. Since C_1 is the *smallest* subset of A that contains B_1 and is closed under f, $C_1 \subseteq C_2$.

    (b) Clearly $B_1 \cup B_2 \subseteq C_1 \cup C_2 \subseteq A$, and by part (a) of exercise 9, $C_1 \cup C_2$ is closed under f. Now suppose $B_1 \cup B_2 \subseteq D \subseteq A$ and D is closed under f. Then since $B_1 \subseteq D$ and C_1 is the *smallest* subset of A that contains B_1 and is closed under f, $C_1 \subseteq D$. Similarly, since $B_2 \subseteq D$, $C_2 \subseteq D$. Therefore $C_1 \cup C_2 \subseteq D$. Since D was arbitrary, this shows that $C_1 \cup C_2$ is the closure of $B_1 \cup B_2$ under f.

    (c) No. Counterexample: $A = \{1, 2, 3\}$, $f = \{(1, 1), (2, 2), (3, 2)\}$, $B_1 = \{1, 2\}$, $B_2 = \{1, 3\}$.

    (d) No. The counterexample in part (c) is a counterexample for (d) as well.

11. Let $\mathcal{F} = \{C \subseteq A \mid B \subseteq C \text{ and } C \text{ is closed under } f\}$. You should be able to check that $A \in \mathcal{F}$, and therefore $\mathcal{F} \neq \varnothing$. Thus, we can let $C = \bigcap \mathcal{F}$, and by exercise 9 of Section 3.3, $C \subseteq A$. We will show that C is the closure of B under f by proving the three properties in Definition 5.4.8.

    To prove the first property, suppose $x \in B$. Let D be an arbitrary element of $\mathcal{F}$. Then by the definition of $\mathcal{F}$, $B \subseteq D$, so $x \in D$. Since D was arbitrary, this shows that $\forall D \in \mathcal{F}(x \in D)$, so $x \in \bigcap \mathcal{F} = C$. Thus, $B \subseteq C$.

    Next, suppose $x, y \in C$ and again let D be an arbitrary element of $\mathcal{F}$. Then since $x, y \in C = \bigcap \mathcal{F}$, $x \in D$ and $y \in D$. But since $D \in \mathcal{F}$, D is closed under f, so $f(x, y) \in D$. Since D was arbitrary, we can conclude that $\forall D \in \mathcal{F}(f(x, y) \in D)$, so $f(x, y) \in \bigcap \mathcal{F} = C$. Thus, we have shown that C is closed under f, which is the second property in Definition 5.4.8.

    Finally, to prove the third property, suppose $B \subseteq D \subseteq A$ and D is closed under f. Then $D \in \mathcal{F}$, and applying exercise 9 of Section 3.3 again we can conclude that $C = \bigcap \mathcal{F} \subseteq D$.

12. (a) $\mathbb{Z}$.

    (b) $\{X \subseteq \mathbb{N} \mid X \text{ is finite}\}$.

13. (a) Let $\mathcal{G} = \{C \subseteq A \mid B \subseteq C \text{ and } C \text{ is closed under } \mathcal{F}\}$. You should be able to check that $A \in \mathcal{G}$, and therefore $\mathcal{G} \neq \varnothing$. Thus, we can let $C = \bigcap \mathcal{G}$, and by exercise 9 of Section 3.3, $C \subseteq A$. We will show that C is the closure of B under $\mathcal{F}$.

    To prove that $B \subseteq C$, suppose $x \in B$. Let D be an arbitrary element of $\mathcal{G}$. Then by the definition of $\mathcal{G}$, $B \subseteq D$, so $x \in D$. Since D was arbitrary, this shows that $\forall D \in \mathcal{G}(x \in D)$, so $x \in \bigcap \mathcal{G} = C$. Thus, $B \subseteq C$.

    Next, suppose $f \in \mathcal{F}$ and $x \in C$ and again let D be an arbitrary element of $\mathcal{G}$. Then since $x \in C = \bigcap \mathcal{G}$, $x \in D$. But since $D \in \mathcal{G}$, D is closed under $\mathcal{F}$, so $f(x) \in D$. Since D was arbitrary, we can conclude that $\forall D \in \mathcal{G}(f(x) \in D)$, so $f(x) \in \bigcap \mathcal{G} = C$. Thus, we have shown that C is closed under $\mathcal{F}$.

    Finally, to prove that C is the *smallest* subset of A containing B that is closed under $\mathcal{F}$, suppose $B \subseteq D \subseteq A$ and D is closed under $\mathcal{F}$. Then $D \in \mathcal{G}$, and applying exercise 9 of Section 3.3 again we can conclude that $C = \bigcap \mathcal{G} \subseteq D$.

    (b) Suppose $x \in \bigcup_{f \in \mathcal{F}} C_f$. Then we can choose some $f \in \mathcal{F}$ such that $x \in C_f$. Since C is closed under $\mathcal{F}$ and $f \in \mathcal{F}$, C is closed under f. Also, $B \subseteq C \subseteq A$. But C_f is the *smallest* subset of A that contains B and is closed under f, so $C_f \subseteq C$. Since $x \in C_f$, $x \in C$. Since x was arbitrary, we conclude that $\bigcup_{f \in \mathcal{F}} C_f \subseteq C$.

(c) No. Counterexample: $A = \{1, 2, 3\}$, $f = \{(1, 1), (2, 3), (3, 3)\}$, $g = \{(1, 2), (2, 2), (3, 3)\}$, $\mathcal{F} = \{f, g\}$, $B = \{1\}$.

(d) No. The counterexample in part (c) is a counterexample for (d) as well.

14. $\mathbb{Z}$.

15. $\mathbb{Q}^+$.

16. (a) Suppose $X \subseteq \mathbb{N}$. Let $E = \{n \in \mathbb{N} \mid n \text{ is even}\}$ and let $O = \{n \in \mathbb{N} \mid n \text{ is odd}\}$. Let $Y = X \cup E$ and $Z = X \cup O$. Clearly Y and Z are both infinite, so $Y \in \mathcal{I}$ and $Z \in \mathcal{I}$. To prove that $Y \cap Z = X$, suppose $n \in Y \cap Z$. Then $n \in Y$ and $n \in Z$.

Case 1. n is even. Then $n \notin O$ and $n \in Z = X \cup O$, so $n \in X$.

Case 2. n is odd. Then $n \notin E$ and $n \in Y = X \cup E$, so $n \in X$.

Thus, $n \in X$. Next, suppose $n \in X$. Then $n \in X \cup E = Y$ and $n \in X \cup O = Z$, so $n \in Y \cap Z$.

(b) $\mathscr{P}(\mathbb{N})$.

17. (a) Yes, by part 1 of Theorem 5.2.5.

(b) Yes, by part 2 of Theorem 5.2.5.

(c) Yes: If f and g are strictly increasing functions, then for all real numbers x and y, if $x < y$ then $g(x) < g(y)$, and therefore $f(g(x)) < f(g(y))$. This shows that $f \circ g$ is strictly increasing.

(d) No. (The composition of two strictly decreasing functions is strictly increasing.)

18. (a) No. Let $f(x) = x$ and $g(x) = -x$. Then f and g are one-to-one, but $(f + g)(x) = 0$, so $f + g$ is not one-to-one.

(b) No. Let $f(x) = x$ and $g(x) = -x$. Then f and g are onto, but $(f + g)(x) = 0$, so $f + g$ is not onto.

(c) Yes: If f and g are strictly increasing functions, then for all real numbers x and y, if $x < y$ then $f(x) < f(y)$ and $g(x) < g(y)$, so $(f + g)(x) = f(x) + g(x) < f(y) + g(y) = (f + g)(y)$.. Therefore $f + g$ is strictly increasing.

(d) Yes. The proof is similar to the proof for part (c).

19. By exercise 16 in Section 4.3, the set of reflexive relations is closed under $\circ$. The set of symmetric relations need not be closed under $\circ$. For example, if $A = \{1, 2, 3\}$, $R = \{(1, 2), (2, 1)\}$, and $S = \{(2, 3), (3, 2)\}$, then R and S are symmetric, but $R \circ S = \{(3, 1)\}$, which is not symmetric. The set of transitive relations also need not be closed under $\circ$. For example, if $A = \{1, 2, 3\}$, $R = \{(1, 2), (3, 3)\}$, and $S = \{(1, 1), (2, 3)\}$, then R and S are transitive, but $R \circ S = \{(1, 2), (2, 3)\}$, which is not transitive.

20. (a) Not closed, because $f(1, 0) = \text{NaN} \notin \mathbb{R}$.

(b) Closed.

(c) Not closed, because $f(-1, -1) = 1 \notin \mathbb{R}^-$.

(d) Not closed, because $f(1, 0) = \text{NaN} \notin \mathbb{Q}$.

(e) Closed.

21. (a) Let $\mathcal{G} = \{C \subseteq A \mid B \subseteq C \text{ and } C \text{ is closed under } \mathcal{F}\}$. You should be able to check that $A \in \mathcal{G}$, and therefore $\mathcal{G} \neq \varnothing$. Thus, we can let $C = \bigcap \mathcal{G}$, and by exercise 9 of Section 3.3, $C \subseteq A$. We will show that C is the closure of B under $\mathcal{F}$.

To prove that $B \subseteq C$, suppose $x \in B$. Let D be an arbitrary element of $\mathcal{G}$. Then by the definition of $\mathcal{G}$, $B \subseteq D$, so $x \in D$. Since D was arbitrary, this shows that $\forall D \in \mathcal{G}(x \in D)$, so $x \in \bigcap \mathcal{G} = C$. Thus, $B \subseteq C$.

Next, suppose $f \in \mathcal{F}$ and $x, y \in C$ and again let D be an arbitrary element of $\mathcal{G}$. Then since $x, y \in C = \bigcap \mathcal{G}$, $x \in D$ and $y \in D$. But since $D \in \mathcal{G}$, D is closed under $\mathcal{F}$, so $f(x, y) \in D$. Since D was arbitrary, we can conclude that $\forall D \in \mathcal{G}(f(x, y) \in D)$, so $f(x, y) \in \bigcap \mathcal{G} = C$. Thus, we have shown that C is closed under $\mathcal{F}$.

Finally, suppose $B \subseteq D \subseteq A$ and D is closed under $\mathcal{F}$. Then $D \in \mathcal{G}$, and applying exercise 9 of Section 3.3 again we can conclude that $C = \bigcap \mathcal{G} \subseteq D$.

(b) We will use the notation $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Suppose $x, y \in \mathbb{Q}(\sqrt{2})$. Then we can choose rational numbers a, b, c, and d such that $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$. Therefore $f(x, y) = x + y = (a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, since $a + c \in \mathbb{Q}$ and $b + d \in \mathbb{Q}$. Also, $g(x, y) = xy = (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, since $ac + 2bd \in \mathbb{Q}$ and $ad + bc \in \mathbb{Q}$. Therefore $\mathbb{Q}(\sqrt{2})$ is closed under $\{f, g\}$. Now suppose $\mathbb{Q} \cup \{\sqrt{2}\} \subseteq D \subseteq \mathbb{R}$ and D is closed under $\{f, g\}$. Let $x \in \mathbb{Q}(\sqrt{2})$ be arbitrary. Then we can choose rational numbers a and b such that $x = a + b\sqrt{2} = f(a, g(b, \sqrt{2}))$. Since $a, b, \sqrt{2} \in D$ and D is closed under $\{f, g\}$, $x \in D$. Since x was arbitrary, $\mathbb{Q}(\sqrt{2}) \subseteq D$.

(c) $\{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$.

Section 5.5

1. (a) Yes. Proof: Suppose $y \in f(W \cup X)$. Then we can choose some $x \in W \cup X$ such that $y = f(x)$. Since $x \in W \cup X$, either $x \in W$ or $x \in X$.

Case 1. $x \in W$. Then $y = f(x) \in f(W)$, so $y \in f(W) \cup f(X)$.

Case 2. $x \in X$. Then $y = f(x) \in f(X)$, so $y \in f(W) \cup f(X)$.

Since y was arbitrary, $f(W \cup X) \subseteq f(W) \cup f(X)$. Now suppose $y \in f(W) \cup f(X)$, so either $y \in f(W)$ or $y \in f(X)$.

Case 1. $y \in f(W)$. Then we can choose some $w \in W$ such that $y = f(w)$. Since $w \in W$, $w \in W \cup X$, so $y = f(w) \in f(W \cup X)$.

Case 2. $y \in f(X)$. Then we can choose some $x \in X$ such that $y = f(x)$. Since $x \in X$, $x \in W \cup X$, so $y = f(x) \in f(W \cup X)$.

Since y was arbitrary, $f(W) \cup f(X) \subseteq f(W \cup X)$. Therefore $f(W \cup X) = f(W) \cup f(X)$.

(b) What is always true is that $f(W) \setminus f(X) \subseteq f(W \setminus X)$, and if f is one-to-one then $f(W \setminus X) = f(W) \setminus f(X)$. Proof: Suppose $y \in f(W) \setminus f(X)$. Then $y \in f(W)$ and $y \notin f(X)$. Since $y \in f(W)$, we can choose some $w \in W$ such that $y = f(w)$. If $w \in X$ then $y = f(w) \in f(X)$, which is a contradiction, so $w \notin X$. Since $w \in W$ and $w \notin X$, $w \in W \setminus X$, so $y = f(w) \in f(W \setminus X)$. Since y was arbitrary, this proves that $f(W) \setminus f(X) \subseteq f(W \setminus X)$.

Now suppose f is one-to-one and $y \in f(W \setminus X)$. Then we can choose some $w \in W \setminus X$ such that $y = f(w)$. Since $w \in W \setminus X$, $w \in W$ and $w \notin X$. Therefore $y = f(w) \in f(W)$. Suppose $y \in f(X)$. Then we can choose some $x \in X$ such that $y = f(x)$. Therefore $f(x) = y = f(w)$, so since f is one-to-one, $w = x \in X$, which is a contradiction. Therefore $y \notin f(X)$, so $y \in f(W) \setminus f(X)$. Since y was arbitrary, $f(W \setminus X) \subseteq f(W) \setminus f(X)$, so $f(W) \setminus f(X) = f(W \setminus X)$.

Example in which $f(W) \setminus f(X) \neq f(W \setminus X)$: $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$, $f = \{(1, 4), (2, 5), (3, 5)\}$, $W = \{1, 2\}$, $X = \{1, 3\}$.

(c) What is always true is that $W \subseteq X \to f(W) \subseteq f(X)$, and if f is one-to-one then $f(W) \subseteq f(X) \to W \subseteq X$. Proof: Suppose $W \subseteq X$. Suppose $y \in f(W)$. Then we can choose some $w \in W$ such that $y = f(w)$. Since $w \in W$ and $W \subseteq X$, $w \in X$, so $y = f(w) \in f(X)$. Since y was arbitrary, this shows that $f(W) \subseteq f(X)$. Thus $W \subseteq X \to f(W) \subseteq f(X)$.

Now suppose f is one-to-one and $f(W) \subseteq f(X)$. Suppose $w \in W$. Then $f(w) \in f(W)$, so since $f(W) \subseteq f(X)$, $f(w) \in f(X)$. Therefore we can choose some $x \in X$ such that $f(w) = f(x)$. But since f is one-to-one, this implies that $w = x \in X$. Since w was arbitrary, this proves that $W \subseteq X$. Thus, if f is one-to-one then $f(W) \subseteq f(X) \to W \subseteq X$.

Example in which $f(W) \subseteq f(X)$ but $W \nsubseteq X$: Same as example in part (b).

2. (a) Yes. Proof: Let $x \in A$ be arbitrary. Then

$$x \in f^{-1}(Y \cap Z) \text{ iff } f(x) \in Y \cap Z \text{ iff } f(x) \in Y \wedge f(x) \in Z$$

$$\text{iff } x \in f^{-1}(Y) \wedge x \in f^{-1}(Z) \text{ iff } x \in f^{-1}(Y) \cap f^{-1}(Z).$$

(b) Yes. Proof: Let $x \in A$ be arbitrary. Then

$$\begin{aligned} x \in f^{-1}(Y \cup Z) &\text{ iff } f(x) \in Y \cup Z \text{ iff } f(x) \in Y \vee f(x) \in Z \\ &\text{iff } x \in f^{-1}(Y) \vee x \in f^{-1}(Z) \text{ iff } x \in f^{-1}(Y) \cup f^{-1}(Z). \end{aligned}$$

(c) Yes. Proof: Let $x \in A$ be arbitrary. Then

$$\begin{aligned} x \in f^{-1}(Y \setminus Z) &\text{ iff } f(x) \in Y \setminus Z \text{ iff } f(x) \in Y \wedge f(x) \notin Z \\ &\text{iff } x \in f^{-1}(Y) \wedge x \notin f^{-1}(Z) \text{ iff } x \in f^{-1}(Y) \setminus f^{-1}(Z). \end{aligned}$$

(d) What is always true is that $Y \subseteq Z \to f^{-1}(Y) \subseteq f^{-1}(Z)$, and if f is onto then $f^{-1}(Y) \subseteq f^{-1}(Z) \to Y \subseteq Z$. Proof: Suppose $Y \subseteq Z$. Suppose $x \in f^{-1}(Y)$. Then $f(x) \in Y$. Since $f(x) \in Y$ and $Y \subseteq Z$, $f(x) \in Z$, so $x \in f^{-1}(Z)$. Since x was arbitrary, this shows that $f^{-1}(Y) \subseteq f^{-1}(Z)$. Thus $Y \subseteq Z \to f^{-1}(Y) \subseteq f^{-1}(Z)$.

Now suppose f is onto and $f^{-1}(Y) \subseteq f^{-1}(Z)$. Suppose $y \in Y$. Since f is onto, we can choose some $x \in A$ such that $f(x) = y$. Since $f(x) = y \in Y$, $x \in f^{-1}(Y)$, and since $f^{-1}(Y) \subseteq f^{-1}(Z)$, it follows that $x \in f^{-1}(Z)$. Therefore $y = f(x) \in Z$. Since y was arbitrary, this shows that $Y \subseteq Z$. Thus, if f is onto then $f^{-1}(Y) \subseteq f^{-1}(Z) \to Y \subseteq Z$.

Example in which $f^{-1}(Y) \subseteq f^{-1}(Z)$ but $Y \not\subseteq Z$: $A = \{1,2,3\}$, $B = \{4,5,6\}$, $f = \{(1,4),(2,5),(3,5)\}$, $Y = \{5,6\}$, $Z = \{4,5\}$.

3. What is always true is that $X \subseteq f^{-1}(f(X))$, and if f is one-to-one then $f^{-1}(f(X)) = X$. Proof: Suppose $x \in X$. Then $f(x) \in f(X)$, so $x \in f^{-1}(f(X))$. Since x was arbitrary, this proves that $X \subseteq f^{-1}(f(X))$.

Now suppose f is one-to-one. Suppose $x \in f^{-1}(f(X))$. Then $f(x) \in f(X)$, so we can choose some $x' \in X$ such that $f(x) = f(x')$. Since f is one-to-one, $x = x' \in X$. Since x was arbitrary, this shows that $f^{-1}(f(X)) \subseteq X$, so $f^{-1}(f(X)) = X$.

An example in which $f^{-1}(f(X)) \neq X$ was given in the text: $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, $X = \{x \in \mathbb{R} \mid 0 \leq x < 2\}$.

4. What is always true is that $f(f^{-1}(Y)) \subseteq Y$, and if f is onto then $f(f^{-1}(Y)) = Y$. Proof: Suppose $y \in f(f^{-1}(Y))$. Then we can choose some $x \in f^{-1}(Y)$ such that $y = f(x)$. Since $x \in f^{-1}(Y)$, $y = f(x) \in Y$. Since y was arbitrary, this shows that $f(f^{-1}(Y)) \subseteq Y$.

Now suppose f is onto. Suppose $y \in Y$. Since f is onto, we can choose some $x \in A$ such that $f(x) = y$. Since $f(x) = y \in Y$, $x \in f^{-1}(Y)$, so $y = f(x) \in f(f^{-1}(Y))$. Since y was arbitrary, this shows that $Y \subseteq f(f^{-1}(Y))$, so $f(f^{-1}(Y)) = Y$.

Example in which $f(f^{-1}(Y)) \neq Y$: $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, $Y = \{x \in \mathbb{R} \mid -4 < x < 4\}$.

5. (a) $\to$ (b). Suppose C is closed under f. Suppose $y \in f(C)$. Then we can choose some $x \in C$ such that $y = f(x)$. Since C is closed under f, $y = f(x) \in C$. Thus $f(C) \subseteq C$.

(b) $\to$ (c). Suppose $f(C) \subseteq C$. Suppose $x \in C$. Then $f(x) \in f(C)$, so since $f(C) \subseteq C$, $f(x) \in C$. Therefore $x \in f^{-1}(C)$. Thus $C \subseteq f^{-1}(C)$.

(c) $\to$ (a). Suppose $C \subseteq f^{-1}(C)$. Suppose $x \in C$. Then since $C \subseteq f^{-1}(C)$, $x \in f^{-1}(C)$, so $f(x) \in C$. Since x was arbitrary, this shows that C is closed under f.

6. Here are two interesting facts:

(a) For all $X \subseteq A$, $(g \circ f)(X) = g(f(X))$.

(b) For all $Z \subseteq C$, $(g \circ f)^{-1}(Z) = f^{-1}(g^{-1}(Z))$.

Proof of (a): Suppose $X \subseteq A$. Suppose $z \in (g \circ f)(X)$. Then we can choose some $x \in X$ such that $z = (g \circ f)(x) = g(f(x))$. Since $x \in X$, $f(x) \in f(X)$, so $z = g(f(x)) \in g(f(X))$.

Now suppose $z \in g(f(X))$. Then we can choose some $y \in f(X)$ such that $z = g(y)$. Since $y \in f(X)$, we can choose some $x \in X$ such that $y = f(x)$. Therefore $z = g(y) = g(f(x)) = (g \circ f)(x) \in (g \circ f)(X)$. Thus $(g \circ f)(X) = g(f(X))$.

Proof of (b): Suppose $Z \subseteq C$. Suppose $x \in A$. Then

$$x \in (g \circ f)^{-1}(Z) \text{ iff } (g \circ f)(x) \in Z \text{ iff } g(f(x)) \in Z \text{ iff } f(x) \in g^{-1}(Z) \text{ iff } x \in f^{-1}(g^{-1}(Z)).$$

7. Let X_1 be the inverse image of Y under f, and let X_2 be the image of Y under f^{-1}. This means that

$$X_1 = \{x \in A \mid f(x) \in Y\},$$
$$X_2 = \{f^{-1}(y) \mid y \in Y\} = \{x \in A \mid \exists y \in Y(f^{-1}(y) = x)\}.$$

We must prove $X_1 = X_2$. Suppose $x \in X_1$. Then $f(x) \in Y$. Let $y = f(x) \in Y$. Then $x = f^{-1}(y) \in X_2$. Now suppose $x \in X_2$. Then we can choose some $y \in Y$ such that $f^{-1}(y) = x$. Therefore $f(x) = y \in Y$, so $x \in X_1$.

Chapter 6

Section 6.1

1. Base case: When $n = 0$, both sides of the equation are 0.

Induction step: Suppose that $n \in \mathbb{N}$ and $0 + 1 + 2 + \cdots + n = n(n+1)/2$. Then

$$\begin{aligned} 0 + 1 + 2 + \cdots + (n+1) &= (0 + 1 + 2 + \cdots + n) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= (n+1)\left(\frac{n}{2} + 1\right) = \frac{(n+1)(n+2)}{2}, \end{aligned}$$

as required.

2. Base case: When $n = 0$, both sides of the equation are 0.

Induction step: Suppose $n \in \mathbb{N}$ and $0^2 + 1^2 + 2^2 + \cdots + n^2 = n(n+1)(2n+1)/6$. Then

$$\begin{aligned} 0^2 + 1^2 + 2^2 + \cdots + (n+1)^2 &= (0^2 + 1^2 + 2^2 + \cdots + n^2) + (n+1)^2 \\ &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = (n+1) \cdot \frac{n(2n+1) + 6(n+1)}{6} \\ &= \frac{(n+1)(2n^2 + 7n + 6)}{6} = \frac{(n+1)(n+2)(2(n+1)+1)}{6}. \end{aligned}$$

3. Base case: When $n = 0$, both sides of the equation are 0.

Induction step: Suppose $n \in \mathbb{N}$ and $0^3 + 1^3 + 2^3 + \cdots + n^3 = [n(n+1)/2]^2$. Then

$$\begin{aligned} 0^3 + 1^3 + 2^3 + \cdots + (n+1)^3 &= \left(0^3 + 1^3 + 2^3 + \cdots + n^3\right) + (n+1)^3 \\ &= \left[\frac{n(n+1)}{2}\right]^2 + (n+1)^3 = (n+1)^2\left[\frac{n^2}{4} + n + 1\right] \\ &= (n+1)^2 \cdot \frac{n^2 + 4n + 4}{4} = \left[\frac{(n+1)(n+2)}{2}\right]^2. \end{aligned}$$

4. For all $n \geq 1$, $1 + 3 + 5 + \cdots + (2n-1) = n^2$. We prove this by mathematical induction.
   Base case: When $n = 1$, both sides of the equation are 1.
   Induction step: Suppose $n \geq 1$ and $1 + 3 + 5 + \cdots + (2n-1) = n^2$. Then

$$\begin{aligned} 1 + 3 + 5 + \cdots + (2(n+1) - 1) &= (1 + 3 + 5 + \cdots + (2n-1)) + (2n+1) \\ &= n^2 + 2n + 1 = (n+1)^2. \end{aligned}$$

5. Base case: When $n = 0$, both sides of the equation are 0.
   Induction step: Suppose $n \in \mathbb{N}$ and $0 \cdot 1 + 1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = n(n+1)(n+2)/3$. Then

$$\begin{aligned} 0 \cdot 1 + 1 \cdot 2 + 2 \cdot 3 + \cdots + (n+1)(n+2) &= (0 \cdot 1 + 1 \cdot 2 + 2 \cdot 3 + \cdots n(n+1)) + (n+1)(n+2) \\ &= \frac{n(n+1)(n+2)}{3} + (n+1)(n+2) \\ &= (n+1)(n+2)\left(\frac{n}{3} + 1\right) = \frac{(n+1)(n+2)(n+3)}{3}. \end{aligned}$$

6. For all $n \in \mathbb{N}$, $0 \cdot 1 \cdot 2 + 1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + n(n+1)(n+2) = n(n+1)(n+2)(n+3)/4$. We prove this by mathematical induction.
   Base case: When $n = 0$, both sides of the equation are 0.
   Induction step: Suppose $n \in \mathbb{N}$ and $0 \cdot 1 \cdot 2 + 1 \cdot 2 \cdot 3 + \cdots + n(n+1)(n+2) = n(n+1)(n+2)(n+3)/4$. Then

$$\begin{aligned} &0 \cdot 1 \cdot 2 + 1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + (n+1)(n+2)(n+3) \\ &\quad = (0 \cdot 1 \cdot 2 + 1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + n(n+1)(n+2)) + (n+1)(n+2)(n+3) \\ &\quad = \frac{n(n+1)(n+2)(n+3)}{4} + (n+1)(n+2)(n+3) \\ &\quad = (n+1)(n+2)(n+3)\left(\frac{n}{4} + 1\right) = \frac{(n+1)(n+2)(n+3)(n+4)}{4}. \end{aligned}$$

7. For all $n \in \mathbb{N}$, $3^0 + 3^1 + 3^2 + \cdots + 3^n = (3^{n+1} - 1)/2$. We prove this by mathematical induction.
   Base case: Setting $n = 0$, we get $3^0 = 1 = (3^1 - 1)/2$.
   Induction step: Suppose $n \in \mathbb{N}$ and $3^0 + 3^1 + 3^2 + \cdots + 3^n = (3^{n+1} - 1)/2$. Then

$$\begin{aligned} 3^0 + 3^1 + 3^2 + \cdots + 3^{n+1} &= (3^0 + 3^1 + 3^2 + \cdots + 3^n) + 3^{n+1} \\ &= \frac{3^{n+1} - 1}{2} + 3^{n+1} = \frac{3 \cdot 3^{n+1} - 1}{2} = \frac{3^{n+2} - 1}{2}. \end{aligned}$$

8. Base case: When $n = 1$, the equation is $1 - 1/2 = 1/2$, which is true.
   Induction step: Suppose $n \geq 1$ and

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{1}{2n-1} - \frac{1}{2n} = \frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n}.$$

   Then

$$\begin{aligned} &1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{1}{2(n+1)-1} - \frac{1}{2(n+1)} \\ &\quad = \left(1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{1}{2n-1} - \frac{1}{2n}\right) + \frac{1}{2n+1} - \frac{1}{2n+2} \\ &\quad = \left(\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n}\right) + \frac{1}{2n+1} - \frac{1}{2n+2} \end{aligned}$$

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

9. (a) Base case: When $n = 0$, $n^2 + n = 0 = 0 \cdot 2$, so $2 \mid (n^2 + n)$.
Induction step: Suppose $n \in \mathbb{N}$ and $2 \mid (n^2 + n)$. Then there is some integer k such that $n^2+n = 2k$. Therefore $(n+1)^2+(n+1) = n^2+3n+2 = n^2+n+2n+2 = 2k+2n+2 = 2(k+n+1)$, so $2 \mid ((n+1)^2 + (n+1))$.
(b) Base case: When $n = 0$, $n^3 - n = 0 = 0 \cdot 6$, so $6 \mid (n^3 - n)$.
Induction step. Suppose $n \in \mathbb{N}$ and $6 \mid (n^3 - n)$. Then there is some integer k such that $n^3 - n = 6k$. Also, by part (a), there is some integer j such that $n^2 + n = 2j$. Therefore $(n+1)^3 - (n+1) = (n^3 + 3n^2 + 3n + 1) - (n+1) = (n^3 - n) + 3(n^2 + n) = 6k + 3(2j) = 6(k + j)$, so $6 \mid ((n+1)^3 - (n+1))$.

10. Base case: When $n = 0$, $9^n - 8n - 1 = 0 = 64 \cdot 0$, so $64 \mid (9^n - 8n - 1)$.
Induction step: Suppose that $n \in \mathbb{N}$ and $64 \mid (9^n - 8n - 1)$. Then there is some integer k such that $9^n - 8n - 1 = 64k$. Therefore

$$\begin{aligned} 9^{n+1} - 8(n+1) - 1 &= 9^{n+1} - 8n - 9 \\ &= 9^{n+1} - 72n - 9 + 64n \\ &= 9(9^n - 8n - 1) + 64n \\ &= 9(64k) + 64n \\ &= 64(9k + n), \end{aligned}$$

so $64 \mid (9^{n+1} - 8(n+1) - 1)$.

11. Base case: When $n = 0$, $4^n + 6n - 1 = 0 = 0 \cdot 9$, so $9 \mid (4^n + 6n - 1)$.
Induction step: Suppose $n \in \mathbb{N}$ and $9 \mid (4^n + 6n - 1)$. Then there is some integer k such that $4^n + 6n - 1 = 9k$. Therefore

$$\begin{aligned} 4^{n+1} + 6(n+1) - 1 &= 4^{n+1} + 6n + 5 \\ &= 4^{n+1} + 24n - 4 + 9 - 18n \\ &= 4(4^n + 6n - 1) + 9 - 18n \\ &= 4(9k) + 9(1 - 2n) = 9(4k + 1 - 2n), \end{aligned}$$

so $9 \mid (4^{n+1} + 6(n+1) - 1)$.

12. (a) Base case: When $n = 0$, $7^n - 5^n = 0 = 2 \cdot 0$, so $7^n - 5^n$ is even.
Induction step: Suppose $n \in \mathbb{N}$ and $7^n - 5^n$ is even. Then there is some integer k such that $7^n - 5^n = 2k$. Therefore

$$\begin{aligned} 7^{n+1} - 5^{n+1} &= 7 \cdot 7^n - 5 \cdot 5^n = 2 \cdot 7^n + 5 \cdot (7^n - 5^n) \\ &= 2 \cdot 7^n + 5 \cdot 2k = 2(7^n + 5k), \end{aligned}$$

so $7^{n+1} - 5^{n+1}$ is even.
(b) Base case: When $n = 0$, $2 \cdot 7^n - 3 \cdot 5^n + 1 = 0 = 0 \cdot 24$, so $24 \mid (2 \cdot 7^n - 3 \cdot 5^n + 1)$.
Induction step: Suppose $n \in \mathbb{N}$ and $24 \mid (2 \cdot 7^n - 3 \cdot 5^n + 1)$. Then there is some integer k such that $2 \cdot 7^n - 3 \cdot 5^n + 1 = 24k$. Also, by part (a), there is some integer j such that $7^n - 5^n = 2j$. Therefore

$$2 \cdot 7^{n+1} - 3 \cdot 5^{n+1} + 1 = 14 \cdot 7^n - 15 \cdot 5^n + 1$$

$$= (2 \cdot 7^n - 3 \cdot 5^n + 1) + 12(7^n - 5^n)$$
$$= 24k + 12(2j) = 24(k + j),$$

so $24 \mid (2 \cdot 7^{n+1} - 3 \cdot 5^{n+1} + 1)$.

13. Let a and b be arbitrary integers. We now use induction to prove that $\forall n \in \mathbb{N}[(a - b) \mid (a^n - b^n)]$.

Base case: When $n = 0$, $a^n - b^n = 0 = 0 \cdot (a - b)$, so $(a - b) \mid (a^n - b^n)$.

Induction step: Suppose $n \in \mathbb{N}$ and $(a - b) \mid (a^n - b^n)$. Then there is some integer k such that $a^n - b^n = k(a - b)$. Therefore

$$\begin{aligned} a^{n+1} - b^{n+1} &= a^{n+1} - ab^n + ab^n - b^{n+1} \\ &= a(a^n - b^n) + b^n(a - b) \\ &= ak(a - b) + b^n(a - b) = (ak + b^n)(a - b), \end{aligned}$$

so $(a - b) \mid (a^{n+1} - b^{n+1})$.

14. Let a and b be arbitrary integers. We now use induction to prove that $\forall n \in \mathbb{N}[(a+b) \mid (a^{2n+1} + b^{2n+1})]$.

Base case: When $n = 0$, $a^{2n+1} + b^{2n+1} = a + b$, so $(a + b) \mid (a^{2n+1} + b^{2n+1})$.

Induction step: Suppose $n \in \mathbb{N}$ and $(a + b) \mid (a^{2n+1} + b^{2n+1})$. Then there is some integer k such that $a^{2n+1} + b^{2n+1} = k(a + b)$. Therefore

$$\begin{aligned} a^{2(n+1)+1} + b^{2(n+1)+1} &= a^{2n+3} + a^2b^{2n+1} - a^2b^{2n+1} + b^{2n+3} \\ &= a^2(a^{2n+1} + b^{2n+1}) - b^{2n+1}(a^2 - b^2) \\ &= a^2(k(a + b)) - b^{2n+1}(a - b)(a + b) = [a^2k - b^{2n+1}(a - b)](a + b), \end{aligned}$$

so $(a + b) \mid (a^{2(n+1)+1} + b^{2(n+1)+1})$.

15. Base case: When $n = 10$, $2^n = 1024 > 1000 = n^3$.

Induction step: Suppose $n \geq 10$ and $2^n > n^3$. Then

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \\ &> 2n^3 && \text{(inductive hypothesis)} \\ &= n^3 + n^3 \\ &\geq n^3 + 10n^2 && \text{(since } n \geq 10\text{)} \\ &= n^3 + 3n^2 + 7n^2 \\ &\geq n^3 + 3n^2 + 70n && \text{(since } n \geq 10\text{)} \\ &= n^3 + 3n^2 + 3n + 67n \\ &> n^3 + 3n^2 + 3n + 1 = (n + 1)^3. \end{aligned}$$

16. (a) Base case: $0 = 2 \cdot 0$, so 0 is even. If 0 is also odd, then there is some integer j such that $0 = 2j + 1$. But then $j = -1/2$, which is not an integer, so we have a contradiction. Therefore 0 is not odd.

Induction step: Suppose $n \in \mathbb{N}$ and n is either even or odd, but not both.

Case 1. n is even and not odd. Then there is some integer k such that $n = 2k$. Then $n + 1 = 2k + 1$, so $n + 1$ is odd. If $n + 1$ is also even, then there is some integer j such that $n + 1 = 2j$. But then $n = 2j - 1 = 2(j - 1) + 1$, so n is odd, which is a contradiction. Therefore $n + 1$ is not even.

Case 2. n is odd and not even. Then there is some integer k such that $n = 2k + 1$. Then $n + 1 = 2k + 2 = 2(k + 1)$, so $n + 1$ is even. If $n + 1$ is also odd, then there is some integer j such that $n + 1 = 2j + 1$. But then $n = 2j$, so n is even, which is a contradiction. Therefore $n + 1$ is not odd.

(b) Let n be an arbitrary integer. If $n \geq 0$, then n is either even or odd, but not both, by part (a). Now suppose $n < 0$. Then $-n$ is a positive integer, so by part (a) $-n$ is either even or odd, but not both.

Case 1. $-n$ is even and not odd. Then for some integer k, $-n = 2k$. Then $n = 2(-k)$, so n is even. If n is also odd, then there is some integer j such that $n = 2j + 1$. But then $-n = -2j - 1 = 2(-j - 1) + 1$, so $-n$ is odd, which is a contradiction. Therefore n is not odd.

Case 2. $-n$ is odd and not even. Then for some integer k, $-n = 2k + 1$. Then $n = -2k - 1 = 2(-k - 1) + 1$, so n is odd. If n is also even, then there is some integer j such that $n = 2j$. But then $-n = 2(-j)$, so $-n$ is even, which is a contradiction. Therefore n is not even.

17. Base case: When $n = 1$, both sides of the equation are equal to 4.

Inductions step: Suppose $n \geq 1$ and $2 \cdot 2^1 + 3 \cdot 2^2 + \cdots + (n+1)2^n = n2^{n+1}$. Then

$$\begin{aligned} 2 \cdot 2^1 + 3 \cdot 2^2 + \cdots + (n+2)2^{n+1} &= (2 \cdot 2^1 + 3 \cdot 2^2 + \cdots + (n+1)2^n) + (n+2)2^{n+1} \\ &= n2^{n+1} + (n+2)2^{n+1} = (2n+2)2^{n+1} \\ &= 2(n+1)2^{n+1} = (n+1)2^{n+2}. \end{aligned}$$

18. (a) The proof doesn't check the base case. In fact, when $n = 0$, the left side of the equation is 1 and the right side is 0, so the equation is false.

(b) For all $n \in \mathbb{N}$, $1 \cdot 3^0 + 3 \cdot 3^1 + 5 \cdot 3^2 + \cdots + (2n+1)3^n = n3^{n+1} + 1$. The proof is by mathematical induction.

Base case: When $n = 0$, both sides of the equation are 1.

Induction step: Suppose $n \in \mathbb{N}$ and $1 \cdot 3^0 + 3 \cdot 3^1 + 5 \cdot 3^2 + \cdots + (2n+1)3^n = n3^{n+1} + 1$. Then

$$\begin{aligned} 1 \cdot 3^0 + 3 \cdot 3^1 + 5 \cdot 3^2 + \cdots + (2(n+1)+1)3^{n+1} & \\ &= (1 \cdot 3^0 + 3 \cdot 3^1 + 5 \cdot 3^2 + \cdots + (2n+1)3^n) + (2n+3)3^{n+1} \\ &= n3^{n+1} + 1 + (2n+3)3^{n+1} = (3n+3)3^{n+1} + 1 \\ &= 3(n+1)3^{n+1} + 1 = (n+1)3^{n+2} + 1. \end{aligned}$$

19. Base case: $n = 0$. Then n is even and $a^n = a^0 = 1 > 0$.

Induction step: Suppose $n \in \mathbb{N}$, if n is even then $a^n > 0$, and if n is odd then $a^n < 0$. We must prove two statements: if $n + 1$ is even then $a^{n+1} > 0$, and if $n + 1$ is odd then $a^{n+1} < 0$.

To prove the first statement, suppose that $n + 1$ is even. Then as in exercise 16, n is odd, so by inductive hypothesis, $a^n < 0$. Multiplying both sides of this inequality by a (and reversing the inequality, since $a < 0$), we get $a^{n+1} > 0$.

The proof of the second statement is similar: Suppose $n+1$ is odd. Then n is even, so by inductive hypothesis, $a^n > 0$. Multiplying by a, we get $a^{n+1} < 0$.

20. (a) Base case: When $n = 1$, the statement to be proven is $0 < a < b$, which was given.

Induction step: Suppose that $n \geq 1$ and $0 < a^n < b^n$. Multiplying this inequality by the positive number a we get $0 < a^{n+1} < ab^n$, and multiplying the inequality $a < b$ by the positive number b^n gives us $ab^n < b^{n+1}$. Combining these inequalities, we can conclude that $0 < a^{n+1} < b^{n+1}$.

(b) Let $n \geq 2$ be arbitrary. Suppose it is not true that $0 < \sqrt[n]{a} < \sqrt[n]{b}$. Since $\sqrt[n]{a}$ and $\sqrt[n]{b}$ are both positive, this means that $0 < \sqrt[n]{b} \leq \sqrt[n]{a}$.

Case 1. $\sqrt[n]{b} = \sqrt[n]{a}$. Raising both sides of this equation to the power n, we get $b = a$, which contradicts the fact that $a < b$.

Case 2. $0 < \sqrt[n]{b} < \sqrt[n]{a}$. Applying part (a), we get $b = (\sqrt[n]{b})^n < (\sqrt[n]{a})^n = a$, which contradicts the fact that $a < b$.

Since we have reached a contradiction in both cases, we conclude that $0 < \sqrt[n]{a} < \sqrt[n]{b}$.

(c) Suppose $n \geq 1$. We are given that $a < b$, and by part (a), $a^n < b^n$. Therefore $b - a > 0$ and $b^n - a^n > 0$, so $(b-a)(b^n - a^n) > 0$. Multiplying this out gives us $b^{n+1} - ba^n - ab^n + a^{n+1} > 0$. Rearranging this, we get the required inequality $ab^n + ba^n < a^{n+1} + b^{n+1}$.

(d) Base case: $n = 2$. By part (c) with $n = 1$, $2ab < a^2 + b^2$. Adding $a^2 + b^2$ to both sides, we get $a^2 + 2ab + b^2 < 2a^2 + 2b^2$, or equivalently $(a+b)^2 < 2(a^2 + b^2)$. Dividing by 4, we get $(a+b)^2/4 < (a^2+b^2)/2$, or equivalently $((a+b)/2)^2 < (a^2+b^2)/2$. This is the required inequality with $n = 2$.

Induction step: Suppose $n \geq 2$ and $((a+b)/2)^n < (a^n + b^n)/2$. Then

$$\begin{aligned}
\left(\frac{a+b}{2}\right)^{n+1} = \left(\frac{a+b}{2}\right)\left(\frac{a+b}{2}\right)^n &< \left(\frac{a+b}{2}\right)\left(\frac{a^n+b^n}{2}\right) && \text{(inductive hypothesis)} \\
&= \frac{a^{n+1} + ab^n + ba^n + b^{n+1}}{4} \\
&< \frac{2a^{n+1} + 2b^{n+1}}{4} && \text{(part (c))} \\
&= \frac{a^{n+1} + b^{n+1}}{2}.
\end{aligned}$$

Section 6.2

1. (a) We must prove that R' is reflexive (on A'), transitive, and antisymmetric. For the first, suppose $x \in A'$. Since R is reflexive (on A) and $x \in A$, $(x, x) \in R$, so $(x, x) \in R \cap (A' \times A') = R'$. This shows that R' is reflexive.

   Next, suppose that $(x, y) \in R'$ and $(y, z) \in R'$. Then $(x, y) \in R$, $(y, z) \in R$, and $x, y, z \in A'$. Since R is transitive, $(x, z) \in R$, so $(x, z) \in R \cap (A' \times A') = R'$. Therefore R' is transitive.

   Finally, suppose that $(x, y) \in R'$ and $(y, x) \in R'$. Then $(x, y) \in R$ and $(y, x) \in R$, so since R is antisymmetric, $x = y$. Thus R' is antisymmetric.

   (b) To see that T is reflexive, suppose $x \in A$. If $x = a$, then $(x, x) = (a, a) \in \{a\} \times A \subseteq T$. If $x \neq a$, then $x \in A'$, so since R' is reflexive, $(x, x) \in R' \subseteq T' \subseteq T$.

   For transitivity, suppose that $(x, y) \in T$ and $(y, z) \in T$. If $x = a$ then $(x, z) = (a, z) \in \{a\} \times A \subseteq T$. Now suppose $x \neq a$. Then $(x, y) \notin \{a\} \times A$, so since $(x, y) \in T = T' \cup (\{a\} \times A)$ we must have $(x, y) \in T'$. But $T' \subseteq A' \times A'$, so $y \in A'$ and therefore $y \neq a$. Similar reasoning now shows that $(y, z) \in T'$. Since T' is transitive, it follows that $(x, z) \in T' \subseteq T$.

   To show that T is antisymmetric, suppose $(x, y) \in T$ and $(y, x) \in T$. If $x = a$ then $(y, x) \notin T'$, so $(y, x) \in \{a\} \times A$ and therefore $y = a = x$. Similarly, if $y = a$ then $x = y$. Now suppose $x \neq a$ and $y \neq a$. Then as in the proof of transitivity it follows that $(x, y) \in T'$ and $(y, x) \in T'$, so by antisymmetry of T', $x = y$.

   We now know that T is a partial order. To see that it is total, suppose $x \in A$ and $y \in A$. If $x = a$ then $(x, y) \in \{a\} \times A \subseteq T$. Similarly, if $y = a$ then $(y, x) \in T$. Now suppose $x \neq a$ and $y \neq a$. Then $x \in A'$ and $y \in A'$, so since T' is a total order, either $(x, y) \in T' \subseteq T$ or $(y, x) \in T' \subseteq T$.

   Finally, to see that $R \subseteq T$, suppose that $(x, y) \in R$. If $x = a$ then $(x, y) \in \{a\} \times A \subseteq T$. Now suppose $x \neq a$. If $y = a$ then the fact that $(x, y) \in R$ would contradict the R-minimality of a. Therefore $y \neq a$. But then $(x, y) \in R \cap (A' \times A') = R' \subseteq T' \subseteq T$.

2. Suppose R is a partial order on a set A. We now use induction to prove that $\forall n \in \mathbb{N} \forall B \subseteq A[B \text{ has } n \text{ elements} \rightarrow \exists T(T \text{ is a partial order on } A \wedge R \subseteq T \wedge \forall x \in B \forall y \in A(xTy \vee yTx))]$.

   Base case: $n = 0$. If $B \subseteq A$ and B has 0 elements then $B = \varnothing$. We can let $T = R$, and the statement $\forall x \in B \forall y \in A(xTy \vee yTx)$ will be true vacuously.

Induction step: Suppose $n \in \mathbb{N}$ and $\forall B \subseteq A[B$ has n elements $\rightarrow \exists T(T$ is a partial order on $A \wedge R \subseteq T \wedge \forall x \in B \forall y \in A(xTy \vee yTx))]$. Suppose $B \subseteq A$ and B has $n+1$ elements. Let b be any element of B and let $B' = B \setminus \{b\}$, a subset of A with n elements. By inductive hypothesis, we can let T' be a partial order on A such that $R \subseteq T'$ and $\forall x \in B' \forall y \in A(xT'y \vee yT'x)$. Let $A_1 = \{x \in A \mid (x, b) \in T'\}$ and $A_2 = A \setminus A_1$. Let $T = T' \cup (A_1 \times A_2)$.

To see that T is reflexive, suppose $x \in A$. Since T' is a partial order on A, $(x, x) \in T'$, so $(x, x) \in T$. Thus T is reflexive. Next, to prove that T is transitive, suppose $(x, y) \in T$ and $(y, z) \in T$. Then $(x, y) \in T' \cup (A_1 \times A_2)$, so either $(x, y) \in T'$ or $(x, y) \in A_1 \times A_2$, and similarly either $(y, z) \in T'$ or $(y, z) \in A_1 \times A_2$. We now consider three cases.

Case 1. $(x, y) \in T'$ and $(y, z) \in T'$. Then since T' is transitive, $(x, z) \in T' \subseteq T$.

Case 2. $(x, y) \in T'$ and $(y, z) \in A_1 \times A_2$. Then $y \in A_1$ and $z \in A_2$. Since $y \in A_1$, by the definition of A_1, $(y, b) \in T'$. Since $(x, y) \in T'$, $(y, b) \in T'$, and T' is transitive, $(x, b) \in T'$, so $x \in A_1$. Since $x \in A_1$ and $z \in A_2$, $(x, z) \in A_1 \times A_2 \subseteq T$.

Case 3. $(x, y) \in A_1 \times A_2$. Then $x \in A_1$ and $y \in A_2$. Since $y \in A_2$, $y \notin A_1$, so $(y, z) \notin A_1 \times A_2$, and therefore $(y, z) \in T'$. Suppose $z \in A_1$. Then by definition of A_1, $(z, b) \in T'$, so since $(y, z) \in T'$, by transitivity of T', $(y, b) \in T'$. But then $y \in A_1$, which is a contradiction. Therefore $z \notin A_1$, so $z \in A_2$. Since $x \in A_1$ and $z \in A_2$, $(x, z) \in A_1 \times A_2 \subseteq T$.

In call cases we have $(x, z) \in T$, so this proves that T is transitive.

To prove that T is antisymmetric, suppose $(x, y) \in T$ and $(y, x) \in T$. As before, either $(x, y) \in T'$ or $(x, y) \in A_1 \times A_2$, and either $(y, x) \in T'$ or $(y, x) \in A_1 \times A_2$. Suppose $(x, y) \in A_1 \times A_2$. Then $x \in A_1$ and $y \in A_2$. Thus $(y, x) \notin A_1 \times A_2$, so $(y, x) \in T'$. Since $x \in A_1$, $(x, b) \in T'$. Since $(y, x) \in T'$, $(x, b) \in T'$, and T' is transitive, $(y, b) \in T'$. But this means $y \in A_1$, which is a contradiction. Therefore it cannot be the case that $(x, y) \in A_1 \times A_2$, so $(x, y) \in T'$. Similar reasoning shows that we can rule out $(y, x) \in A_1 \times A_2$, so $(y, x) \in T'$. Since $(x, y) \in T'$, $(y, x) \in T'$, and T' is antisymmetric, $y = x$. Thus T is antisymmetric.

We have now shown that T is a partial order on A. Since $R \subseteq T'$ and $T' \subseteq T$, $R \subseteq T$. Finally, let $x \in B$ and $y \in A$ be arbitrary. Once again we consider cases.

Case 1. $x \in B'$. Then by the choice of T', either $xT'y$ or $yT'x$. Since $T' \subseteq T$, it follows that either xTy or yTx.

Case 2. $x \notin B'$. Then $x = b$. We now consider two subcases.

Case 2a. $y \in A_1$. Then $(y, x) = (y, b) \in T' \subseteq T$, so yTx.

Case 2b. $y \notin A_1$, so $y \in A_2$. Notice that $(b, b) \in T'$, so $b \in A_1$. Therefore $(x, y) = (b, y) \in A_1 \times A_2 \subseteq T$, so xTy.

Thus either xTy or yTx, as required.

3. We will prove by induction that $\forall n \geq 1 \forall B \subseteq A[B$ has n elements $\rightarrow B$ has an R-smallest element and an R-largest element].

Base case: $n = 1$. Suppose $B \subseteq A$ and B has 1 element. Then $B = \{b\}$, for some $b \in A$. Since b is the only element of B and R is reflexive, $\forall x \in B(bRx)$ and $\forall x \in B(xRb)$, so b is both the R-smallest element of B and the R-largest element of B.

Induction step. Suppose $n \geq 1$ and $\forall B \subseteq A[B$ has n elements $\rightarrow B$ has an R-smallest element and an R-largest element]. Now suppose $B \subseteq A$ and B has $n+1$ elements. Let b be any element of B, and let $B' = B \setminus \{b\}$. Then B' has n elements, so by inductive hypothesis we can let c be the R-smallest element of B' and d the R-largest element of B'.

Since R is a total order, either bRc or cRb.

Case 1. bRc. Let x be an arbitrary element of B. If $x = b$, then since R is reflexive, bRx. If $x \neq b$, then $x \in B'$, so since c is the R-smallest element of B', cRx. By transitivity of R, since bRc and cRx, bRx. Thus $\forall x \in B(bRx)$, so b is the R-smallest element of B.

Case 2. cRb. Let x be an arbitrary element of B. If $x = b$, then since cRb, cRx. If $x \neq b$, then $x \in B'$, so since c is the R-smallest element of B', cRx. Thus $\forall x \in B(cRx)$, so c is the R-smallest

element of B.

Thus, B has an R-smallest element. A similar argument shows that either b or d is the R-largest element of B.

4. (a) We will prove the statement: $\forall n \geq 1 \forall B \subseteq A[B \text{ has } n \text{ elements} \rightarrow \exists x \in B \forall y \in B((x,y) \in R \circ R)]$. We proceed by induction on n.

Base case: Suppose $n = 1$. If $B \subseteq A$ and B has one element, then for some $x \in B$, $B = \{x\}$. Since R is reflexive, $(x,x) \in R$, and therefore $(x,x) \in R \circ R$. But x is the only element in B, so $\forall y \in B((x,y) \in R \circ R)$, as required.

Induction step: Suppose that $n \geq 1$ and for every $B \subseteq A$, if B has n elements then $\exists x \in B \forall y \in B((x,y) \in R \circ R)$. Now suppose that $B \subseteq A$ and B has $n+1$ elements. Choose some $b \in B$, and let $B' = B \setminus \{b\}$. Then $B' \subseteq A$ and B' has n elements, so by inductive hypothesis there is some $x \in B'$ such that $\forall y \in B'((x,y) \in R \circ R)$. We now consider two cases.

Case 1: $(x,b) \in R \circ R$. Then $\forall y \in B((x,y) \in R \circ R)$, so we are done.

Case 2: $(x,b) \notin R \circ R$. In this case, we will prove that $\forall y \in B((b,y) \in R \circ R)$. To do this, let $y \in B$ be arbitrary. If $y = b$, then since R is reflexive, $(b,b) \in R$, and therefore $(b,y) = (b,b) \in R \circ R$. Now suppose $y \neq b$. Then $y \in B'$, so by the choice of x we know that $(x,y) \in R \circ R$. This means that for some $z \in A$, $(x,z) \in R$ and $(z,y) \in R$. We have $(x,z) \in R$, so if $(z,b) \in R$ then $(x,b) \in R \circ R$, contrary to the assumption for this case. Therefore $(z,b) \notin R$, so by the hypothesis on R, $(b,z) \in R$. But then since $(b,z) \in R$ and $(z,y) \in R$, we have $(b,y) \in R \circ R$, as required.

(b) Let $A =$ the set of contestants and let $R = \{(x,y) \in A \times A \mid x \text{ beats } y\} \cup i_A$. By assumption, for all x and y in A, if $x \neq y$ then either x beats y or y beats x, so $xRy \vee yRx$. But also if $x = y$ then $(x,y) \in i_A \subseteq R$, so xRy. Thus R satisfies the hypothesis in part (a). We now apply part (a) with $B = A$ to conclude that there is some $x \in A$ such that for all $y \in A$, $(x,y) \in R \circ R$. We claim that x is excellent. To prove this, suppose $y \in A$ and $y \neq x$. Then $(x,y) \in R \circ R$, so there is some $z \in A$ such that $(x,z) \in R$ and $(z,y) \in R$. If $z = x$ then since $(z,y) \in R$, $(x,y) \in R$. But since $x \neq y$, $(x,y) \notin i_A$, so by the definition of A, x beats y. Similarly, if $z = y$ then since $(x,z) \in R$, $(x,y) \in R$, so x beats y. Finally, if $z \neq x$ and $z \neq y$ then x beats z and z beats y. This proves that x is excellent.

5. Base case: $n = 1$. $F_0 = 2^{(2^0)} + 1 = 3$ and $F_1 = 2^{(2^1)} + 1 = 5$, so $F_1 = F_0 + 2$.

Induction step: Suppose $n \geq 1$ and $F_n = (F_0 \cdot F_1 \cdot F_2 \cdots F_{n-1}) + 2$. Then

$$\begin{aligned}(F_0 \cdot F_1 \cdot F_2 \cdots F_n) + 2 &= ((F_0 \cdot F_1 \cdot F_2 \cdots F_{n-1}) \cdot F_n) + 2 \\ &= (F_n - 2) \cdot F_n + 2 = \left(2^{(2^n)} - 1\right)\left(2^{(2^n)} + 1\right) + 2 \\ &= \left(2^{(2^n)}\right)^2 - 1 + 2 = 2^{(2^n \cdot 2)} + 1 \\ &= 2^{(2^{n+1})} + 1 = F_{n+1}.\end{aligned}$$

6. Base case: If $n = 1$, then the statement to be proven is that for every real number a_1, $|a_1| \leq |a_1|$, which is clearly true.

Induction step. Suppose $n \geq 1$ and for all real numbers $a_1, a_2, \ldots, a_n$, $|a_1 + a_2 + \cdots + a_n| \leq |a_1| + |a_2| + \cdots + |a_n|$. Now suppose $a_1, a_2, \ldots, a_{n+1}$ are real numbers. Then

$$\begin{aligned}|a_1 + a_2 + \cdots + a_{n+1}| &= |(a_1 + a_2 + \cdots + a_n) + a_{n+1}| \\ &\leq |a_1 + a_2 + \cdots + a_n| + |a_{n+1}| \quad \text{(triangle inequality: ex. 13(c) in Sect. 3.5)} \\ &\leq |a_1| + |a_2| + \cdots + |a_n| + |a_{n+1}| \quad \text{(inductive hypothesis).}\end{aligned}$$

7. (a) Suppose a and b are positive real numbers. Then $a^2 - 2ab + b^2 = (a-b)^2 \geq 0$. Adding $2ab$ to both sides gives us $a^2 + b^2 \geq 2ab$, and then dividing by ab, which is positive, we get $a/b + b/a \geq 2$.

(b) Since $a \le b \le c$, $c - a \ge 0$ and $c - b \ge 0$, so $c^2 - bc - ac + ab = (c-a)(c-b) \ge 0$. Adding ac to both sides gives us $ab + c^2 - bc \ge ac$, and dividing by ac, we get $b/c + c/a - b/a \ge 1$.

(c) We use induction.

Base case: If $n = 2$, the statement to be proven is that if $0 < a_1 \le a_2$ then $a_1/a_2 + a_2/a_1 \ge 2$. This follows from part (a).

Induction step. Suppose $n \ge 2$ and for all numbers $a_1, a_2, \ldots, a_n$, if $0 < a_1 \le a_2 \le \cdots \le a_n$ then $a_1/a_2 + a_2/a_3 + \cdots + a_{n-1}/a_n + a_n/a_1 \ge n$. Now suppose $a_1, a_2, \ldots, a_{n+1}$ are real numbers and $0 < a_1 \le a_2 \le \cdots \le a_{n+1}$. Then

$$\begin{aligned}\frac{a_1}{a_2} + \frac{a_2}{a_3} + \cdots + \frac{a_n}{a_{n+1}} + \frac{a_{n+1}}{a_1} &= \left(\frac{a_1}{a_2} + \frac{a_2}{a_3} + \cdots + \frac{a_{n-1}}{a_n} + \frac{a_n}{a_1}\right) + \left(\frac{a_n}{a_{n+1}} + \frac{a_{n+1}}{a_1} - \frac{a_n}{a_1}\right) \\ &\ge n + \left(\frac{a_n}{a_{n+1}} + \frac{a_{n+1}}{a_1} - \frac{a_n}{a_1}\right) \qquad \text{(inductive hypothesis)} \\ &\ge n + 1 \qquad \text{(part (b)).}\end{aligned}$$

8. (a) Let $m = (a+b)/2$, the arithmetic mean of a and b, and let $d = (a-b)/2$. Then it is easy to check that $m + d = a$ and $m - d = b$, so

$$\sqrt{ab} = \sqrt{(m+d)(m-d)} = \sqrt{m^2 - d^2} \le \sqrt{m^2} = m = \frac{a+b}{2}.$$

(b) We use induction on n.

Base case: $n = 1$. This case is taken care of by part (a).

Induction step: Suppose $n \ge 1$, and the arithmetic mean–geometric mean inequality holds for lists of length 2^n. Now let $a_1, a_2, \ldots, a_{2^{n+1}}$ be a list of 2^{n+1} positive real numbers. Let

$$m_1 = \frac{a_1 + a_2 + \cdots + a_{2^n}}{2^n}, \quad m_2 = \frac{a_{2^n+1} + a_{2^n+2} + \cdots + a_{2^{n+1}}}{2^n}.$$

Notice that $a_1 + a_2 + \cdots + a_{2^n} = m_1 2^n$, and similarly $a_{2^n+1} + a_{2^n+2} + \cdots + a_{2^{n+1}} = m_2 2^n$. Also, by inductive hypothesis, we know that $m_1 \ge \sqrt[2^n]{a_1 a_2 \cdots a_{2^n}}$ and $m_2 \ge \sqrt[2^n]{a_{2^n+1} a_{2^n+2} \cdots a_{2^{n+1}}}$. Therefore

$$\begin{aligned}\frac{a_1 + a_2 + \cdots + a_{2^{n+1}}}{2^{n+1}} &= \frac{m_1 2^n + m_2 2^n}{2^{n+1}} = \frac{m_1 + m_2}{2} \ge \sqrt{m_1 m_2} \\ &\ge \sqrt{\sqrt[2^n]{a_1 a_2 \cdots a_{2^n}}\ \sqrt[2^n]{a_{2^n+1} a_{2^n+2} \cdots a_{2^{n+1}}}} \\ &= \sqrt[2^{n+1}]{a_1 a_2 \cdots a_{2^{n+1}}}.\end{aligned}$$

(c) We use induction on n.

Base case: If $n = n_0$, then by assumption the arithmetic mean–geometric mean inequality fails for some list of length n.

Induction step: Suppose $n \ge n_0$, and there are positive real numbers $a_1, a_2, \ldots, a_n$ such that

$$\frac{a_1 + a_2 + \cdots + a_n}{n} < \sqrt[n]{a_1 a_2 \cdots a_n}.$$

Let $m = (a_1 + a_2 + \cdots + a_n)/n$, and let $a_{n+1} = m$. Then we have $m < \sqrt[n]{a_1 a_2 \cdots a_n}$, so $m^n < a_1 a_2 \cdots a_n$. Multiplying both sides of this inequality by m gives us $m^{n+1} < a_1 a_2 \cdots a_n m = a_1 a_2 \cdots a_{n+1}$, so $m < \sqrt[n+1]{a_1 a_2 \cdots a_{n+1}}$. But notice that we also have $mn = a_1 + a_2 + \cdots + a_n$, so

$$\frac{a_1 + \cdots + a_{n+1}}{n+1} = \frac{mn + m}{n+1} = \frac{m(n+1)}{n+1} = m < \sqrt[n+1]{a_1 a_2 \cdots a_{n+1}}.$$

Thus, we have a list of length $n+1$ for which the arithmetic mean–geometric mean inequality fails.

(d) Suppose that the arithmetic mean–geometric mean inequality fails for some list of positive real numbers. Let n_0 be the length of this list, and choose an integer $n \geq 1$ such that $n_0 \leq 2^n$. (In fact, we could just let $n = n_0$, as you will show in exercise 12(a) in Section 6.3.) Then by part (b), the arithmetic mean–geometric mean inequality holds for all lists of length 2^n, but by part (c), it must fail for some list of length 2^n. This is a contradiction, so the inequality must always hold.

9. Suppose $n \geq 2$ and $a_1, a_2, \ldots, a_n$ is a list of positive real numbers. By the arithmetic mean–geometric mean inequality (exercise 8) applied to the numbers $1/a_1, 1/a_2, \ldots, 1/a_n$, we have

$$\frac{\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}}{n} \geq \sqrt[n]{\frac{1}{a_1} \cdot \frac{1}{a_2} \cdots \frac{1}{a_n}} = \frac{1}{\sqrt[n]{a_1 a_2 \cdots a_n}} > 0.$$

By exercise 6 in Section 3.1,

$$\frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}} \leq \sqrt[n]{a_1 a_2 \cdots a_n}.$$

10. (a) Suppose a_1, a_2, b_1, and b_2 are real numbers, $a_1 \leq a_2$, and $b_1 \leq b_2$. Then $(a_1 b_1 + a_2 b_2) - (a_1 b_2 + a_2 b_1) = (a_2 - a_1)(b_2 - b_1) \geq 0$. Therefore $a_1 b_2 + a_2 b_1 \leq a_1 b_1 + a_2 b_2$.

(b) We use induction on n.

Base case: $n = 1$. Suppose a_1 and b_1 are real numbers and f is a one-to-one, onto function from $\{1\}$ to $\{1\}$. Then $f(1) = 1$, so $a_1 b_{f(1)} = a_1 b_1$.

Induction step. Suppose $n \geq 1$ and the result holds for sequences of real numbers of length n. Now suppose $a_1, a_2, \ldots, a_{n+1}$ and $b_1, b_2, \ldots, b_{n+1}$ are real numbers, $a_1 \leq a_2 \leq \cdots \leq a_{n+1}$, $b_1 \leq b_2 \leq \cdots \leq b_{n+1}$, and f is a one-to-one onto function from $\{1, 2, \ldots, n+1\}$ to $\{1, 2, \ldots, n+1\}$. We consider two cases.

Case 1. $f(n+1) = n+1$. Let $f' = f \setminus \{(n+1, n+1)\}$. Then f' is a one-to-one, onto function from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$. (In the language of exercise 7 in Section 5.1, f' is the restriction of f to $\{1, 2, \ldots, n\}$.) Therefore, by the inductive hypothesis,

$$\begin{aligned} a_1 b_{f(1)} + a_2 b_{f(2)} + \cdots + a_{n+1} b_{f(n+1)} &= (a_1 b_{f'(1)} + a_2 b_{f'(2)} + \cdots + a_n b_{f'(n)}) + a_{n+1} b_{n+1} \\ &\leq a_1 b_1 + a_2 b_2 + \cdots + a_n b_n + a_{n+1} b_{n+1}. \end{aligned}$$

Case 2. $f(n+1) \neq n+1$. Let $k = f(n+1) \leq n$. Since f is onto, there is some $j \leq n$ such that $f(j) = n+1$. Now define $g : \{1, 2, \ldots, n+1\}$ to $\{1, 2, \ldots, n+1\}$ as follows:

$$g(x) = \begin{cases} k, & \text{if } x = j, \\ n+1, & \text{if } x = n+1, \\ f(x), & \text{otherwise.} \end{cases}$$

In other words, g is the same as f, except that $g(j) = k$ and $g(n+1) = n+1$. Notice that g is also a one-to-one, onto function from $\{1, 2, \ldots, n+1\}$ to itself, and since $g(n+1) = n+1$, the reasoning in case 1 applies to g. Therefore, by case 1,

$$a_1 b_{g(1)} + a_2 b_{g(2)} + \cdots + a_{n+1} b_{g(n+1)} \leq a_1 b_1 + a_2 b_2 + \cdots a_{n+1} b_{n+1}. \qquad (*)$$

Also, $a_j \leq a_{n+1}$ and $b_k \leq b_{n+1}$, so by part (a),

$$a_j b_{f(j)} + a_{n+1} b_{f(n+1)} = a_j b_{n+1} + a_{n+1} b_k \leq a_j b_k + a_{n+1} b_{n+1} = a_j b_{g(j)} + a_{n+1} b_{g(n+1)},$$

and therefore

$$(a_j b_{f(j)} + a_{n+1} b_{f(n+1)}) - (a_j b_{g(j)} + a_{n+1} b_{g(n+1)}) \leq 0. \qquad (**)$$

Adding inequalities $(*)$ and $(**)$, we get the desired inequality,

$$a_1 b_{f(1)} + a_2 b_{f(2)} + \cdots + a_{n+1} b_{f(n+1)} \leq a_1 b_1 + a_2 b_2 + \cdots a_{n+1} b_{n+1}.$$

11. We proceed by induction on n.

Base case: $n = 0$. If A has 0 elements, then $A = \varnothing$, so $\mathscr{P}(A) = \{\varnothing\}$, which has $1 = 2^0$ elements.

Induction step: Suppose that for every set A with n elements, $\mathscr{P}(A)$ has 2^n elements. Now suppose that A has $n+1$ elements. Let a be any element of A, and let $A' = A \setminus \{a\}$. Then A' has n elements, so by inductive hypothesis $\mathscr{P}(A')$ has 2^n elements. There are two kinds of subsets of A: those that contain a as an element, and those that don't. The subsets that don't contain a are just the subsets of A', and there are 2^n of these. Those that do contain a are the sets of the form $X \cup \{a\}$, where $X \in \mathscr{P}(A')$, and there are also 2^n of these, since there are 2^n possible choices for X. Thus the total number of elements of $\mathscr{P}(A)$ is $2^n + 2^n = 2^{n+1}$.

12. We proceed by induction on n.

Base case: $n = 0$. If A has 0 elements, then $A = \varnothing$, so $\mathscr{P}_2(A) = \varnothing$, which has 0 elements, and $n(n-1)/2 = 0$.

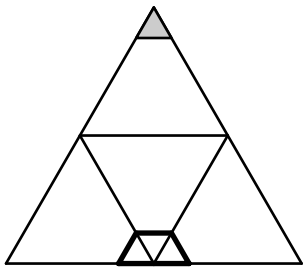
Induction step: Suppose $n \in \mathbb{N}$, and for every set A, if A has n elements then $\mathscr{P}_2(A)$ as $n(n-1)/2$ elements. Now suppose A is a set with $n+1$ elements. Let a be some element of A, and let $A' = A \setminus \{a\}$. Then A' has n elements, so by inductive hypothesis $\mathscr{P}_2(A')$ has $n(n-1)/2$ elements. There are two kinds of two-element subsets of A: those that contain a as an element, and those that don't. The subsets that don't contain a are just the two-element subsets of A', and there are $n(n-1)/2$ of these. Those that do contain a are the sets of the form $\{a, x\}$, where $x \in A'$, and there are n of these, since there are n possibilities for x. Thus the total number of elements of $\mathscr{P}_2(A)$ is

$$\frac{n(n-1)}{2} + n = \frac{n^2+n}{2} = \frac{(n+1)n}{2}.$$

13. We use induction on n.

Base case: Suppose $n = 1$. Then the triangle is cut into 4 congruent equilateral triangles and one corner is removed. The remaining three triangles can be covered by one trapezoidal tile.

Induction step: Suppose n is a positive integer, and an equilateral triangle cut into a grid of 4^n congruent equilateral triangles, with one corner removed, can be covered with trapezoidal tiles. Now consider an equilateral triangle cut into a grid of 4^{n+1} congruent equilateral triangles, with one corner removed. The division lines include line segments connecting the centers of the sides of the triangle. These segments divide the triangle into four triangular subgrids, each of which is divided into 4^n triangles. The corner that has been removed comes from one of these four subgrids. Place one trapezoidal tile at the point where the other three triangular subgrids meet, so that it covers one corner of each of these subgrids, as shown in the figure below. The area remaining to be covered now contains every triangle except for one corner in each of the triangular subgrids, so by applying the inductive hypothesis to each subgrid we see that this area can be covered with tiles.



14. Base case: $n = 1$. One chord cuts the circle into two regions, and $(n^2+n+2)/2 = 2$.

Induction step: Suppose that when n chords are drawn, the circle is cut into $(n^2+n+2)/2$ regions. When another chord is drawn, it will intersect each of the first n chords exactly once. Therefore it will pass through $n+1$ regions, cutting each of those regions in two. (Each time it crosses one of the first n chords, it passes from one region to another.) Therefore the number of regions after the next chord

is drawn is

$$\frac{n^2+n+2}{2}+(n+1)=\frac{n^2+3n+4}{2}=\frac{(n+1)^2+(n+1)+2}{2},$$

as required.

15. Base case: When $n=1$, there is one chord, cutting the circle into two regions. Color one region white and the other black.

    Induction step: Suppose that the regions created by n chords can be colored as required, and consider a circle with $n+1$ chords. Remove one chord and apply the inductive hypothesis to color the regions as required. Then add in the chord that was removed and reverse the colors of all regions on one side of that chord.

16. We use induction to prove that for every $n \in \mathbb{N}$, if A is a set with n elements, $f : A \to A$, and f is one-to-one, then f is onto.

    Base case: $n = 0$. If A has 0 elements and $f : A \to A$, then $A = \varnothing$, $f = \varnothing$, and f is both one-to-one and onto (vacuously).

    Induction step: Suppose $n \in \mathbb{N}$ and for every set A with n elements and every function $f : A \to A$, if f is one-to-one then f is onto. Now suppose A has $n+1$ elements, $f : A \to A$, and f is one-to-one but not onto. Since f is not onto, there is some $a \in A$ such that $a \notin \text{Ran}(f)$. Let $A' = A \setminus \{a\}$ and $f' = f \cap (A' \times A')$. Suppose $x \in A'$. Then $(x, f(x)) \in f$ and since $a \notin \text{Ran}(f)$, $f(x) \neq a$, so $f(x) \in A'$. Therefore $(x, f(x)) \in A' \times A'$, so $(x, f(x)) \in f'$. Now suppose $(x, y_1) \in f'$ and $(x, y_2) \in f'$. Then $(x, y_1) \in f$ and $(x, y_2) \in f$, so since f is a function, $y_1 = y_2$. This proves that $f' : A' \to A'$. Note that for every $x \in A'$, $(x, f'(x)) \in f' \subseteq f$, so $f(x) = f'(x)$. To see that f' is one-to-one, suppose $x_1, x_2 \in A'$ and $f'(x_1) = f'(x_2)$. Then $f(x_1) = f(x_2)$, so since f is one-to-one, $x_1 = x_2$. By inductive hypothesis, f' must map onto A'. Since $a \notin \text{Ran}(f)$, $f(a) \neq a$, so $f(a) \in A'$. Therefore, since f' is onto, there is some $x \in A'$ such that $f'(x) = f(a)$. Since $x \in A'$, $x \neq a$, but $f(x) = f'(x) = f(a)$, which contradicts the fact that f is one-to-one.

17. To establish that every natural number is an element of A, you would have to let n be an arbitrary natural number and then *prove* that $n \in A$; the proof merely assumes that $n \in A$. This assumption applies only to the single (arbitrarily chosen) natural number n; it doesn't apply to all natural numbers.

18. The mistake is the sentence "Now let a_3 be an element of A that is different from both a_1 and a_2." For such an element a_3 to exist, A must have at least three elements. At this point in the proof, we know that A has $n+1$ elements. If $n \geq 2$, then A has at least three elements, and this step is correct. But if $n = 1$ then A has only two elements. So the induction step doesn't work when $n = 1$.

Section 6.3

1. We will prove by induction that for all $n \geq 1$,

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}.$$

Base case: When $n = 1$, both sides of the equation are equal to $1/2$.
Induction step: Suppose $n \geq 1$ and $\sum_{i=1}^{n} 1/(i(i+1)) = n/(n+1)$. Then

$$\begin{aligned}
\sum_{i=1}^{n+1} \frac{1}{i(i+1)} &= \sum_{i=1}^{n} \frac{1}{i(i+1)} + \frac{1}{(n+1)(n+2)} && \text{(definition of summation)} \\
&= \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} && \text{(inductive hypothesis)} \\
&= \frac{n^2+2n+1}{(n+1)(n+2)} = \frac{(n+1)^2}{(n+1)(n+2)} = \frac{n+1}{n+2}.
\end{aligned}$$

2. Base case: When $n = 1$, both sides of the equation are equal to 1/6.
Induction step: Suppose $n \geq 1$ and

$$\sum_{i=1}^{n} \frac{1}{i(i+1)(i+2)} = \frac{n^2+3n}{4(n+1)(n+2)}.$$

Then

$$\begin{aligned}
\sum_{i=1}^{n+1} \frac{1}{i(i+1)(i+2)} &= \sum_{i=1}^{n} \frac{1}{i(i+1)(i+2)} + \frac{1}{(n+1)(n+2)(n+3)} \\
&= \frac{n^2+3n}{4(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} && \text{(inductive hypothesis)} \\
&= \frac{n^3+6n^2+9n+4}{4(n+1)(n+2)(n+3)} = \frac{(n+1)(n^2+5n+4)}{4(n+1)(n+2)(n+3)} \\
&= \frac{(n^2+2n+1)+(3n+3)}{4(n+2)(n+3)} = \frac{(n+1)^2+3(n+1)}{4(n+2)(n+3)}.
\end{aligned}$$

3. Base case: When $n = 2$, both sides of the equation are equal to 1/3.
Induction step: Suppose $n \geq 2$ and

$$\sum_{i=2}^{n} \frac{1}{(i-1)(i+1)} = \frac{3n^2-n-2}{4n(n+1)}.$$

Then

$$\begin{aligned}
\sum_{i=1}^{n+1} \frac{1}{(i-1)(i+1)} &= \sum_{i=1}^{n} \frac{1}{(i-1)(i+1)} + \frac{1}{n(n+2)} \\
&= \frac{3n^2-n-2}{4n(n+1)} + \frac{1}{n(n+2)} && \text{(inductive hypothesis)} \\
&= \frac{3n^3+5n^2-4n-4}{4n(n+1)(n+2)} + \frac{4n+4}{4n(n+1)(n+2)} \\
&= \frac{3n^2+5n}{4(n+1)(n+2)} = \frac{3(n+1)^2-(n+1)-2}{4(n+1)(n+2)}.
\end{aligned}$$

4. Base case: When $n = 0$, both sides of the equation are equal to 1.
Induction step: Suppose $n \in \mathbb{N}$ and

$$\sum_{i=0}^{n} (2i+1)^2 = \frac{(n+1)(2n+1)(2n+3)}{3}.$$

Then

$$\begin{aligned}
\sum_{i=0}^{n+1} (2i+1)^2 &= \sum_{i=0}^{n} (2i+1)^2 + (2n+3)^2 \\
&= \frac{(n+1)(2n+1)(2n+3)}{3} + (2n+3)^2 && \text{(inductive hypothesis)} \\
&= \frac{(2n+3)(2n^2+9n+10)}{3} = \frac{(n+2)(2n+3)(2n+5)}{3}.
\end{aligned}$$

5. Base case: When $n = 0$, both sides of the equation are equal to 1.
Induction step: Suppose $n \in \mathbb{N}$ and

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}.$$

Then

$$\begin{aligned}\sum_{i=0}^{n+1} r^i &= \sum_{i=0}^{n} r^i + r^{n+1} \\ &= \frac{r^{n+1} - 1}{r - 1} + r^{n+1} && \text{(inductive hypothesis)} \\ &= \frac{r^{n+2} - 1}{r - 1}.\end{aligned}$$

6. Base case: $n = 1$. Then

$$\sum_{i=1}^{n} \frac{1}{i^2} = 1 \leq 1 = 2 - \frac{1}{n}.$$

Induction step: Suppose that

$$\sum_{i=1}^{n} \frac{1}{i^2} \leq 2 - \frac{1}{n}.$$

Then

$$\begin{aligned}\sum_{i=1}^{n+1} \frac{1}{i^2} &= \sum_{i=1}^{n} \frac{1}{i^2} + \frac{1}{(n+1)^2} \leq 2 - \frac{1}{n} + \frac{1}{(n+1)^2} \\ &= 2 - \frac{n^2 + n + 1}{n(n+1)^2} < 2 - \frac{n^2 + n}{n(n+1)^2} = 2 - \frac{1}{n+1}.\end{aligned}$$

7. (a) We use induction on n.
Base case: When $n = 0$, the equation says $a_0 + b_0 = a_0 + b_0$, which is true.
Induction step: Suppose $n \in \mathbb{N}$, and for any sequences of real numbers $a_0, a_1, \ldots, a_n$ and $b_0, b_1, \ldots, b_n$, $\sum_{i=0}^{n}(a_i + b_i) = \sum_{i=0}^{n} a_i + \sum_{i=0}^{n} b_i$. Now suppose $a_0, a_1, \ldots, a_{n+1}$ and $b_0, b_1, \ldots, b_{n+1}$ are sequences of real numbers. Then

$$\begin{aligned}\sum_{i=0}^{n+1}(a_i + b_i) &= \sum_{i=0}^{n}(a_i + b_i) + (a_{n+1} + b_{n+1}) \\ &= \left(\sum_{i=0}^{n} a_i + \sum_{i=0}^{n} b_i\right) + (a_{n+1} + b_{n+1}) && \text{(inductive hypothesis)} \\ &= \left(\sum_{i=0}^{n} a_i + a_{n+1}\right) + \left(\sum_{i=0}^{n} b_i + b_{n+1}\right) \\ &= \sum_{i=0}^{n+1} a_i + \sum_{i=0}^{n+1} b_i.\end{aligned}$$

(b) We use induction on n.
Base case: When $n = 0$, both sides of the equation are equal to ca_0.

Induction step: Suppose $n \in \mathbb{N}$, and for any real numbers c and $a_0, a_1, \ldots, a_n$, $c \cdot \sum_{i=0}^{n} a_i = \sum_{i=0}(c \cdot a_i)$. Then

$$\begin{aligned} c \cdot \sum_{i=0}^{n+1} a_i &= c \cdot \left(\sum_{i=0}^{n} a_i + a_{n+1} \right) \\ &= c \cdot \sum_{i=0}^{n} a_i + c \cdot a_{n+1} \\ &= \sum_{i=0}^{n} (c \cdot a_i) + c \cdot a_{n+1} && \text{(inductive hypothesis)} \\ &= \sum_{i=0}^{n+1} (c \cdot a_i). \end{aligned}$$

8. (a) We let m be arbitrary and then prove by induction that for all $n \geq m$, $H_n - H_m \geq (n-m)/n$.
Base case: $n = m$. Then $H_n - H_m = 0 \geq 0 = (n-m)/n$.
Induction step: Suppose that $n \geq m$ and $H_n - H_m \geq (n-m)/n$. Then

$$\begin{aligned} H_{n+1} - H_m = H_n + \frac{1}{n+1} - H_m &\geq \frac{n-m}{n} + \frac{1}{n+1} \\ &\geq \frac{n-m}{n+1} + \frac{1}{n+1} = \frac{n+1-m}{n+1}. \end{aligned}$$

(b) Base case: If $n = 0$ then $H_{2^n} = H_1 = 1 \geq 1 = 1 + n/2$.
Induction step: Suppose $n \geq 0$ and $H_{2^n} \geq 1 + n/2$. By part (a),

$$H_{2^{n+1}} - H_{2^n} \geq \frac{2^{n+1} - 2^n}{2^{n+1}} = \frac{1}{2}.$$

Therefore

$$H_{2^{n+1}} \geq H_{2^n} + \frac{1}{2} \geq 1 + \frac{n}{2} + \frac{1}{2} = 1 + \frac{n+1}{2}.$$

(c) Since $\lim_{n\to\infty}(1 + n/2) = \infty$, by part (b) $\lim_{n\to\infty} H_{2^n} = \infty$. Clearly the H_n's form an increasing sequence, so $\lim_{n\to\infty} H_n = \infty$.

9. Base case: When $n = 2$, $\sum_{k=1}^{n-1} H_k = H_1 = 1 = 2(3/2) - 2 = nH_n - n$.
Induction step: Suppose $n \geq 2$ and $\sum_{k=1}^{n-1} H_k = nH_n - n$. Then

$$\begin{aligned} \sum_{k=1}^{n} H_k &= \sum_{k=1}^{n-1} H_k + H_n \\ &= nH_n - n + H_n && \text{(inductive hypothesis)} \\ &= (n+1)H_n + 1 - (n+1) = (n+1)\left(H_n + \frac{1}{n+1} \right) - (n+1) \\ &= (n+1)H_{n+1} - (n+1). \end{aligned}$$

10. We will prove by induction that for all $n \geq 1$, $\sum_{i=1}^{n}(i \cdot (i!)) = (n+1)! - 1$.
Base case: When $n = 1$, both sides of the equation are equal to 1.
Induction step: Suppose $n \geq 1$ and $\sum_{i=1}^{n}(i \cdot (i!)) = (n+1)! - 1$. Then

$$\sum_{i=1}^{n+1}(i \cdot (i!)) = \sum_{i=1}^{n}(i \cdot (i!)) + (n+1) \cdot (n+1)!$$

$$= (n+1)! - 1 + (n+1)\cdot(n+1)! \qquad \text{(inductive hypothesis)}$$
$$= (n+2)\cdot(n+1)! - 1 = (n+2)! - 1.$$

11. We will prove by induction that for all $n \in \mathbb{N}$, $\sum_{i=0}^{n}(i/(i+1)!) = 1 - 1/(n+1)!$.
Base case: When $n = 0$, both sides of the equation are equal to 0.
Induction step: Suppose $n \in \mathbb{N}$ and $\sum_{i=0}^{n}(i/(i+1)!) = 1 - 1/(n+1)!$. Then

$$\begin{aligned}\sum_{i=0}^{n+1}\frac{i}{(i+1)!} &= \sum_{i=0}^{n}\frac{i}{(i+1)!} + \frac{n+1}{(n+2)!} \\ &= 1 - \frac{1}{(n+1)!} + \frac{n+1}{(n+2)!} \qquad \text{(inductive hypothesis)} \\ &= 1 - \frac{n+2}{(n+2)!} + \frac{n+1}{(n+2)!} = 1 - \frac{1}{(n+2)!}.\end{aligned}$$

12. (a) We will prove by induction that for all $n \in \mathbb{N}$, $2^n \geq n+1$, from which the desired conclusion follows.
Base case: When $n = 0$, $2^n = 2^0 = 1 \geq 0 + 1 = n + 1$.
Induction step. Suppose $n \in \mathbb{N}$ and $2^n \geq n+1$. Then $2^{n+1} = 2\cdot 2^n \geq 2\cdot(n+1) = 2n+2 \geq n+2$.

(b) Base case: $n = 9$. Then $n! = 362880 \geq 262144 = (2^n)^2$.
Induction step: Suppose that $n \geq 9$ and $n! \geq (2^n)^2$. Then

$$\begin{aligned}(n+1)! &= (n+1)\cdot n! \geq (n+1)\cdot(2^n)^2 \geq 10\cdot 2^{2n} \geq 2^2\cdot 2^{2n} \\ &= 2^{2n+2} = (2^{n+1})^2.\end{aligned}$$

(c) Base case: $n = 0$. Then $n! = 1 \leq 1 = 2^{(n^2)}$.
Induction step: Suppose that $n \in \mathbb{N}$ and $n! \leq 2^{(n^2)}$. Then

$$\begin{aligned}2^{((n+1)^2)} &= 2^{n^2+2n+1} = 2^{(n^2)}\cdot 2^{2n+1} \geq 2^{(n^2)}\cdot 2^{n+1} \\ &> n!\cdot(n+1) \qquad \text{(by inductive hypothesis and part (a))} \\ &= (n+1)!.\end{aligned}$$

13. (a) Base case: When $n = 0$, $(k^2+n)! = (k^2)! \geq 1 = k^{2n}$.
Induction step: Suppose $n \in \mathbb{N}$ and $(k^2+n)! \geq k^{2n}$. Then $(k^2+n+1)! = (k^2+n+1)\cdot(k^2+n)! \geq k^2\cdot k^{2n} = k^{2n+2} = k^{2(n+1)}$.

(b) Base case: When $n = 2k^2$, by part (a), $n! = (k^2+k^2)! \geq k^{2k^2} = k^n$.
Induction step: Suppose $n \geq 2k^2$ and $n! \geq k^n$. Then $(n+1)! = (n+1)\cdot n! \geq (n+1)\cdot k^n > k\cdot k^n = k^{n+1}$.

14. Let a be an arbitrary real number and m an arbitrary natural number. We now prove by induction that for all $n \in \mathbb{N}$, $(a^m)^n = a^{mn}$.
Base case: When $n = 0$, $(a^m)^n = (a^m)^0 = 1 = a^0 = a^{mn}$.
Induction step: Suppose $n \in \mathbb{N}$ and $(a^m)^n = a^{mn}$. Then

$$\begin{aligned}(a^m)^{n+1} &= (a^m)^n\cdot a^m && \text{(definition of exponentiation)} \\ &= a^{mn}\cdot a^m && \text{(inductive hypothesis)} \\ &= a^{mn+m} && \text{(Example 6.3.2)} \\ &= a^{m(n+1)}.\end{aligned}$$

15. Base case: $n = 0$. Then $a_n = a_0 = 0 = 2^0 - 0 - 1 = 2^n - n - 1$.
Induction step: Suppose that $n \in \mathbb{N}$ and $a_n = 2^n - n - 1$. Then

$$\begin{aligned} a_{n+1} &= 2a_n + n = 2(2^n - n - 1) + n \\ &= 2^{n+1} - 2n - 2 + n = 2^{n+1} - n - 2 = 2^{n+1} - (n+1) - 1. \end{aligned}$$

16. We will prove by induction that for all $n \in \mathbb{N}$, $a_n = 2^{(2^n)}$.
Base case: $n = 0$. Then $a_n = a_0 = 2 = 2^{(2^0)} = 2^{(2^n)}$.
Induction step: Suppose $n \in \mathbb{N}$ and $a_n = 2^{(2^n)}$. Then $a_{n+1} = (a_n)^2 = (2^{(2^n)})^2 = 2^{(2^n \cdot 2)} = 2^{(2^{n+1})}$.

17. We will prove by induction that for all $n \geq 1$, $a_n = 1/n$.
Base case: $n = 1$. Then $a_n = a_1 = 1 = 1/n$.
Induction step: Suppose $n \geq 1$ and $a_n = 1/n$. Then

$$a_{n+1} = \frac{a_n}{a_n + 1} = \frac{1/n}{1/n + 1} = \frac{1/n}{(n+1)/n} = \frac{1}{n+1}.$$

18. (a) $\binom{n}{0} = n!/(0!n!) = 1$ and $\binom{n}{n} = n!/(n!0!) = 1$.
(b)

$$\begin{aligned} \binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\ &= \frac{n!(n-k+1)}{k!(n-k+1)!} + \frac{n!k}{k!(n-k+1)!} \\ &= \frac{n!(n+1)}{k!(n+1-k)!} = \frac{(n+1)!}{k!(n+1-k)!} = \binom{n+1}{k}. \end{aligned}$$

(c) We follow the hint.
Base case: $n = 0$. Suppose A is a set with 0 elements. Then $A = \varnothing$, the only value of k we have to worry about is $k = 0$, $\mathscr{P}_0(A) = \{\varnothing\}$, which has 1 element, and $\binom{0}{0} = 1$.
Induction step: Suppose the desired conclusion holds for sets with n elements, and A is a set with $n + 1$ elements. Let a be an element of A, and let $A' = A \setminus \{a\}$, which is a set with n elements. Now suppose $0 \leq k \leq n + 1$. We consider three cases.
Case 1: $k = 0$. Then $\mathscr{P}_k(A) = \{\varnothing\}$, which has 1 element, and $\binom{n+1}{k} = 1$.
Case 2: $k = n + 1$. Then $\mathscr{P}_k(A) = \{A\}$, which has 1 element, and $\binom{n+1}{k} = 1$.
Case 3. $0 < k \leq n$. There are two kinds of k-element subsets of A: those that contain a as an element, and those that don't. The k-element subsets that don't contain a are just the k-element subsets of A', and by inductive hypothesis there are $\binom{n}{k}$ of these. Those that do contain a are the sets of the form $X \cup \{a\}$, where $X \in \mathscr{P}_{k-1}(A')$, and by inductive hypothesis there are $\binom{n}{k-1}$ of these, since this is the number of possibilities for X. Therefore by part (b), the total number of k-element subsets of A is

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

(d) We let x and y be arbitrary and then prove the equation by induction on n.
Base case: $n = 0$. Then both sides of the equation are equal to 1.
Induction step: We will make use of parts (a) and (b). Suppose that

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

Then

$$(x+y)^{n+1} = (x+y)(x+y)^n$$

$$
\begin{aligned}
&= (x+y)\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k \quad \text{(by inductive hypothesis)}\\
&= (x+y)\left[\binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 \right.\\
&\qquad \left. + \cdots + \binom{n}{n}y^n\right]\\
&= \binom{n}{0}x^{n+1} + \binom{n}{0}x^n y + \binom{n}{1}x^n y + \binom{n}{1}x^{n-1}y^2\\
&\qquad + \cdots + \binom{n}{n}xy^n + \binom{n}{n}y^{n+1}\\
&= x^{n+1} + \left[\binom{n}{0} + \binom{n}{1}\right]x^n y + \left[\binom{n}{1} + \binom{n}{2}\right]x^{n-1}y^2\\
&\qquad + \cdots + \left[\binom{n}{n-1} + \binom{n}{n}\right]xy^n + y^{n+1}\\
&= \binom{n+1}{0}x^{n+1} + \binom{n+1}{1}x^n y + \binom{n+1}{2}x^{n-1}y^2\\
&\qquad + \cdots + \binom{n+1}{n}xy^n + \binom{n+1}{n+1}y^{n+1}\\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}x^{n+1-k}y^k.
\end{aligned}
$$

19. (a) Proof 1: We apply part (d) of exercise 18, with $x = y = 1$:

$$2^n = (1+1)^n = \sum_{k=0}^{n}\binom{n}{k}1^{n-k}1^k = \sum_{k=0}^{n}\binom{n}{k}.$$

Proof 2: Let A be a set with n elements. By part (c) of exercise 18, $\sum_{k=0}^{n}\binom{n}{k}$ is the number of elements in $\mathscr{P}(A)$. By exercise 11 of Section 6.2, this number is 2^n.

(b) We apply part (d) of exercise 18, with $x = 1$ and $y = -1$:

$$0 = (1-1)^n = \sum_{k=0}^{n}\binom{n}{k}1^{n-k}(-1)^k = \sum_{k=0}^{n}(-1)^k\binom{n}{k}.$$

20. We will prove by induction that for all $n \geq 1$, $0 < a_n < 1/2$, from which the desired conclusion follows.

Base case: $n = 1$. Then $a_n = a_1 = 1/4$, so $0 < a_n < 1/2$.

Induction step: Suppose $n \geq 1$ and $0 < a_n < 1/2$. Then by Example 3.1.2, $a_n^2 < (1/2)^2 = 1/4$, so $a_{n+1} = (a_n)^2 + 1/4 < 1/4 + 1/4 = 1/2$. It is also clear that $a_{n+1} = a_n^2 + 1/4 \geq 1/4 > 0$, so $0 < a_{n+1} < 1/2$.

21. (a) $f_1(x) = 2^{f_0(x)} = 2^x$, $f_2(x) = 2^{f_1(x)} = 2^{(2^x)}$, $f_3(x) = 2^{f_2(x)} = 2^{(2^{(2^x)})}$.

(b) Let x and y be arbitrary positive integers with $x < y$. We now prove by induction that for all $n \in \mathbb{N}$, $f_n(x) < f_n(y)$. Base case: $n = 0$. Then $f_n(x) = f_0(x) = x < y = f_0(y) = f_n(y)$.

Induction step: Suppose $n \in \mathbb{N}$ and $f_n(x) < f_n(y)$. Then $f_{n+1}(x) = 2^{f_n(x)} < 2^{f_n(y)} = f_{n+1}(y)$.

(c) Let m be an arbitrary natural number and x an arbitrary positive integer. We now prove by induction that for all $n \geq m+1$, $f_m(x) < f_n(x)$.

Base case: $n = m+1$. Then by exercise 12(a), $f_m(x) < 2^{f_m(x)} = f_{m+1}(x) = f_n(x)$.

Induction step: Suppose $n \geq m+1$ and $f_m(x) < f_n(x)$. As in the base case, by exercise 12(a), $f_n(x) < 2^{f_n(x)} = f_{n+1}(x)$. Therefore $f_m(x) < f_{n+1}(x)$.

(d) Suppose $n \in \mathbb{N}$. By part (c), for every $x \in \mathbb{Z}^+$, $f_n(x) < f_{n+1}(x)$, so $f_n \in O(f_{n+1})$. Now suppose $f_{n+1} \in O(f_n)$. Then we can choose $a \in \mathbb{Z}^+$ and $c \in \mathbb{R}^+$ such that for all $x > a$, $f_{n+1}(x) \leq cf_n(x)$. Let x be any positive integer such that $x > a$, $x \geq c$, and $x \geq 5$. Note that by part (c), $f_n(x) \geq f_0(x) = x \geq 5$. Therefore

$$\begin{aligned} f_{n+1}(x) = 2^{f_n(x)} &> (f_n(x))^2 && \text{(Example 6.1.3, since } f_n(x) \geq 5) \\ &\geq cf_n(x) && \text{(since } f_n(x) \geq f_0(x) = x \geq c). \end{aligned}$$

This contradicts the fact that for all $x > a$, $f_{n+1}(x) \leq cf_n(x)$. Therefore $f_{n+1} \notin O(f_n)$.

(e) $g(1) = f_1(1) = 2^1 = 2$, $g(2) = f_2(2) = 2^{(2^2)} = 2^4 = 16$, and $g(3) = f_3(3) = 2^{(2^{(2^3)})} = 2^{256} = 115792089237316195423570985008687907853269984665640564039457584007913129639936$.

(f) Suppose $n \in \mathbb{N}$. Then by part (c), for every $x > n$, $f_n(x) < f_x(x) = g(x)$. Therefore for every $n \in \mathbb{N}$, $f_n \in O(g)$. Now suppose $n \in \mathbb{N}$ and $g \in O(f_n)$. Since $f_{n+1} \in O(g)$, by exercise 19(b) in Section 5.1, $f_{n+1} \in O(f_n)$, which contradicts part (d).

22. By changing the goal to a stronger statement, we made the inductive hypothesis stronger, which helped in the induction step.

Section 6.4

1. (a) ($\rightarrow$) Suppose that $\forall n Q(n)$. Let n be arbitrary. Then $Q(n+1)$ is true, which means $\forall k < n+1\, P(k)$. In particular, since $n < n+1$, $P(n)$ is true. Since n was arbitrary, this shows that $\forall n P(n)$.

($\leftarrow$) Suppose that $\forall n P(n)$. Then for any n, it is clearly true that $\forall k < n\, P(k)$, which means that $Q(n)$ is true.

(b) Base case: $n = 0$. Then $Q(n)$ is the statement $\forall k < 0\, P(k)$, which is vacuously true.

Induction step: Suppose $Q(n)$ is true. This means that $\forall k < n\, P(k)$ is true, so by assumption, it follows that $P(n)$ is true. Therefore $\forall k < n+1\, P(k)$ is true, which means that $Q(n+1)$ is true.

2. Suppose $q \in \mathbb{N}$, $q > 0$, and $\forall k < q[0 < k \rightarrow \neg\exists j \in \mathbb{Z}^+(j/k = \sqrt{2})]$. Now suppose there is some $p \in \mathbb{Z}^+$ such that $p/q = \sqrt{2}$. As in the proof of Theorem 6.4.5, we can show that p and q are both even, so there are positive integers j and k such that $p = 2j$ and $q = 2k$. Therefore $0 < k < q$ and $j/k = p/q = \sqrt{2}$, which contradicts the inductive hypothesis. Thus $\neg\exists p \in \mathbb{Z}^+(p/q = \sqrt{2})$.

3. Suppose $\sqrt{2}$ is rational, and let $S = \{q \in \mathbb{Z}^+ \mid \exists p \in \mathbb{Z}^+(p/q = \sqrt{2})\} \neq \varnothing$. By the well-ordering principle, let q be the smallest element of S, and let p be a positive integer such that $p/q = \sqrt{2}$. Then $p^2/q^2 = 2$, so $p^2 = 2q^2$. Since $1 < \sqrt{2} = p/q < 2$, $q < p < 2q$, and therefore $p - q$ and $2q - p$ are positive integers. Since $p^2 = 2q^2$,

$$\left(\frac{2q-p}{p-q}\right)^2 = \frac{4q^2 - 4pq + p^2}{p^2 - 2pq + q^2} = \frac{6q^2 - 4pq}{3q^2 - 2pq} = 2,$$

so $(2q-p)/(p-q) = \sqrt{2}$. Therefore $p - q \in S$ and $p - q < 2q - q = q$, which contradicts the fact that q is the smallest element of S.

4. (a) Suppose $\sqrt{6}$ is rational. Let $S = \{q \in \mathbb{Z}^+ \mid \exists p \in \mathbb{Z}^+(p/q = \sqrt{6})\}$. Then $S \neq \varnothing$, so we can let q be the smallest element of S, and we can choose a positive integer p such that $p/q = \sqrt{6}$. Therefore $p^2 = 6q^2$, so p^2 is even, and hence p is even. This means that $p = 2\overline{p}$, for some integer $\overline{p}$. Thus $4\overline{p}^2 = 6q^2$, so $2\overline{p}^2 = 3q^2$ and therefore $3q^2$ is even. It is easy to check that if q is odd then $3q^2$ is odd, so q must be even, which means that $q = 2\overline{q}$ for some integer $\overline{q}$. But then $\sqrt{6} = \overline{p}/\overline{q}$ and $\overline{q} < q$, contradicting the fact that q is the smallest element of S.

(b) Suppose that $\sqrt{2}+\sqrt{3}=p/q$. Squaring both sides gives us $5+2\sqrt{6}=p^2/q^2$, so $\sqrt{6}=(p^2-5q^2)/(2q^2)$, which contradicts part (a).

5. We use strong induction to prove that $\forall n \in \mathbb{N}(n \geq 12 \rightarrow$ some combination of red and blue beads is worth n Martian credits). Suppose $n \in \mathbb{N}$, $n \geq 12$, and $\forall k < n(k \geq 12 \rightarrow$ some combination of red and blue beads is worth k Martian credits). We now consider several cases.

Case 1. $n = 12$. Then 4 blue beads is worth n credits.

Case 2. $n = 13$. Then 1 red bead and 2 blue beads is worth n credits.

Case 3. $n = 14$. Then 2 red beads is worth n credits.

Case 4. $n \geq 15$. Then $n-3 \geq 12$, so by inductive hypothesis there are natural numbers b and r such that b blue beads and r red beads are worth $n-3$ credits. Therefore $b+1$ blue beads and r red beads are worth $n-3+3=n$ credits.

6. We use strong induction. Suppose $n \geq 1$ and for all k, if $1 \leq k < n$ then $x^k + 1/x^k$ is an integer.

Case 1. $n = 1$. Then $x^n + 1/x^n = x + 1/x$, which is an integer by assumption.

Case 2. $n = 2$. Then $x^2 + 1/x^2 = (x + 1/x)^2 - 2$, which is an integer.

Case 3. $n \geq 3$. Then by inductive hypothesis, $x^{n-1} + 1/x^{n-1}$ and $x^{n-2} + 1/x^{n-2}$ are integers, and therefore

$$x^n + \frac{1}{x^n} = \left(x^{n-1} + \frac{1}{x^{n-1}}\right)\left(x + \frac{1}{x}\right) - \left(x^{n-2} + \frac{1}{x^{n-2}}\right)$$

is also an integer.

7. (a) We use ordinary induction on n.

Base case: $n = 0$. Both sides of the equation are equal to 0.

Induction step: Suppose that $\sum_{i=0}^{n} F_i = F_{n+2} - 1$. Then

$$\sum_{i=0}^{n+1} F_i = \sum_{i=0}^{n} F_i + F_{n+1} = (F_{n+2} - 1) + F_{n+1} = F_{n+3} - 1.$$

(b) We use ordinary induction on n.

Base case: $n = 0$. Both sides of the equation are equal to 0.

Induction step. Suppose that $\sum_{i=0}^{n} (F_i)^2 = F_n F_{n+1}$. Then

$$\sum_{i=0}^{n+1} (F_i)^2 = \sum_{i=0}^{n} (F_i)^2 + (F_{n+1})^2 = F_n F_{n+1} + (F_{n+1})^2 = F_{n+1}(F_n + F_{n+1}) = F_{n+1}F_{n+2}.$$

(c) We use ordinary induction on n.

Base case: $n = 0$. Both sides of the equation are equal to 1.

Induction step: Suppose that $\sum_{i=0}^{n} F_{2i+1} = F_{2n+2}$. Then

$$\sum_{i=0}^{n+1} F_{2i+1} = \sum_{i=0}^{n} F_{2i+1} + F_{2n+3} = F_{2n+2} + F_{2n+3} = F_{2n+4} = F_{2(n+1)+2}.$$

(d) We will use induction to prove that for all n, $\sum_{i=0}^{n} F_{2i} = F_{2n+1} - 1$.

Base case: $n = 0$. Both sides of the equation are equal to 0.

Induction step: Suppose $\sum_{i=0}^{n} F_{2i} = F_{2n+1} - 1$. Then

$$\sum_{i=0}^{n+1} F_{2i} = \sum_{i=0}^{n} F_{2i} + F_{2n+2} = F_{2n+1} - 1 + F_{2n+2} = F_{2n+3} - 1 = F_{2(n+1)+1} - 1.$$

8. (a) Let $m \geq 1$ be arbitrary. We now prove by strong induction that $\forall n \in \mathbb{N}(F_{m+n} = F_{m-1}F_n + F_mF_{n+1})$. Suppose that $n \in \mathbb{N}$ and $\forall k < n(F_{m+k} = F_{m-1}F_k + F_mF_{k+1})$.
Case 1. $n = 0$. Then $F_{m-1}F_n + F_mF_{n+1} = F_{m-1} \cdot 0 + F_m \cdot 1 = F_m = F_{m+n}$.
Case 2. $n = 1$. Then $F_{m-1}F_n + F_mF_{n+1} = F_{m-1} \cdot 1 + F_m \cdot 1 = F_{m+1} = F_{m+n}$.
Case 3. $n \geq 2$. Then by inductive hypothesis,

$$F_{m+n-2} = F_{m-1}F_{n-2} + F_mF_{n-1},$$
$$F_{m+n-1} = F_{m-1}F_{n-1} + F_mF_n.$$

Adding these two equations, we get

$$F_{m+n} = F_{m+n-2} + F_{m+n-1} = F_{m-1}(F_{n-2} + F_{n-1}) + F_m(F_{n-1} + F_n) = F_{m-1}F_n + F_mF_{n+1}.$$

(b) Once again we let $m \geq 1$ be arbitrary and then proceed by strong induction on n. Suppose that $n \geq 1$ and $\forall k(1 \leq k < n \to F_{m+k} = F_{m+1}F_{k+1} - F_{m-1}F_{k-1})$.
Case 1. $n = 1$. Then $F_{m+1}F_{n+1} - F_{m-1}F_{n-1} = F_{m+1} \cdot 1 + F_{m-1} \cdot 0 = F_{m+1} = F_{m+n}$.
Case 2. $n = 2$. Then $F_{m+1}F_{n+1} - F_{m-1}F_{n-1} = F_{m+1} \cdot 2 - F_{m-1} \cdot 1 = F_{m+1} + (F_{m+1} - F_{m-1}) = F_{m+1} + F_m = F_{m+2} = F_{m+n}$.
Case 3. $n \geq 3$. Then by inductive hypothesis,

$$F_{m+n-2} = F_{m+1}F_{n-1} - F_{m-1}F_{n-3},$$
$$F_{m+n-1} = F_{m+1}F_n - F_{m-1}F_{n-2}.$$

Adding these two equations, we get

$$F_{m+n} = F_{m+n-2} + F_{m+n-1} = F_{m+1}(F_{n-1} + F_n) - F_{m-1}(F_{n-3} + F_{n-2}) = F_{m+1}F_{n+1} - F_{m-1}F_{n-1}.$$

(c) We use ordinary induction.
Base case: $n = 0$. Then $(F_n)^2 + (F_{n+1})^2 = 0^2 + 1^2 = 1 = F_{2n+1}$ and $(F_{n+2})^2 - (F_n)^2 = 1^2 - 0^2 = 1 = F_{2n+2}$.
Induction step: Suppose

$$(F_n)^2 + (F_{n+1})^2 = F_{2n+1}, \tag{$*$}$$
$$(F_{n+2})^2 - (F_n)^2 = F_{2n+2}. \tag{$**$}$$

Adding $(*)$ and $(**)$ gives

$$(F_{n+1})^2 + (F_{n+2})^2 = F_{2n+1} + F_{2n+2} = F_{2n+3}, \tag{$***$}$$

which is the first equation we must prove. To prove the second, we compute

$$\begin{aligned}
(F_{n+3})^2 - (F_{n+1})^2 &= (F_{n+2} + F_{n+1})^2 - (F_{n+1})^2 \\
&= (F_{n+2})^2 + 2F_{n+2}F_{n+1} + (F_{n+1})^2 - (F_{n+1})^2 \\
&= (F_{n+2})^2 + 2(F_{n+1} + F_n)F_{n+1} \\
&= (F_{n+2})^2 + 2(F_{n+1})^2 + 2F_nF_{n+1} \\
&= (F_{n+1})^2 + (F_{n+2})^2 + ((F_{n+1})^2 + 2F_nF_{n+1} + (F_n)^2) - (F_n)^2 \\
&= (F_{n+1})^2 + (F_{n+2})^2 + (F_{n+1} + F_n)^2 - (F_n)^2 \\
&= (F_{n+1})^2 + (F_{n+2})^2 + (F_{n+2})^2 - (F_n)^2 \\
&= F_{2n+3} + F_{2n+2} \qquad \text{(by } (**) \text{ and } (***)\text{)} \\
&= F_{2n+4}.
\end{aligned}$$

(d) Let $m \in \mathbb{N}$ be arbitrary. We first use induction to prove that $\forall k \in \mathbb{N}(F_m \mid F_{km})$.

Base case: $k = 0$. Then $F_{km} = F_0 = 0 = 0 \cdot F_m$, so $F_m \mid F_{km}$.

Induction step: Suppose $F_m \mid F_{km}$. Then there is some integer j such that $F_{km} = jF_m$. Therefore by part (a),

$$F_{(k+1)m} = F_{km+m} = F_{km-1}F_m + F_{km}F_{m+1} = F_{km-1}F_m + (jF_m)F_{m+1} = (F_{km-1} + jF_{m+1})F_m,$$

so $F_m \mid F_{(k+1)m}$.

Finally, to complete the problem, suppose $m \mid n$. Then there is some natural number k such that $n = km$, so by the statement we have just proven, $F_m \mid F_n$.

(e) We use ordinary induction.

Base case: If $n = 1$, then

$$\sum_{i=0}^{n-1} \binom{2n-i-2}{i} = \binom{0}{0} = 1 = F_{2n-1},$$
$$\sum_{i=0}^{n-1} \binom{2n-i-1}{i} = \binom{1}{0} = 1 = F_{2n}.$$

Induction step: Suppose $n \geq 1$ and

$$F_{2n-1} = \sum_{i=0}^{n-1} \binom{2n-i-2}{i}, \qquad F_{2n} = \sum_{i=0}^{n-1} \binom{2n-i-1}{i}.$$

Then

$$\begin{aligned}
F_{2n+1} = F_{2n} + F_{2n-1} &= \sum_{i=0}^{n-1} \binom{2n-i-1}{i} + \sum_{i=0}^{n-1} \binom{2n-i-2}{i} \\
&= \binom{2n-1}{0} + \binom{2n-2}{1} + \cdots + \binom{n}{n-1} + \binom{2n-2}{0} + \binom{2n-3}{1} + \cdots + \binom{n-1}{n-1} \\
&= \binom{2n-1}{0} + \left(\binom{2n-2}{1} + \binom{2n-2}{0}\right) + \left(\binom{2n-3}{2} + \binom{2n-3}{1}\right) + \cdots \\
&\qquad + \left(\binom{n}{n-1} + \binom{n}{n-2}\right) + \binom{n-1}{n-1} \\
&= 1 + \binom{2n-1}{1} + \binom{2n-2}{2} + \cdots + \binom{n+1}{n-1} + 1 \qquad \text{(by exercise 18 in Section 6.3)} \\
&= \binom{2n}{0} + \binom{2n-1}{1} + \binom{2n-2}{2} + \cdots + \binom{n}{n} = \sum_{i=0}^{n} \binom{2n-i}{i}.
\end{aligned}$$

Similarly,

$$\begin{aligned}
F_{2n+2} = F_{2n+1} + F_{2n} &= \sum_{i=0}^{n} \binom{2n-i}{i} + \sum_{i=0}^{n-1} \binom{2n-i-1}{i} \\
&= \binom{2n}{0} + \binom{2n-1}{1} + \cdots + \binom{n}{n} + \binom{2n-1}{0} + \binom{2n-2}{1} + \cdots + \binom{n}{n-1} \\
&= \binom{2n}{0} + \left(\binom{2n-1}{1} + \binom{2n-1}{0}\right) + \left(\binom{2n-2}{2} + \binom{2n-2}{1}\right) + \cdots
\end{aligned}$$

$$+\left(\binom{n}{n}+\binom{n}{n-1}\right)$$
$$=1+\binom{2n}{1}+\binom{2n-1}{2}+\cdots+\binom{n+1}{n} \qquad \text{(by exercise 18 in Section 6.3)}$$
$$=\binom{2n+1}{0}+\binom{2n}{1}+\binom{2n-1}{2}+\cdots+\binom{n+1}{n}=\sum_{i=0}^{n}\binom{2n+1-i}{i}.$$

9. (a) ($\rightarrow$) Suppose a_0, a_1, a_2, ... is a Gibonacci sequence. Then in particular $a_2 = a_0 + a_1$, which means $c^2 = 1+c$. Solving this quadratic equation by the quadratic formula leads to the conclusion $c = (1 \pm \sqrt{5})/2$.

   ($\leftarrow$) Suppose either $c = (1+\sqrt{5})/2$ or $c = (1-\sqrt{5})/2$. Then $c^2 = 1 + c$, and therefore for every $n \geq 2$, $a_n = c^n = c^{n-2}c^2 = c^{n-2}(1+c) = c^{n-2} + c^{n-1} = a_{n-2} + a_{n-1}$.

   (b) It will be convenient to introduce the notation $c_1 = (1+\sqrt{5})/2$ and $c_2 = (1-\sqrt{5})/2$. Then for any $n \geq 2$, $a_n = sc_1^n + tc_2^n = sc_1^{n-2}c_1^2 + tc_2^{n-2}c_2^2 = sc_1^{n-2}(1+c_1) + tc_2^{n-2}(1+c_2) = (sc_1^{n-2} + tc_2^{n-2}) + (sc_1^{n-1} + tc_2^{n-1}) = a_{n-2} + a_{n-1}$.

   (c) Let $s = (5a_0 + (2a_1 - a_0)\sqrt{5})/10$ and $t = (5a_0 - (2a_1 - a_0)\sqrt{5})/10$. For all $n \in \mathbb{N}$ let

$$b_n = s\left(\frac{1+\sqrt{5}}{2}\right)^n + t\left(\frac{1-\sqrt{5}}{2}\right)^n,$$

   and notice that by part (b), b_0, b_1, ... is a Gibonacci sequence.

   We now prove by strong induction that for all $n \in \mathbb{N}$, $a_n = b_n$, which will solve the problem. Suppose $n \in \mathbb{N}$ and for all $k < n$, $a_k = b_k$.

   Case 1. $n = 0$. Then

$$b_0 = s\left(\frac{1+\sqrt{5}}{2}\right)^0 + t\left(\frac{1-\sqrt{5}}{2}\right)^0$$
$$= \frac{5a_0 + (2a_1 - a_0)\sqrt{5}}{10} + \frac{5a_0 - (2a_1 - a_0)\sqrt{5}}{10}$$
$$= \frac{10a_0}{10} = a_0.$$

   Case 2. $n = 1$. Then

$$b_1 = s\left(\frac{1+\sqrt{5}}{2}\right)^1 + t\left(\frac{1-\sqrt{5}}{2}\right)^1$$
$$= \left(\frac{5a_0 + (2a_1 - a_0)\sqrt{5}}{10}\right)\left(\frac{1+\sqrt{5}}{2}\right) + \left(\frac{5a_0 - (2a_1 - a_0)\sqrt{5}}{10}\right)\left(\frac{1-\sqrt{5}}{2}\right)$$
$$= \frac{10a_1 + (4a_0 + 2a_1)\sqrt{5}}{20} + \frac{10a_1 - (4a_0 + 2a_1)\sqrt{5}}{20}$$
$$= \frac{20a_1}{20} = a_1.$$

   Case 3. $n \geq 2$. Then since both the a's and the b's are Gibonacci sequences, $a_n = a_{n-2} + a_{n-1} = b_{n-2} + b_{n-1} = b_n$.

10. The Lucas numbers form a Gibonacci sequence, so we can apply our solution to exercise 9(c) to find a formula for them. According to that solution, for every n, $L_n = s((1+\sqrt{5})/2)^n + t((1-\sqrt{5})/2)^n$,

where

$$s = \frac{5L_0 + (2L_1 - L_0)\sqrt{5}}{10} = \frac{10 + 0 \cdot \sqrt{5}}{10} = 1, \qquad t = \frac{5L_0 - (2L_1 - L_0)\sqrt{5}}{10} = \frac{10 - 0 \cdot \sqrt{5}}{10} = 1.$$

Thus,

$$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

11. Imitating exercise 9, we first consider sequence of the form $a_n = c^n$, for some constant c. If such a sequence satisfies the recurrence $a_n = 5a_{n-1} - 6a_{n-2}$, then in particular $a_2 = 5a_1 - 6a_0$, so $c^2 = 5c - 6$. The solutions to this quadratic equation are $c = 2, 3$.

    Now consider sequences of the form $a_n = s2^n + t3^n$, for any two numbers s and t. For any such sequence, if $n \geq 2$ then $5a_{n-1} - 6a_{n-2} = 5(s2^{n-1} + t3^{n-1}) - 6(s2^{n-2} + t3^{n-2}) = 4s2^{n-2} + 9t3^{n-2} = s2^n + t3^n = a_n$. In other words, any such sequence will satisfy the recurrence in the exercise. If we can choose s and t so that $a_0 = -1$ and $a_1 = 0$, then the sequence will be the sequence determined by the recursive definition in the exercise.

    Since $a_0 = s2^0 + t3^0 = s + t$ and $a_1 = s2^1 + t3^1 = 2s + 3t$, we want s and t satisfying the equations

$$s + t = -1, \qquad 2s + 3t = 0.$$

    The unique solution to this system of equations is $s = -3$, $t = 2$. So the sequence is given by the formula $a_n = -3 \cdot 2^n + 2 \cdot 3^n$.

12. We use strong induction. Suppose that $n \in \mathbb{N}$, and for all $k < n$, $a_k = F_k$.

    Case 1. $n = 0$. Then $a_n = a_0 = 0 = F_0 = F_n$.

    Case 2. $n = 1$. Then $a_n = a_1 = 1 = F_1 = F_n$.

    Case 3. $n = 2$. Then $a_n = a_2 = 1 = F_2 = F_n$.

    Case 4. $n \geq 3$. Then

$$\begin{aligned} a_n &= \frac{1}{2}a_{n-3} + \frac{3}{2}a_{n-2} + \frac{1}{2}a_{n-1} \\ &= \frac{1}{2}F_{n-3} + \frac{3}{2}F_{n-2} + \frac{1}{2}F_{n-1} && \text{(inductive hypothesis)} \\ &= \frac{1}{2}(F_{n-3} + F_{n-2}) + F_{n-2} + \frac{1}{2}F_{n-1} \\ &= \frac{1}{2}F_{n-1} + F_{n-2} + \frac{1}{2}F_{n-1} \\ &= F_{n-2} + F_{n-1} = F_n. \end{aligned}$$

13. We use strong induction. Suppose $n \in \mathbb{N}$ and for all $k < n$, P_k has F_{k+2} elements.

    Case 1. $n = 0$. $P_0 = \{\varnothing\}$, which has 1 element, and $F_{n+2} = F_2 = 1$.

    Case 2. $n = 1$. $P_1 = \{\varnothing, \{1\}\}$, which has 2 elements, and $F_{n+2} = F_3 = 2$.

    Case 3. $n \geq 2$. The elements of P_n that don't contain n are the elements of P_{n-1}, and by inductive hypothesis there are F_{n+1} of them. If an element of P_n contains n, then since it cannot contain consecutive integers, it must not contain $n - 1$. Therefore it must have the form $X \cup \{n\}$, where $X \in P_{n-2}$, and every set of this form will be in P_n. The number of such sets is F_n, since by inductive hypothesis that is the number of possibilities for X. Therefore the number of elements of P_n is $F_{n+1} + F_n = F_{n+2}$.

14. (a) If $n \geq 0$ then the result follows from the division algorithm, Theorem 6.4.1. Now suppose $n < 0$. Then $-n - 1 \geq 0$, so we can apply Theorem 6.4.1 to $-n - 1$ and m to conclude that there are natural numbers q' and r' such that $-n - 1 = q'm + r'$ and $0 \leq r' < m$, so $0 \leq r' \leq m - 1$. Therefore $n = -q'm - r' - 1 = (-q' - 1)m + (m - 1 - r')$. Let $q = -q' - 1$ and $r = m - 1 - r'$. Then q and r are integers, $n = qm + r$, and since $0 \leq r' \leq m - 1$, $0 \leq r \leq m - 1 < m$.

(b) Suppose $n = qm + r = q'm + r'$, where q, r, q', and r' are integers, $0 \le r < m$, and $0 \le r' < m$. Then $(q - q')m = r' - r$ and $-m < r' - r < m$, so $-m < (q - q')m < m$. Dividing by m, we get $-1 < q - q' < 1$. Since the only integer between -1 and 1 is 0, we must have $q - q' = 0$. Therefore $q = q'$, and $r' - r = (q - q')m = 0$, so $r = r'$.

(c) Suppose n is an integer. By part (a), there are integers q and r such that $n = 3q + r$ ands $0 \le r < 3$, so $r \in \{0, 1, 2\}$. Therefore $n - r = 3q$, so $n \equiv r \pmod 3$. This proves that at least one of the three statements is true. To show that only one statement is true, suppose that $n \equiv r_1 \pmod 3$ and $n \equiv r_2 \pmod 3$, where $r_1, r_2 \in \{0, 1, 2\}$. Then there are integers q_1 and q_2 such that $n - r_1 = 3q_1$ and $n - r_2 = 3q_2$. Therefore $n = 3q_1 + r_1 = 3q_2 + r_2$, and by part (b) it follows that $r_1 = r_2$.

15. Let a be the larger of $5k$ and $k(k + 1)$. Now suppose $n > a$, and by the division algorithm choose q and r such that $n = qk + r$ and $0 \le r < k$. Note that if $q \le 4$ then $n = qk + r \le 4k + r < 5k \le a$, which is a contradiction. Therefore $q > 4$, so $q \ge 5$, and by Example 6.1.3 it follows that $2^q \ge q^2$. Similar reasoning shows that $q \ge k + 1$, so $q^2 \ge q(k + 1) = qk + q > qk + k > qk + r = n$. Therefore $2^n \ge 2^{qk} = (2^q)^k \ge (q^2)^k \ge n^k$.

16. (a) We use induction on k.

Base case: $k = 1$. Suppose $f_1 \in O(g)$ and a_1 is a real number, and let $f(n) = a_1 f_1(n)$. We must prove that $f \in O(g)$. Since $f_1 \in O(g)$, we can choose $a \in \mathbb{Z}^+$ and $c \in \mathbb{R}^+$ such that for all $n > a$, $|f_1(n)| \le c|g(n)|$. Let $c' = (|a_1| + 1)c \in \mathbb{R}^+$. Then for all $n > a$, $|f(n)| = |a_1||f_1(n)| \le (|a_1| + 1)c|g(n)| = c'|g(n)|$, so $f \in O(g)$.

Induction step: Assume the statement holds for k, and suppose f_1, f_2, ..., f_{k+1} are elements of $O(g)$ and a_1, a_2, ..., a_{k+1} are real numbers. Let $h(n) = a_1 f_1(n) + a_2 f_2(n) + \cdots + a_k f_k(n)$ and $f(n) = a_1 f_1(n) + a_2 f_2(n) + \cdots + a_{k+1} f_{k+1}(n) = h(n) + a_{k+1} f_{k+1}(n)$. Then by inductive hypothesis, $h \in O(g)$, and therefore by exercise 19(c) of Section 5.1, $f \in O(g)$.

17. We will prove by induction that for all $n \in \mathbb{N}$, $a_n = 2^n$.

Base case: When $n = 0$, $a_n = a_0 = 1 = 2^0 = 2^n$.

Induction step: Suppose $n \in \mathbb{N}$ and $a_n = 2^n$. If $n = 0$ then $a_{n+1} = a_1 = 1 + a_0 = 1 + 1 = 2 = 2^1 = 2^{n+1}$. Now suppose $n \ge 1$. Then

$$a_{n+1} = 1 + \sum_{i=0}^{n} a_i = 1 + \sum_{i=0}^{n-1} a_i + a_n = a_n + a_n = 2a_n = 2 \cdot 2^n = 2^{n+1}.$$

(Note: An alternative approach is to use strong induction and apply Example 6.1.1.)

18. We will prove by induction that for all $n \in \mathbb{N}$, $a_n = F_{n+2}/F_{n+1}$.

Base case: When $n = 0$, $a_n = a_0 = 1 = 1/1 = F_2/F_1 = F_{n+2}/F_{n+1}$.

Induction step: Suppose $n \in \mathbb{N}$ and $a_n = F_{n+2}/F_{n+1}$. Then

$$a_{n+1} = 1 + \frac{1}{a_n} = 1 + \frac{F_{n+1}}{F_{n+2}} = \frac{F_{n+2} + F_{n+1}}{F_{n+2}} = \frac{F_{n+3}}{F_{n+2}}.$$

19. (a) We first prove the following lemma.

Lemma. *For every integer n, if $n \not\equiv 0 \pmod 3$ then $n^2 \equiv 1 \pmod 3$.*

Proof. Suppose n is an integer and $n \not\equiv 0 \pmod 3$. Then by exercise 14(c), either $n \equiv 1 \pmod 3$ or $n \equiv 2 \pmod 3$.

Case 1. $n \equiv 1 \pmod 3$. Then there is some integer k such that $n - 1 = 3k$, so $n = 3k + 1$. Therefore $n^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$, so $n^2 - 1 = 3(3k^2 + 2k)$ and $n^2 \equiv 1 \pmod 3$.

Case 2. $n \equiv 2 \pmod 3$. Then there is some integer k such that $n = 3k + 2$, so $n^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$ and therefore $n^2 \equiv 1 \pmod 3$. □

Now, to solve the problem, suppose m and n are integers and $3 \mid (m^2+n^2)$. Then $m^2+n^2 \equiv 0 \pmod 3$. Suppose $m \not\equiv 0 \pmod 3$. Then by the lemma, $m^2 \equiv 1 \pmod 3$, so there is some integer j such that $m^2 = 3j+1$.

Case 1. $n \equiv 0 \pmod 3$. Then there is some integer k such that $n = 3k$. Therefore $m^2+n^2 = 3j+1+9k^2 = 3(j+3k^2)+1$, so $m^2+n^2 \equiv 1 \pmod 3$. By exercise 14(c), this contradicts the fact that $m^2+n^2 \equiv 0 \pmod 3$.

Case 2. $n \not\equiv 0 \pmod 3$. Then by the lemma $n^2 \equiv 1 \pmod 3$, so there is some integer k such that $n^2 = 3k+1$. Therefore $m^2+n^2 = 3j+1+3k+1 = 3(j+k)+2$, so $m^2+n^2 \equiv 2 \pmod 3$. Once again, by exercise 14(c), this contradicts $m^2+n^2 \equiv 0 \pmod 3$.

Thus it is not possible that $m \not\equiv 0 \pmod 3$, so $m \equiv 0 \pmod 3$ and therefore $3 \mid m$. A similar argument shows that $3 \mid n$.

(b) Adding the two equations in $(*)$ we get $c^2+d^2 = 3a^2+3b^2 = 3(a^2+b^2)$. Therefore $3 \mid (c^2+d^2)$, so by part (a), $3 \mid c$ and $3 \mid d$.

(c) By part (b), there are positive integers j and k such that $c = 3j$ and $d = 3k$. Therefore adding the equations in $(*)$ gives $3a^2+3b^2 = c^2+d^2 = 9j^2+9k^2$. Dividing by 3, we get $a^2+b^2 = 3(j^2+k^2)$, so $3 \mid (a^2+b^2)$ and by part (a), $3 \mid a$ and $3 \mid b$.

(d) By part (c), there are positive integers s and t such that $a = 3s$ and $b = 3t$. Substituting into $(*)$ we get

$$9s^2+18t^2 = 9j^2, \qquad 18s^2+9t^2 = 9k^2.$$

Dividing both equations by 9 gives us

$$s^2+2t^2 = j^2, \qquad 2s^2+t^2 = k^2.$$

Therefore $k \in S$. But $d = 3k > k$, so this contradicts the choice of d as the *smallest* element of S.

20. (a) Let $x = BC$ and $y = BE$. Then $AE = EF = BC = x$, so $AB = AE+BE = x+y$. The equality of ratios in the problem is then

$$\frac{x}{y} = \frac{x+y}{x} = 1+\frac{y}{x}.$$

If we let $r = x/y$, then the equation is $r = 1+1/r$. Multiplying by r, we get $r^2 = r+1$, so $r^2-r-1 = 0$. The quadratic formula now gives us $r = (1 \pm \sqrt{5})/2$. Since r is clearly positive, we must have $r = (1+\sqrt{5})/2 = \varphi$.

(b) We write all angles in degrees but drop the degree sign. Let $x = \cos(36)$. We use several trigonometric identities:

$$\begin{aligned}
\cos(108) &= \cos(180-72) = -\cos(72),\\
\cos(72) &= \cos(2\cdot 36) = 2\cos^2(36)-1 = 2x^2-1,\\
\cos(108) &= \cos(36+72) = \cos(36)\cos(72)-\sin(36)\sin(2\cdot 36)\\
&= x(2x^2-1)-2\sin^2(36)\cos(36) = 2x^3-x-2(1-\cos^2(36))\cos(36)\\
&= 2x^3-x-2(1-x^2)x = 4x^3-3x.
\end{aligned}$$

The equation $\cos(108) = -\cos(72)$ now gives us $4x^3-3x = -2x^2+1$, so

$$4x^3+2x^2-3x-1 = 0. \qquad (*)$$

Since $4x^3+2x^2-3x-1 = (x+1)(4x^2-2x-1)$, by the quadratic formula the solutions to $(*)$ are

$$x = -1, \quad x = \frac{2+\sqrt{20}}{8} = \frac{1+\sqrt{5}}{4} \approx 0.809, \quad x = \frac{2-\sqrt{20}}{8} = \frac{1-\sqrt{5}}{4} \approx -0.309.$$

Since $0 < x < 1$, the only possibility is $x = (1+\sqrt{5})/4 = \varphi/2$.

(c) By Example 6.2.3, the angles in the pentagon $ABCDE$, measured in degrees, add up to $3 \cdot 180 = 540$, and therefore $\angle ABC = 540/5 = 108$. Since $\triangle ABC$ is isosceles, $\angle BAC = \angle BCA = 36$. Let M be the midpoint of AC. Then $\triangle AMB$ is a right triangle, and $AM = \cos(36)$. Similarly, $MC = \cos(36)$, so by part (b), $AC = 2\cos(36) = \varphi$.

21. (a) For any numbers a, b, c, and d,

$$\begin{aligned}
(ab)(cd) &= (cd)(ab) && \text{(commutative law)}\\
&= c(d(ab)) && \text{(associative law)}\\
&= c((da)b) && \text{(associative law)}\\
&= c((ad)b) && \text{(commutative law).}
\end{aligned}$$

(b) To simplify notation, we will assume that any product is the left-grouped product unless parentheses are used to indicate otherwise. We use strong induction on n. Assume the statement is true for products of fewer than n terms, and consider any product of $a_1, a_2, \ldots, a_n$. If $n = 1$, then the only product is the left-grouped product, so there is nothing to prove. Now suppose $n > 1$. Then our product has the form pq, where p is a product of $a_1, \ldots, a_{k-1}$ and q is a product of $a_k, \ldots, a_n$ for some k with $2 \le k \le n$. By inductive hypothesis, $p = a_1 \cdots a_{k-1}$ and $q = a_k \cdots a_n$ (where by our convention, these two products are left-grouped). Thus, it will suffice to prove $(a_1 \cdots a_{k-1})(a_k \cdots a_n) = a_1 \cdots a_n$. If $k = n$, then the left-hand side of this equation is already left-grouped, so there is nothing to prove. If $k < n$, then

$$\begin{aligned}
&(a_1 \cdots a_{k-1})(a_k \cdots a_n)\\
&\quad = (a_1 \cdots a_{k-1})((a_k \cdots a_{n-1})a_n) && \text{(definition of left-grouped)}\\
&\quad = ((a_1 \cdots a_{k-1})(a_k \cdots a_{n-1}))a_n && \text{(associative law)}\\
&\quad = (a_1 \cdots a_{n-1})a_n && \text{(inductive hypothesis)}\\
&\quad = a_1 \cdots a_n && \text{(definition of left-grouped).}
\end{aligned}$$

(c) By part (b), we may assume that the two products are left-grouped. Thus, we must prove that if $b_1, b_2, \ldots, b_n$ is some reordering of $a_1, a_2, \ldots, a_n$, then $a_1 \cdots a_n = b_1 \cdots b_n$, where as in part (b) we assume products are left-grouped unless parentheses indicate otherwise. We use induction on n. If $n = 1$ then the products are clearly equal because $b_1 = a_1$. Now suppose the statement is true for products of length n, and suppose that $b_1, \ldots, b_{n+1}$ is a reordering of $a_1, \ldots, a_{n+1}$. Then b_{n+1} is one of $a_1, \ldots, a_{n+1}$. If $b_{n+1} = a_{n+1}$ then

$$\begin{aligned}
b_1 \cdots b_{n+1} &= (b_1 \cdots b_n)a_{n+1} && \text{(definition of left-grouped)}\\
&= (a_1 \cdots a_n)a_{n+1} && \text{(inductive hypothesis)}\\
&= a_1 \cdots a_{n+1} && \text{(definition of left-grouped).}
\end{aligned}$$

Now suppose $b_{n+1} = a_k$ for some $k \le n$. We will write $a_1 \cdots \widehat{a_k} \cdots a_n$ for the (left-grouped) product of the numbers $a_1, \ldots, a_n$ with the factor a_k left out. Then

$$\begin{aligned}
b_1 \cdots b_{n+1} &= (b_1 \cdots b_n)a_k && \text{(definition of left-grouped)}\\
&= (a_1 \cdots \widehat{a_k} \cdots a_{n+1})a_k && \text{(inductive hypothesis)}\\
&= ((a_1 \cdots \widehat{a_k} \cdots a_n)a_{n+1})a_k && \text{(definition of left-grouped)}\\
&= (a_1 \cdots \widehat{a_k} \cdots a_n)(a_{n+1}a_k) && \text{(associative law)}\\
&= (a_1 \cdots \widehat{a_k} \cdots a_n)(a_k a_{n+1}) && \text{(commutative law)}\\
&= ((a_1 \cdots \widehat{a_k} \cdots a_n)a_k)a_{n+1} && \text{(associative law)}\\
&= (a_1 \cdots a_n)a_{n+1} && \text{(inductive hypothesis)}\\
&= a_1 \cdots a_{n+1} && \text{(definition of left-grouped).}
\end{aligned}$$

Section 6.5

1. For all n, $B_n = \{n\}$. We prove this by induction.
   Base case: If $n = 0$, then $B_n = B_0 = B = \{0\} = \{n\}$.
   Induction step: Suppose $n \in \mathbb{N}$ and $B_n = \{n\}$. Then $B_{n+1} = f(B_n) = \{f(n)\} = \{n + 1\}$.

2. For all n, $B_n = \{x \in \mathbb{Z} \mid x \geq -n\}$. We prove this by induction.
   Base case: If $n = 0$, then $B_n = B_0 = B = \mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 0\}$.
   Induction step. Suppose $n \in \mathbb{N}$ and $B_n = \{x \in \mathbb{Z} \mid x \geq -n\}$. Suppose $c \in B_{n+1} = f(B_n)$. Then there is some $b \in B_n$ such that $c = f(b) = b - 1$. Since $b \in B_n$, $b \in \mathbb{Z}$ and $b \geq -n$. Therefore $b - 1 \in \mathbb{Z}$ and $b - 1 \geq -n - 1 = -(n + 1)$, so $c = b - 1 \in \{x \in \mathbb{Z} \mid x \geq -(n + 1)\}$. Next, suppose $c \in \{x \in \mathbb{Z} \mid x \geq -(n + 1)\}$. Then $c \in \mathbb{Z}$ and $c \geq -(n + 1) = -n - 1$. Let $b = c + 1$. Then $b \in \mathbb{Z}$ and $b \geq -n$, so $b \in \{x \in \mathbb{Z} \mid x \geq -n\} = B_n$, and $c = b - 1 = f(b) \in f(B_n) = B_{n+1}$. This proves that $B_{n+1} = \{x \in \mathbb{Z} \mid x \geq -(n + 1)\}$.

3. Let $C = \bigcup_{n\in\mathbb{N}} B_n$. Since every element of $\mathcal{F}$ is a function from A to A, it is not hard to see that for every n, $B_n \subseteq A$ (try proving it by induction), so $C \subseteq A$. It is also clear that $B = B_0 \subseteq C$. To see that C is closed under every function $f \in \mathcal{F}$, suppose $f \in \mathcal{F}$ and $x \in C$. Since $C = \bigcup_{n\in\mathbb{N}} B_n$, we can choose some $n \in \mathbb{N}$ such that $x \in B_n$. Therefore $f(x) \in f(B_n) \subseteq B_{n+1} \subseteq C$. Finally, suppose $B \subseteq D \subseteq A$ and D is closed under every function $f \in \mathcal{F}$. We claim that for every $n \in \mathbb{N}$, $B_n \subseteq D$, from which it will follow that $C \subseteq D$. We prove this by induction on n. For the base case, $B_0 = B \subseteq D$ by assumption. Now suppose $B_n \subseteq D$ and $x \in B_{n+1}$. Then by the definition of B_{n+1}, there is some $f \in \mathcal{F}$ such that $x \in f(B_n)$, which means that $x = f(b)$ for some $b \in B_n$. By the inductive hypothesis, $B_n \subseteq D$, so $b \in D$. Since D is closed under f, $x = f(b) \in D$.

4. $B_0 = \{\varnothing\}$, $B_1 = \{X \in \mathscr{P}(\mathbb{N}) \mid X \text{ has exactly one element}\}$, $B_2 = \{X \in \mathscr{P}(\mathbb{N}) \mid X \text{ has either one or two elements}\}$, ... In general, for every positive integer n, $B_n = \{X \in \mathscr{P}(\mathbb{N}) \mid X \neq \varnothing \text{ and } X \text{ has at most } n \text{ elements}\}$. We prove this last statement by induction on n.
   Base case: When $n = 1$ we have $B_n = B_1 = \{f_k(\varnothing) \mid k \in \mathbb{N}\} = \{\{k\} \mid k \in \mathbb{N}\} = \{X \in \mathscr{P}(\mathbb{N}) \mid X \text{ has exactly one element}\}$.
   Induction step: Suppose $n \geq 1$ and $B_n = \{X \in \mathscr{P}(\mathbb{N}) \mid X \neq \varnothing \text{ and } X \text{ has at most } n \text{ elements}\}$. Now suppose $Y \in B_{n+1}$. Then for some $k \in \mathbb{N}$ and $Z \in B_n$, $Y = f_k(Z) = Z \cup \{k\}$. The number of elements of Y is either the same as the number of elements in Z (if $k \in Z$), or one larger (if $k \notin Z$). Since $Z \in B_n$, by inductive hypothesis, $Z \neq \varnothing$ and Z has at most n elements. Therefore $Y \neq \varnothing$ and Y has at most $n + 1$ elements, so $Y \in \{X \in \mathscr{P}(\mathbb{N}) \mid X \neq \varnothing \text{ and } X \text{ has at most } n + 1 \text{ elements}\}$. Now suppose $Y \in \{X \in \mathscr{P}(\mathbb{N}) \mid X \neq \varnothing \text{ and } X \text{ has at most } n + 1 \text{ elements}\}$. Then $Y \neq \varnothing$, so we can choose some $k \in Y$. If Y has fewer than $n + 1$ elements, then $Y \in B_n$ and $Y = f_k(Y)$, so $Y \in B_{n+1}$. If Y has $n + 1$ elements, then $Y \setminus \{k\} \in B_n$ and $Y = f_k(Y \setminus \{k\})$, and again we conclude that $Y \in B_{n+1}$. Thus $B_{n+1} = \{X \in \mathscr{P}(\mathbb{N}) \mid X \neq \varnothing \text{ and } X \text{ has at most } n + 1 \text{ elements}\}$.

5. The closure is the set $C = \{n \in \mathbb{Z} \mid n \geq 2\}$. It is clear that C is closed under f. By Theorem 6.4.2, every element of C is either prime or is a product of primes, so every element of C must be in any set that contains P and is closed under f.

6. The mistake is the sentence "Then by the definition of C, there is some $m \in \mathbb{N}$ such that $x, y \in B_m$." The correct conclusion is that there are $m, n \in \mathbb{N}$ such that $x \in B_m$ and $y \in B_n$.

7. (a) $B_0 = \{x \in \mathbb{R} \mid -2 \leq x \leq 0\}$, $B_1 = \{x \in \mathbb{R} \mid 0 \leq x \leq 4\}$, $B_2 = \{x \in \mathbb{R} \mid 0 \leq x \leq 16\}$, ... In general, for every positive integer n, $B_n = \{x \in \mathbb{R} \mid 0 \leq x \leq 2^{(2^n)}\}$.
   (b) $\bigcup_{n\in\mathbb{N}} B_n = \{x \in \mathbb{R} \mid x \geq -2\}$. Therefore $-1, 3 \in \bigcup_{n\in\mathbb{N}} B_n$ but $f(-1, 3) = -3 \notin \bigcup_{n\in\mathbb{N}} B_n$, so $\bigcup_{n\in\mathbb{N}} B_n$ is not closed under f. In other words, property 2 in Definition 5.4.8 does not hold.
   (c) The closure is $\mathbb{R}$. To see why, suppose $B \subseteq D \subseteq \mathbb{R}$ and D is closed under f. Then for all $n \in \mathbb{N}$, $B_n \subseteq D$ (that part of the proof in exercise 6 is correct), so $\bigcup_{n\in\mathbb{N}} B_n = \{x \in \mathbb{R} \mid x \geq -2\} \subseteq D$.

But now for any negative real number x, $-x \in D$ and $-1 \in D$, so since D is closed under f, $x = f(-x, -1) \in D$. Thus $\mathbb{R} \subseteq D$.

8. (a) Let m be an arbitrary natural number. We now prove by induction that for all $n \geq m$, $B_m \subseteq B_n$.
Base case: $n = m$. Then $B_m \subseteq B_m = B_n$.
Induction step: Suppose $n \geq m$ and $B_m \subseteq B_n$. Clearly $B_n \subseteq B_n \cup f(B_n \times B_n) = B_{n+1}$, so $B_m \subseteq B_{n+1}$.

(b) Let $C = \bigcup_{n \in \mathbb{N}} B_n$. It is not hard to see that each set B_n is a subset of A, so $C \subseteq A$, and $B = B_0 \subseteq C$.
To see that C is closed under f, suppose $x, y \in C$. Then by the definition of C, there are $m, n \in \mathbb{N}$ such that $x \in B_m$ and $y \in B_n$. If $m \leq n$ then, by part (a), $B_m \subseteq B_n$, so $x \in B_n$. Therefore $f(x, y) \in f(B_n \times B_n) \subseteq B_{n+1}$, so $f(x, y) \in C$. A similar argument applies if $m > n$.
Finally, suppose $B \subseteq D \subseteq A$ and D is closed under f. To prove that $C \subseteq D$, it will suffice to prove that $\forall n \in \mathbb{N}(B_n \subseteq D)$. We prove this by induction. The base case holds because $B_0 = B \subseteq D$ by assumption. For the induction step, suppose $B_n \subseteq D$ and let $x \in B_{n+1}$ be arbitrary. By the definition of B_{n+1} either $x \in B_n$ or $x = f(a, b)$ for some $a, b \in B_n$. In the first case, $x \in D$ because by inductive hypothesis, $B_n \subseteq D$. In the second case, $a, b \in D$, so since D is closed under f, $x = f(a, b) \in D$. Therefore $B_{n+1} \subseteq D$.

9. If $B = \varnothing$ then for all $n \in \mathbb{N}$, $B_n = \varnothing$, so the closure is $\varnothing$. If $B \neq \varnothing$ then $B_0 = B$ and for all $n \geq 1$, $B_n = \{c\}$; the closure is $B \cup \{c\}$.

10. We use induction on n.
Base case: $n = 1$. Then $x = 2! + 2 = 4$. The only value of i we have to worry about is $i = 0$, and for this value of i we have $i + 2 = 2$ and $x + i = 4$. Since $2 \mid 4$, we have $(i + 2) \mid (x + i)$, as required.
Induction step: Suppose that n is a positive integer, and for every integer i, if $0 \leq i \leq n - 1$ then $(i + 2) \mid ((n + 1)! + 2 + i)$. Now let $x = (n + 2)! + 2$, and suppose that $0 \leq i \leq n$. If $i = n$ then we have

$$x + i = (n + 2)! + 2 + i = (i + 2)! + (i + 2) = (i + 2)((i + 1)! + 1),$$

so $(i + 2) \mid (x + i)$. Now suppose $0 \leq i \leq n - 1$. By inductive hypothesis, we know that $(i + 2) \mid ((n + 1)! + 2 + i)$, so we can choose some integer k such that $(n + 1)! + 2 + i = k(i + 2)$, and therefore $(n + 1)! = (k - 1)(i + 2)$. Therefore

$$\begin{aligned} x + i &= (n + 2)! + 2 + i = (n + 2)(n + 1)! + (i + 2) \\ &= (n + 2)(k - 1)(i + 2) + (i + 2) = (i + 2)((n + 2)(k - 1) + 1), \end{aligned}$$

so $(i + 2) \mid (x + i)$.

11. Let m be an arbitrary positive integer. We now prove by induction that for all $n \in \mathbb{Z}^+$, $R^{m+n} = R^m \circ R^n$.
Base case: $n = 1$. By definition, $R^{m+n} = R^{m+1} = R^m \circ R = R^m \circ R^1 = R^m \circ R^n$.
Induction step: Suppose $n \in \mathbb{Z}^+$ and $R^{m+n} = R^m \circ R^n$. Then

$$\begin{aligned} R^{m+n+1} &= R^{m+n} \circ R && \text{(definition of } R^{m+n+1}\text{)} \\ &= (R^m \circ R^n) \circ R && \text{(inductive hypothesis)} \\ &= R^m \circ (R^n \circ R) && \text{(associativity of } \circ\text{: Theorem 4.2.5, part 4)} \\ &= R^m \circ R^{n+1} && \text{(definition of } R^{n+1}\text{)}. \end{aligned}$$

12. (a) We use induction.
Base case: If $n = 1$, then $f^n = f$, which is a function from A to A by assumption.
Induction step: Suppose $n \in \mathbb{Z}^+$ and $f^n : A \to A$. Then by Theorem 5.1.5, since $f^{n+1} = f^n \circ f$, $f^{n+1} : A \to A$.

(b) We use induction.

Base case: If $n = 1$, then $f^n(B) = f(B_0) = B_1 = B_n$.

Induction step: Suppose $n \in \mathbb{Z}^+$ and $f^n(B) = B_n$. Then by exercise 11, $f^{n+1} = f^{1+n} = f^1 \circ f^n = f \circ f^n$. Therefore, by our solution to exercise 6 in Section 5.5, $f^{n+1}(B) = (f \circ f^n)(B) = f(f^n(B)) = f(B_n) = B_{n+1}$.

13. (a) Suppose a is a periodic point for f. Then for some positive integer n, $f^n(a) = a$. Let $D = \{f(a), f^2(a), \ldots, f^n(a)\}$, which is a finite set. Notice that $a = f^n(a) \in D$, so $\{a\} \subseteq D$. Suppose $x \in D$. Then for some $k \in \{1, 2, \ldots, n\}$, $x = f^k(a)$. If $k < n$ then $f(x) = f(f^k(a)) = (f^1 \circ f^k)(a) = f^{k+1}(a) \in D$. If $k = n$ then $x = f^n(a) = a$, so $f(x) = f(a) \in D$. Thus, D is closed under f. By definition, the closure of $\{a\}$ under f must be a subset of D, so it is finite.

(b) No. Counterexample: $f : \mathbb{R} \to \mathbb{R}$, $f(x) = |x|$, $a = -1$.

14. Clearly T is a relation on A and $R = R^1 \subseteq T$. To see that T is transitive, suppose $(x, y) \in T$ and $(y, z) \in T$. Then by the definition of T, we can choose positive integers n and m such that $(x, y) \in R^n$ and $(y, z) \in R^m$. Thus by exercise 11, $(x, z) \in R^m \circ R^n = R^{m+n}$, so $(x, z) \in \bigcup_{n \in \mathbb{Z}^+} R^n = T$. Therefore T is transitive.

Finally, suppose $R \subseteq S \subseteq A \times A$ and S is transitive. We must show that $T \subseteq S$, and clearly by the definition of T it suffices to show that $\forall n \in \mathbb{Z}^+(R^n \subseteq S)$. We prove this by induction on n. We have assumed $R \subseteq S$, so when $n = 1$ we have $R^n = R^1 = R \subseteq S$. For the induction step, suppose n is a positive integer and $R^n \subseteq S$. Now suppose $(x, y) \in R^{n+1}$. Then by definition of R^{n+1} we can choose some $z \in A$ such that $(x, z) \in R$ and $(z, y) \in R^n$. By assumption $R \subseteq S$, and by inductive hypothesis $R^n \subseteq S$. Therefore $(x, z) \in S$ and $(z, y) \in S$, so since S is transitive, $(x, y) \in S$. Since (x, y) was an arbitrary element of R^{n+1}, this shows that $R^{n+1} \subseteq S$.

15. We use induction.

Base case: $n = 1$. Then $R^n = R \subseteq S = S^n$.

Induction step: Suppose $n \in \mathbb{Z}^+$ and $R^n \subseteq S^n$. Suppose $(x, y) \in R^{n+1} = R^n \circ R$. Then we can choose some $z \in A$ such that $(x, z) \in R$ and $(z, y) \in R^n$. Since $R \subseteq S$ and $R^n \subseteq S^n$, $(x, z) \in S$ and $(z, y) \in S^n$. Therefore $(x, y) \in S^n \circ S = S^{n+1}$. Since (x, y) was arbitrary, $R^{n+1} \subseteq S^{n+1}$.

16. (a) $R \cap S \subseteq R$ and $R \cap S \subseteq S$. Therefore by exercise 15, for every positive integer n, $(R \cap S)^n \subseteq R^n$ and $(R \cap S)^n \subseteq S^n$, so $(R \cap S)^n \subseteq R^n \cap S^n$. However, the two need not be equal. For example, if $A = \{1, 2, 3, 4\}$, $R = \{(1, 2), (2, 4)\}$, and $S = \{(1, 3), (3, 4)\}$, then $(R \cap S)^2 = \varnothing$ but $R^2 \cap S^2 = \{(1, 4)\}$.

(b) $R \subseteq R \cup S$ and $S \subseteq R \cup S$. Therefore by exercise 15, for every positive integer n, $R^n \subseteq (R \cup S)^n$ and $S^n \subseteq (R \cup S)^n$, so $R^n \cup S^n \subseteq (R \cup S)^n$. However, the two need not be equal. Counterexample: $A = \{1, 2, 3\}$, $R = \{(1, 2)\}$, $S = \{(2, 3)\}$.

17. (a) Let $m = d(a, b)$ and $n = d(b, c)$. Then $(a, b) \in R^m$ and $(b, c) \in R^n$, so by exercise 11, $(a, c) \in R^n \circ R^m = R^{m+n}$. Therefore $d(a, c) \leq m + n = d(a, b) + d(b, c)$.

(b) Let $n = d(a, c)$. Then $(a, c) \in R^n = R^{(n-m)+m} = R^{n-m} \circ R^m$, so there is some $b \in A$ such that $(a, b) \in R^m$ and $(b, c) \in R^{n-m}$. Therefore $d(a, b) \leq m$ and $d(b, c) \leq n - m$. If either $d(a, b) < m$ or $d(b, c) < n - m$ then $d(a, b) + d(b, c) < m + n - m = n = d(a, c)$, which would contradict part (a). Therefore $d(a, b) = m$ and $d(b, c) = n - m = d(a, c) - m$.

18. (a) We use induction.

Base case: $n = 1$. Suppose $(a, b) \in R^1 = R$. Let $f = \{(0, a), (1, b)\}$. Then f is an R-path from a to b of length 1. For the other direction, suppose f is an R-path from a to b of length 1. By the definition of R-path, this means that $f(0) = a$, $f(1) = b$, and $(f(0), f(1)) \in R$. Therefore $(a, b) \in R = R^1$.

Induction step: Suppose n is a positive integer and $R^n = \{(a, b) \in A \times A \mid$ there is an R-path from a to b of length $n\}$. Now suppose $(a, b) \in R^{n+1} = R^1 \circ R^n$ by exercise 11. Then there

is some c such that $(a, c) \in R^n$ and $(c, b) \in R$. By inductive hypothesis, there is an R-path f from a to c of length n. Then $f \cup \{(n+1, b)\}$ is an R-path from a to b of length $n+1$. For the other direction, suppose f is an R-path from a to b of length $n+1$. Let $c = f(n)$. Then $f \setminus \{(n+1, b)\}$ is an R-path from a to c of length n, so by inductive hypothesis $(a, c) \in R^n$. But also $(c, b) = (f(n), f(n+1)) \in R$, so $(a, b) \in R^1 \circ R^n = R^{n+1}$.

(b) This follows from part (a) and exercise 14.

19. (a) Suppose f is an R-path from a to b of length n, but f is not one-to-one. Then we can choose i and j such that $0 \le i < j \le n$ and $f(i) = f(j)$. Let

$$g = \{(0, f(0)), (1, f(1)), \ldots, (i, f(i)) = (i, f(j)), (i+1, f(j+1)), \ldots, (i+n-j, f(n))\}.$$

Notice that since $a \neq b$, it cannot be the case that $i = 0$ and $j = n$, so either $i \ge 1$ or $j \le n-1$, and therefore $i + n - j \ge 1$. It is not hard to check that g is an R-path from a to b of length $i+n-j < n$, so by exercise 18(a), $(a, b) \in R^{i+n-j}$. But this contradicts the definition of $n = d(a, b)$ as the *smallest* positive integer m such that $(a, b) \in R^m$.

(b) Suppose f is an R-path from a to a of length n and it is not the case that $\forall i < n \forall j < n(f(i) = f(j) \to i = j)$. Then we can choose i and j so that $0 \le i < j < n$ and $f(i) = f(j)$. Now the same method as in part (a) can be used to construct an R-path from a to a of length $i + n - j$, contradicting the definition of $d(a, a)$.

20. By exercise 14, $\bigcup\{R^n \mid 1 \le n \le m\} \subseteq \bigcup_{n \in \mathbb{Z}^+} R^n = T$, so we just need to prove $T \subseteq \bigcup\{R^n \mid 1 \le n \le m\}$.

Suppose $(a, b) \in T$. Let $n = d(a, b)$. Then $(a, b) \in R^n$, so by exercise 18(a), we can let f be an R-path from a to b of length n. By exercise 19, $f(0)$, $f(1)$, $\ldots$, $f(n-1)$ are n distinct elements of A. But A has only m elements, so $n \le m$. Therefore $(a, b) \in \bigcup\{R^n \mid 1 \le n \le m\}$.

Chapter 7

Section 7.1

1. (a) $D(a) = D(57) = \{1, 3, 19, 57\}$, $D(b) = D(36) = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$, $D(a) \cap D(b) = \{1, 3\}$.

(b) The Euclidean algorithm shows that $\gcd(57, 36) = 3$. Here are the steps:

n	q_n	r_n	Division
0		57	
1		36	$57 = 1 \cdot 36 + 21$
2	1	21	$36 = 1 \cdot 21 + 15$
3	1	15	$21 = 1 \cdot 15 + 6$
4	1	6	$15 = 2 \cdot 6 + 3$
5	2	3	$6 = 2 \cdot 3 + 0$
6	2	0	

2. (a) The extended Euclidean algorithm shows that $\gcd(775, 682) = 31 = -7 \cdot 775 + 8 \cdot 682$:

n	q_n	r_n	s_n	t_n	Division
0		775	1	0	
1		682	0	1	$775 = 1 \cdot 682 + 93$
2	1	93	$1 - 1 \cdot 0 = 1$	$0 - 1 \cdot 1 = -1$	$682 = 7 \cdot 93 + 31$
3	7	31	$0 - 7 \cdot 1 = -7$	$1 - 7 \cdot (-1) = 8$	$93 = 3 \cdot 31 + 0$
4	3	0			

(b) The extended Euclidean algorithm shows that $\gcd(562, 243) = 1 = 16 \cdot 562 - 37 \cdot 243$:

n	q_n	r_n	s_n	t_n	Division
0		562	1	0	
1		243	0	1	$562 = 2 \cdot 243 + 76$
2	2	76	$1 - 2 \cdot 0 = 1$	$0 - 2 \cdot 1 = -2$	$243 = 3 \cdot 76 + 15$
3	3	15	$0 - 3 \cdot 1 = -3$	$1 - 3 \cdot (-2) = 7$	$76 = 5 \cdot 15 + 1$
4	5	1	$1 - 5 \cdot (-3) = 16$	$-2 - 5 \cdot 7 = -37$	$15 = 15 \cdot 1 + 0$
5	15	0			

3. (a) The extended Euclidean algorithm shows that $\gcd(2790, 1206) = 18 = 16 \cdot 2790 - 37 \cdot 1206$:

n	q_n	r_n	s_n	t_n	Division
0		2790	1	0	
1		1206	0	1	$2790 = 2 \cdot 1206 + 378$
2	2	378	$1 - 2 \cdot 0 = 1$	$0 - 2 \cdot 1 = -2$	$1206 = 3 \cdot 378 + 72$
3	3	72	$0 - 3 \cdot 1 = -3$	$1 - 3 \cdot (-2) = 7$	$378 = 5 \cdot 72 + 18$
4	5	18	$1 - 5 \cdot (-3) = 16$	$-2 - 5 \cdot 7 = -37$	$72 = 4 \cdot 18 + 0$
5	4	0			

(b) The extended Euclidean algorithm shows that $\gcd(191, 156) = 1 = -49 \cdot 191 + 60 \cdot 156$:

n	q_n	r_n	s_n	t_n	Division
0		191	1	0	
1		156	0	1	$191 = 1 \cdot 156 + 35$
2	1	35	$1 - 1 \cdot 0 = 1$	$0 - 1 \cdot 1 = -1$	$156 = 4 \cdot 35 + 16$
3	4	16	$0 - 4 \cdot 1 = -4$	$1 - 4 \cdot (-1) = 5$	$35 = 2 \cdot 16 + 3$
4	2	3	$1 - 2 \cdot (-4) = 9$	$-1 - 2 \cdot 5 = -11$	$16 = 5 \cdot 3 + 1$
5	5	1	$-4 - 5 \cdot 9 = -49$	$5 - 5 \cdot (-11) = 60$	$3 = 3 \cdot 1 + 0$
6	3	0			

4. Note that $a = 1 \cdot a + 0 \cdot b \in L$, so L is not the empty set, and $L \subseteq \mathbb{Z}^+ \subseteq \mathbb{N}$. Therefore, by the well-ordering principle, L has a smallest element. Let d be the smallest element of L. Since $d \in L$, there are integers s and t such that $d = sa + tb$. Let q and r be the quotient and remainder when a is divided by d. Thus, $a = qd + r$ and $0 \leq r < d$. Suppose $r \neq 0$. Then $r \in \mathbb{Z}^+$ and

$$r = a - qd = a - q(sa + tb) = (1 - qs)a - (qt)b,$$

so $r \in L$. But $r < d$, so this contradicts the fact that d is the smallest element of L. Therefore $r = 0$, so $a = qd$, which implies that $d \mid a$. A similar argument shows that $d \mid b$, so $d \in D(a) \cap D(b)$. To show that it is the largest element of $D(a) \cap D(b)$, suppose $c \in D(a) \cap D(b)$. Then there are integers j and k such that $a = jc$ and $b = kc$, so $d = sa + tb = sjc + tkc = (sj + tk)c$. Therefore $c \mid d$, which implies that $c \leq d$.

5. Let n be an arbitrary integer.

($\rightarrow$) Suppose n is a linear combination of a and b. Then there are integers s and t such that $n = sa + tb$. Since $d = \gcd(a, b)$, $d \mid a$ and $d \mid b$, so there are integers j and k such that $a = jd$ and $b = kd$. Therefore $n = sa + tb = sjd + tkd = (sj + tk)d$, so $d \mid n$.

($\leftarrow$) Suppose $d \mid n$. Then there is some integer k such that $n = kd$. By Theorem 7.1.4, there are integers s and t such that $d = sa + tb$. Therefore $n = kd = k(sa + tb) = (ks)a + (kt)b$, so n is a linear combination of a and b.

6. We will prove that $D(a) \cap D(b) = D(a + bc) \cap D(b)$, from which the desired conclusion follows. Suppose $d \in D(a) \cap D(b)$. Then there are integers j and k such that $a = jd$ and $b = kd$. Therefore $a + bc = jd + kdc = (j + kc)d$, so $d \in D(a + bc)$. Since we also have $d \in D(b)$, we conclude that $d \in D(a + bc) \cap D(b)$.

Now suppose that $d \in D(a + bc) \cap D(b)$. Then there are integers j and k such that $a + bc = jd$ and $b = kd$. Therefore $a = jd - bc = jd - kdc = (j - kc)d$, so $d \in D(a)$. Since we also have $d \in D(b)$, we

conclude that $d \in D(a) \cap D(b)$.

7. (a) No. Counterexample: $a = b = 2$, $a' = 3$, $b' = 4$.
   (b) Yes. Suppose $a \mid a'$ and $b \mid b'$. Let $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$. Since $d \mid a$ and $a \mid a'$, by Theorem 3.3.7, $d \mid a'$. Similarly, $d \mid b'$. Therefore, by Theorem 7.1.6, $d \mid \gcd(a', b')$.

8. Let $d = \gcd(5a + 2, 13a + 5)$. Note that $13(5a + 2) - 5(13a + 5) = (65a + 26) - (65a + 25) = 1$. Thus, 1 is a linear combination of $5a + 2$ and $13a + 5$, and by exercise 5 it follows that $d \mid 1$, so $d = 1$.

9. We use strong induction on the maximum of a and b. In other words, we prove the following statement by strong induction:

$$\forall k \in \mathbb{Z}^+[\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+(\max(a, b) = k \to \gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1)],$$

where $\max(a, b)$ denotes the maximum of a and b.

Let $k \in \mathbb{Z}^+$ be arbitrary and assume that for every positive integer $k' < k$,

$$\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+(\max(a, b) = k' \to \gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1).$$

Now let a and b be arbitrary positive integers and assume that $\max(a, b) = k$. We may assume that $a \geq b$, since otherwise we can swap the values of a and b. We consider two cases.

Case 1. $a = b$. Then

$$\gcd(2^a - 1, 2^b - 1) = \gcd(2^a - 1, 2^a - 1) = 2^a - 1 = 2^{\gcd(a,a)} - 1 = 2^{\gcd(a,b)} - 1.$$

Case 2. $a > b$. Let $c = a - b > 0$, so that $a = c + b$. Let $k' = \max(c, b)$. Since $b < a$ and $c < a$, $k' < a = \max(a, b) = k$. Therefore

$$\begin{aligned}
\gcd(2^a - 1, 2^b - 1) &= \gcd(2^c - 1 + 2^a - 2^c, 2^b - 1) \\
&= \gcd(2^c - 1 + 2^c(2^b - 1), 2^b - 1) \\
&= \gcd(2^c - 1, 2^b - 1) && \text{(exercise 6)} \\
&= 2^{\gcd(c,b)} - 1 && \text{(inductive hypothesis)} \\
&= 2^{\gcd(c+b,b)} - 1 && \text{(exercise 6)} \\
&= 2^{\gcd(a,b)} - 1.
\end{aligned}$$

10. Let $d = \gcd(a, b)$ and $e = \gcd(na, nb)$. Then $d \mid a$ and $d \mid b$, so there are integers j and k such that $a = jd$ and $b = kd$. Therefore $na = j(nd)$ and $nb = k(nd)$, so $nd \mid na$ and $nd \mid nb$. Since e is the *greatest* common divisor of na and nb, $nd \leq e$.

    Since $n \mid na$ and $n \mid nb$, by Theorem 7.1.6, $n \mid e$, so we can choose an integer r such that $e = nr$. Since $e \mid na$ and $e \mid nb$, we can choose integers s and t such that $na = se = snr$ and $nb = te = tnr$. Dividing these equations by n, we conclude that $a = sr$ and $b = tr$. Therefore $r \mid a$ and $r \mid b$. Since d is the *greatest* common divisor of a and b, $r \leq d$, so $e = nr \leq nd$. Combining this with our earlier conclusion that $nd \leq e$, we have $e = nd$; in other words, $\gcd(na, nb) = n \gcd(a, b)$.

11. (a) Let $d = \gcd(a, b)$. Suppose $n \in D(d)$. Then $n \mid d$. Since $d \mid a$ and $d \mid b$, it follows by Theorem 3.3.7 that $n \mid a$ and $n \mid b$, so $n \in D(a) \cap D(b)$.

        Now suppose $n \in D(a) \cap D(b)$. Then $n \mid a$ and $n \mid b$, so by Theorem 7.1.6, $n \mid d$, and therefore $n \in D(d)$. Thus $D(\gcd(a, b)) = D(d) = D(a) \cap D(b)$.

    (b) By definition, $\gcd(\gcd(a, b), c)$ is the largest element of $D(\gcd(a, b)) \cap D(c)$. But by part (a), $D(\gcd(a, b)) \cap D(c) = D(a) \cap D(b) \cap D(c)$. Thus, $\gcd(\gcd(a, b), c)$ is the largest element of $D(a) \cap D(b) \cap D(c)$.

12. (a) The Euclidean algorithm shows that $\gcd(55, 34) = 1$:

n	q_n	r_n	Division
0		55	
1		34	$55 = 1 \cdot 34 + 21$
2	1	21	$34 = 1 \cdot 21 + 13$
3	1	13	$21 = 1 \cdot 13 + 8$
4	1	8	$13 = 1 \cdot 8 + 5$
5	1	5	$8 = 1 \cdot 5 + 3$
6	1	3	$5 = 1 \cdot 3 + 2$
7	1	2	$3 = 1 \cdot 2 + 1$
8	1	1	$2 = 2 \cdot 1 + 0$
9	2	0	

The numbers r_i are the Fibonacci numbers. There are 8 divisions.

(b) There are $n - 1$ division steps, and $\gcd(F_{n+1}, F_n) = 1$. To prove this, let r_0, r_1, ... be the sequence of numbers produced by the Euclidean algorithm. We claim first that for every $k \leq n-1$, $r_k = F_{n+1-k}$. We prove this by strong induction. Suppose that $k \leq n - 1$ and for all $k' < k$, $r_{k'} = F_{n+1-k'}$. We consider three cases.

Case 1. $k = 0$. Then $r_k = r_0 = F_{n+1} = F_{n+1-0}$.

Case 2. $k = 1$. Then $r_k = r_1 = F_n = F_{n+1-1}$.

Case 3. $k \geq 2$. Then r_k is the remainder when dividing r_{k-2} by r_{k-1}. By inductive hypothesis, $r_{k-2} = F_{n+3-k}$ and $r_{k-1} = F_{n+2-k}$. By the definition of the Fibonacci numbers, $F_{n+3-k} = 1 \cdot F_{n+2-k} + F_{n+1-k}$, and since $k \leq n - 1$, $n + 1 - k \geq 2$, so $F_{n+1-k} < F_{n+2-k}$. Therefore the quotient when dividing r_{k-2} by r_{k-1} is 1, and the remainder is F_{n+1-k}, so $r_k = F_{n+1-k}$.

This completes the proof by induction that for all $k \leq n - 1$, $r_k = F_{n+1-k}$. In particular, we have $r_{n-2} = F_3 = 2$ and $r_{n-1} = F_2 = 1$. To compute r_n, we divide by r_{n-2} by r_{n-1}, which gives a quotient of 2 and remainder of 0. Thus $r_n = 0$, so there are $n - 1$ division steps, and $\gcd(F_{n+1}, F_n) = r_{n-1} = 1$.

13. (a) We use strong induction. Suppose $k < m$, and for all $k' < k$, $r_{m-k'} \geq F_{k'+2}$. We consider three cases.

Case 1. $k = 0$. Then $r_{m-k} = r_m \neq 0$, so $r_{m-k} \geq 1 = F_2 = F_{k+2}$.

Case 2. $k = 1$. Then $m \geq 2$, so $r_{m-1} > r_m \geq 1$. Therefore $r_{m-k} = r_{m-1} \geq 2 = F_3 = F_{k+2}$.

Case 3. $k \geq 2$. Then r_{m-k+2} is the remainder when dividing r_{m-k} by r_{m-k+1}. Let q_{m-k+2} be the quotient. Since $r_{m-k} > r_{m-k+1}$, the quotient is at least 1, so

$$\begin{aligned} r_{m-k} &= q_{m-k+2} \cdot r_{m-k+1} + r_{m-k+2} \\ &\geq 1 \cdot r_{m-(k-1)} + r_{m-(k-2)} \\ &\geq F_{k+1} + F_k && \text{(inductive hypothesis)} \\ &= F_{k+2}. \end{aligned}$$

(b) Let $\alpha = (1 - \sqrt{5})/2 \approx -0.618$. Then $-1 < \alpha < 0$, and you can prove by induction that for every positive integer k, $-1 < \alpha^k < 1$.

Let k be an arbitrary positive integer. Then by Theorem 6.4.3,

$$F_k = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}} = \frac{\varphi^k - \alpha^k}{\sqrt{5}} > \frac{\varphi^k - 1}{\sqrt{5}} = \frac{\varphi^k}{\sqrt{5}} - \frac{1}{\sqrt{5}} > \frac{\varphi^k}{\sqrt{5}} - 1.$$

(c) Applying first part (a) with $k = m - 1$ and then part (b), we get

$$b = r_1 = r_{m-(m-1)} \geq F_{m+1} > \frac{\varphi^{m+1}}{\sqrt{5}} - 1.$$

Rearranging this inequality, we get

$$\varphi^{m+1} < (b+1)\sqrt{5}.$$

Taking the logarithm of both sides and applying properties of logarithms, we get

$$(m+1)\log\varphi = \log(\varphi^{m+1}) < \log((b+1)\sqrt{5}) = \log(b+1) + \frac{\log 5}{2},$$

and therefore

$$m < \frac{\log(b+1)}{\log\varphi} + \frac{\log 5}{2\log\varphi} - 1.$$

(d) We apply part (c), using base-10 logarithms. Suppose b has at most 100 digits. Then $b+1 \le 10^{100}$, so $\log(b+1) \le 100$, and the number of divisions when using the Euclidean algorithm is

$$m < \frac{\log(b+1)}{\log\varphi} + \frac{\log 5}{2\log\varphi} - 1 \le \frac{100}{\log\varphi} + \frac{\log 5}{2\log\varphi} - 1 \approx 479.169.$$

Since m is an integer, $m \le 479$.

14. (a) Suppose a and b are positive integers. By the division algorithm (Theorem 6.4.1), there are natural numbers q_0 and r_0 such that $a = q_0 b + r_0$ and $r_0 < b$. We now consider two cases.

Case 1. $r_0 \le b/2$. Let $q = q_0$ and $r = r_0$. Then $a = qb + r$ and $r \le b/2$.

Case 2. $r_0 > b/2$. Let $q = q_0 + 1$ and $r = b - r_0 > 0$. Then

$$a = q_0 b + r_0 = (q_0+1)b - (b - r_0) = qb - r$$

and $r = b - r_0 < b - b/2 = b/2$.

Thus, there are natural numbers q and r such that $r \le b/2$ and either $a = qb + r$ or $a = qb - r$.

(b) We will prove that $D(a) \cap D(b) = D(b) \cap D(r)$, from which the desired conclusion follows. If $a = qb + r$ then the proof is exactly the same as in the text. Now consider the case $a = qb - r$. Suppose $d \in D(a) \cap D(b)$. Then there are integers j and k such that $a = jd$ and $b = kd$. Therefore $r = qb - a = qkd - jd = (qk - j)d$, so $d \in D(r)$. Since we also have $d \in D(b)$, $d \in D(b) \cap D(r)$.

Now suppose $d \in D(b) \cap D(r)$. Then there are integers j and k such that $b = jd$ and $r = kd$. Therefore $a = qb - r = qjd - kd = (qj - k)d$, so $d \in D(a)$. Since we also have $d \in D(b)$, $d \in D(a) \cap D(b)$.

(c) The proof is almost exactly the same as in the text. If there is no n such that $r_n = 0$, then the sequence r_0, r_1, ... is an infinite sequence, and for every $n \ge 1$, $r_{n+1} \le r_n/2 < r_n$. Therefore $\{r_0, r_1, \ldots\}$ is a nonempty set of natural numbers with no smallest element, which contradicts the well-ordering principle. Thus there must be some positive integer m such that $r_m \ne 0$ and $r_{m+1} = 0$. Applying part (b) repeatedly, we have

$$\gcd(a,b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{m-1}, r_m) = r_m.$$

(d) The least absolute remainder Euclidean algorithm takes fewer steps, as these calculations show:

Euclidean Algorithm

n	q_n	r_n	Division
0		1515	
1		555	$1515 = 2 \cdot 555 + 405$
2	2	405	$555 = 1 \cdot 405 + 150$
3	1	150	$405 = 2 \cdot 150 + 105$
4	2	105	$150 = 1 \cdot 105 + 45$
5	1	45	$105 = 2 \cdot 45 + 15$
6	2	15	$45 = 3 \cdot 15 + 0$
7	3	0	

Least Absolute Remainder Euclidean Algorithm

n	q_n	r_n	Division
0		1515	
1		555	$1515 = 3 \cdot 555 - 150$
2	3	150	$555 = 4 \cdot 150 - 45$
3	4	45	$150 = 3 \cdot 45 + 15$
4	3	15	$45 = 3 \cdot 15 + 0$
5	3	0	

Section 7.2

1. $650 = 2 \cdot 5^2 \cdot 13$, $756 = 2^2 \cdot 3^3 \cdot 7$, $1067 = 11 \cdot 97$.

2. $\text{lcm}(1495, 650) = 1495 \cdot 650 / \gcd(1495, 650) = 971750/65 = 14950$.

3. $\text{lcm}(1953, 868) = 1953 \cdot 868 / \gcd(1953, 868) = 1695204/217 = 7812$.

4. Let e and f be arbitrary real numbers. We consider two cases.
   Case 1. $e \leq f$. Then $\min(e, f) = e$ and $\max(e, f) = f$, so $\min(e, f) + \max(e, f) = e + f$.
   Case 2. $e > f$. Then $\min(e, f) = f$ and $\max(e, f) = e$, so $\min(e, f) + \max(e, f) = f + e = e + f$.

5. We prove the contrapositives of both directions.
   ($\rightarrow$) Suppose some prime number p appears in the prime factorizations of both a and b. Then $p \mid a$ and $p \mid b$, so $\gcd(a, b) \geq p > 1$, and therefore a and b are not relatively prime.
   ($\leftarrow$) Suppose a and b are not relatively prime. Let $d = \gcd(a, b) > 1$. Let p be any prime number in the prime factorization of d. Then since $d \mid a$ and $d \mid b$, p must occur in the prime factorizations of both a and b.

6. ($\rightarrow$) Suppose a and b are relatively prime. Then by Theorem 7.1.4, there are integers s and t such that $sa + tb = \gcd(a, b) = 1$.
   ($\leftarrow$) Suppose there are integers s and t such that $sa + tb = 1$. By exercise 5 in Section 7.1, $\gcd(a, b) \mid 1$, so $\gcd(a, b) = 1$.

7. Suppose d is a positive integer such that $d \mid a'$ and $d \mid b'$. Since $a' \mid a$ and $b' \mid b$, by the transitivity of the divisibility relation, $d \mid a$ and $d \mid b$. Since a and b are relatively prime, $d = 1$. Thus, the only common divisor of a' and b' is 1, so a' and b' are relatively prime.

8. Let $d = \gcd(a, b)$ and $x = ab/\gcd(a, b) = ab/d$.
   (a) Since $d = \gcd(a, b)$, $d \mid b$, so there is some integer k such that $b = kd$. Therefore $x = akd/d = ak$, so x is an integer and $a \mid x$. A similar argument shows that $b \mid x$, so x is a common multiple of a and b. Since m is the *least* common multiple, $m \leq x$.
   (b) Suppose $r > 0$. Since $a \mid m$, there is some integer t such that $m = ta$. Therefore $r = ab - qm = ab - qta = (b - qt)a$, so $a \mid r$. Similarly, $b \mid r$. But $r < m$, so this contradicts the definition of m as the *least* positive integer that is divisible by both a and b. Therefore $r = 0$.
   (c) With t defined as in part (b), $ab = qm = qta$. Dividing both sides by a, we get $b = qt$, so $q \mid b$. The proof that $q \mid a$ is similar.
   (d) Since $q \mid a$ and $q \mid b$, $q \leq \gcd(a, b)$. Therefore $ab = qm \leq \gcd(a, b)m$, so $m \geq ab/\gcd(a, b)$.

9. By Theorem 7.1.4, there are integers s and t such that $d = sa + tb = sjd + tkd$. Dividing this equation by d, we get $1 = sj + tk$, so by exercise 6, j and k are relatively prime.

10. Suppose a, b, and d are positive integers and $d \mid ab$. Let $d_2 = \gcd(d, b)$. Then there are positive integers d_1 and k such that $d = d_1 d_2$ and $b = kd_2$, and by exercise 9, d_1 and k are relatively prime. Since $d \mid ab$, we can choose an integer j such that $ab = jd$. Therefore $akd_2 = jd_1 d_2$, and dividing by d_2 we get $ak = jd_1$. Thus $d_1 \mid ak$. Since $\gcd(d_1, k) = 1$, by Theorem 7.2.2, $d_1 \mid a$. Thus we have $d = d_1 d_2$, $d_1 \mid a$, and $d_2 \mid b$.

11. Suppose a, b, and m are positive integers, $a \mid m$, and $b \mid m$. Then we can choose integers j and k such that $m = ja = kb$. Also, $a \mid \text{lcm}(a, b)$ and $b \mid \text{lcm}(a, b)$, so we can choose integers s and t such that $\text{lcm}(a, b) = sa = tb$. Let q and r be the quotient and remainder when m is divided by $\text{lcm}(a, b)$. Then $m = q\,\text{lcm}(a, b) + r$ and $0 \leq r < \text{lcm}(a, b)$. Suppose $r > 0$. Then $r = m - q\,\text{lcm}(a, b) = ja - qsa = (j - qs)a$, so $a \mid r$, and also $r = m - q\,\text{lcm}(a, b) = kb - qtb = (k - qt)b$, so $b \mid r$. This contradicts the fact that $\text{lcm}(a, b)$ is the *smallest* positive integer that is divisible by both a and b. Thus $r = 0$, so $m = q\,\text{lcm}(a, b)$ and $\text{lcm}(a, b) \mid m$.

12. Let $n = \text{lcm}(\text{lcm}(a,b),c)$. Since $a \mid m$ and $b \mid m$, by exercise 11, $\text{lcm}(a,b) \mid m$. Since n is the *smallest* positive integer that is divisible by both $\text{lcm}(a,b)$ and c, $n \leq m$.

    Since $n = \text{lcm}(\text{lcm}(a,b),c)$, $\text{lcm}(a,b) \mid n$ and $c \mid n$. But also $a \mid \text{lcm}(a,b)$ and $b \mid \text{lcm}(a,b)$, so by Theorem 3.3.7, $a \mid n$ and $b \mid n$. Since m is the *smallest* positive integer that is divisible by a, b, and c, $m \leq n$. Combining this with our earlier conclusion that $n \leq m$, we have $m = n = \text{lcm}(\text{lcm}(a,b),c)$.

13. Suppose a and b are positive integers and $a^2 \mid b^2$. Let the prime factorization of b be $b = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Then the prime factorization of b^2 is $b^2 = p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k}$. Since $a^2 \mid b^2$, every prime factor of a must be one of p_1, p_2, ..., p_k, so $a = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$ for some natural numbers f_1, f_2, ..., f_k. Therefore $a^2 = p_1^{2f_1} p_2^{2f_2} \cdots p_k^{2f_k}$. Since $a^2 \mid b^2$, for every i we must have $2f_i \leq 2e_i$, and therefore $f_i \leq e_i$. Thus $a \mid b$.

14. (a) Suppose p is prime and $5p + 9 \in \{n^2 \mid n \in \mathbb{N}\}$. Then there is some natural number n such that $5p + 9 = n^2$. Note that $n^2 = 5p + 9 > 9$, so $n \geq 4$. Rearranging the equation $5p + 9 = n^2$, we get $5p = n^2 - 9 = (n-3)(n+3)$, so $p \mid ((n-3)(n+3))$. Since p is prime, by Theorem 7.2.3 it follows that either $p \mid (n-3)$ or $p \mid (n+3)$.

    If $p \mid (n-3)$, then there is some integer k such that $n-3 = kp$, so $5p = (n-3)(n+3) = kp(n+3)$. Dividing by p, we conclude that $5 = k(n+3)$, so $(n+3) \mid 5$. But since $n \geq 4$, $n + 3 \geq 7$, so this is impossible. Thus $p \nmid (n-3)$, so we must have $p \mid (n+3)$. Therefore there is an integer k such that $n + 3 = kp$, so $5p = (n+3)(n-3) = kp(n-3)$. Dividing by p, we get $5 = k(n-3)$, so $(n-3) \mid 5$. But the only divisors of 5 are 1 and 5, so either $n - 3 = 1$ or $n - 3 = 5$. In other words, either $n = 4$ or $n = 8$.

    We now check each of these values of n to see if it leads to a solution for p. If $n = 4$, then $5p + 9 = n^2 = 16$, so $p = 7/5$, which is not an integer. If $n = 8$, then $5p + 9 = n^2 = 64$, so $p = 55/5 = 11$, which is a prime number. Thus the only solution is $p = 11$.

    (b) Suppose p is a prime and $15p + 4 \in \{n^2 \mid n \in \mathbb{N}\}$. Then there is some natural number n such that $15p + 4 = n^2$. Since $n^2 > 4$, $n \geq 3$. Rearranging the equation $15p + 4 = n^2$, we get $15p = n^2 - 4 = (n-2)(n+2)$. Therefore $p \mid ((n-2)(n+2))$, so since p is prime, either $p \mid (n-2)$ or $p \mid (n+2)$.

    If $p \mid (n-2)$ then there is some positive integer k such that $n-2 = kp$, so $15p = (n-2)(n+2) = kp(n+2)$, and dividing by p we get $15 = k(n+2)$. Therefore $(n+2) \mid 15$. Since $D(15) = \{1, 3, 5, 15\}$, this implies that $n + 2$ must be 1, 3, 5, or 15. But we also have $n \geq 3$, so $n + 2 \geq 5$. Therefore either $n + 2 = 5$ or $n + 2 = 15$, which means that either $n = 3$ or $n = 13$.

    If $p \mid (n+2)$ then similar reasoning leads to the conclusion that $(n-2) \mid 15$, so $n - 2$ must be 1, 3, 5, or 15, which means n is one of 3, 5, 7, or 17.

    We now have n narrowed down to five possible values: 3, 5, 7, 13, or 17. We can now check each to see whether it leads to a solution for p:

$$\begin{aligned}
&n = 3: \quad p = 1/3, \text{ which is not an integer;}\\
&n = 5: \quad p = 7/5, \text{ which is not an integer;}\\
&n = 7: \quad p = 3, \text{ which is prime;}\\
&n = 13: \quad p = 11, \text{ which is prime;}\\
&n = 17: \quad p = 19, \text{ which is prime.}
\end{aligned}$$

    Thus, there are three solutions for p: 3, 11, and 19.

    (c) Suppose p is a prime and $5p + 8 \in \{n^3 \mid n \in \mathbb{N}\}$. Then there is some natural number n such that $5p + 8 = n^3$. Since $n^3 > 8$, $n \geq 3$. From $5p + 8 = n^3$ we get $5p = n^3 - 8 = (n-2)(n^2 + 2n + 4)$, and imitating the reasoning used in parts (a) and (b) we can conclude that either $(n-2) \mid 5$ or $(n^2 + 2n + 4) \mid 5$. But since $n \geq 3$, $n^2 + 2n + 4 \geq 19$, so $(n^2 + 2n + 4) \nmid 5$. Therefore $(n-2) \mid 5$, so

either $n-2=1$ or $n-2=5$, which means that either $n=3$ or $n=7$. If $n=3$ then $p=19/5$, which is not an integer. If $n=7$, then $p=67$, which is prime. So $p=67$ is the only solution.

15. (a) Suppose $x, y \in H$. Then we can choose natural numbers m and n such that $x = 4m+1$ and $y = 4n+1$. Therefore $xy = (4m+1)(4n+1) = 16mn+4m+4n+1 = 4(4mn+m+n)+1 \in H$.

    (b) We prove by strong induction that for every natural number m, if $m > 1$ and $m \in H$ then m is either a Hilbert prime or a product of two or more Hilbert primes. So suppose that $m \in H$ and $m > 1$, and for every $k < m$, if $k > 1$ and $k \in H$ then k is either a Hilbert prime or a product of two or more Hilbert primes. Of course, if m is a Hilbert prime then there is nothing to prove, so suppose that m is not a Hilbert prime. Then we can choose Hilbert numbers a and b such that $m = ab$, $a < m$, and $b < m$. Note that since $a < m = ab$, it follows that $b > 1$, and similarly we must have $a > 1$. Thus, by inductive hypothesis, each of a and b is either a Hilbert prime or a product of Hilbert primes. But then since $m = ab$, m is a product of Hilbert primes.

    (c) First note that $441 = 4 \cdot 110 + 1$, so $441 \in H$. We have $441 = 9 \cdot 49 = 21 \cdot 21$. Each of the numbers 9, 49, and 21 can be written as a product of smaller natural numbers in only one way: $9 = 3 \cdot 3$, $49 = 7 \cdot 7$, and $21 = 3 \cdot 7$. However, 3 and 7 are not Hilbert numbers, so 9, 49, and 21 are Hilbert primes.

16. Let $p_1, p_2, \ldots, p_k$ be a list of all primes that occur in the prime factorization of either a or b, so that

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \qquad b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

for some natural numbers $e_1, e_2, \ldots, e_k$ and $f_1, f_2, \ldots, f_k$. For $i = 1, 2, \ldots, k$, let

$$g_i = \begin{cases} e_i, & \text{if } e_i \geq f_i, \\ 0, & \text{if } e_i < f_i, \end{cases} \qquad h_i = \begin{cases} 0, & \text{if } e_i \geq f_i, \\ f_i, & \text{if } e_i < f_i. \end{cases}$$

Let

$$c = p_1^{g_1} p_2^{g_2} \cdots p_k^{g_k}, \qquad d = p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k}.$$

Then for all i, $g_i \leq e_i$ and $h_i \leq f_i$, and therefore $c \mid a$ and $d \mid b$. Also, c and d have no prime factors in common, so by exercise 5, c and d are relatively prime. Finally,

$$cd = p_1^{g_1+h_1} \cdots p_k^{g_k+h_k} = p_1^{\max(e_1,f_1)} \cdots p_k^{\max(e_k,f_k)} = \operatorname{lcm}(a, b).$$

17. (a) Let s, t, u, and v be integers such that

$$\gcd(a, b) = sa + tb, \qquad \gcd(a, c) = ua + vc.$$

Then

$$\gcd(a, b) \cdot \gcd(a, c) = (sa + tb)(ua + vc) = (sua + svc + tbu)a + (tv)bc.$$

Thus, $\gcd(a, b) \cdot \gcd(a, c)$ is a linear combination of a and bc, and by exercise 5 in Section 7.1 it follows that $\gcd(a, bc) \mid (\gcd(a, b) \cdot \gcd(a, c))$.

    (b) Let $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$. Since $d \mid b$ and $b \mid bc$, $d \mid bc$. Since $d \mid a$ and $d \mid bc$, by Theorem 7.1.6, $d \mid \gcd(a, bc)$; in other words, $\gcd(a, b) \mid \gcd(a, bc)$. A similar argument shows that $\gcd(a, c) \mid \gcd(a, bc)$. Therefore, by exercise 11, $\operatorname{lcm}(\gcd(a, b), \gcd(a, c)) \mid \gcd(a, bc)$.

    (c) Since b and c are relatively prime, $\gcd(a, b) \mid b$, and $\gcd(a, c) \mid c$, by exercise 7, $\gcd(a, b)$ and $\gcd(a, c)$ are relatively prime. Therefore

$$\operatorname{lcm}(\gcd(a, b), \gcd(a, c)) = \frac{\gcd(a, b) \cdot \gcd(a, c)}{\gcd(\gcd(a, b), \gcd(a, c))} = \frac{\gcd(a, b) \cdot \gcd(a, c)}{1} = \gcd(a, b) \cdot \gcd(a, c).$$

Substituting into part (b), we get $(\gcd(a, b) \cdot \gcd(a, c)) \mid \gcd(a, bc)$, and thus $\gcd(a, b) \cdot \gcd(a, c) \leq \gcd(a, bc)$. And by part (a) we have $\gcd(a, bc) \leq \gcd(a, b) \cdot \gcd(a, c)$. Combining these facts, we conclude that $\gcd(a, bc) = \gcd(a, b) \cdot \gcd(a, c)$.

18. Suppose m is a positive integer and $2^m + 1$ is prime. Suppose m is not a power of two. Then the prime factorization of m must include some odd prime number p, so there is some positive integer r such that $m = pr$. Since p is odd, there is some positive integer n such that $p = 2n + 1$. Therefore $2^m + 1 = 2^{(2n+1)r} + 1 = (2^r)^{2n+1} + 1^{2n+1}$. By exercise 14 in Section 6.1, $(2^r + 1) \mid ((2^r)^{2n+1} + 1^{2n+1})$, so $(2^r + 1) \mid (2^m + 1)$. Since $r < m$, $1 < 2^r + 1 < 2^m + 1$, so this contradicts the fact that $2^m + 1$ is prime. Therefore m is a power of two.

19. (a) Since x is a positive rational number, there are positive integers m and n such that $x = m/n$. Let $d = \gcd(m, n)$. By exercise 9, we can let a and b be positive integers such that $m = da$, $n = db$, and $\gcd(a, b) = 1$. Then
$$x = \frac{m}{n} = \frac{da}{db} = \frac{a}{b}.$$

(b) Since $a/b = c/d$, $ad = bc$. Therefore $a \mid bc$. Since $\gcd(a, b) = 1$, by Theorem 7.2.2, $a \mid c$. A similar argument shows $c \mid a$, so $a = c$. Therefore $ad = bc = ba$, and dividing both sides by a we conclude that $b = d$.

(c) By part (a), we have $x = a/b$, where a and b are relatively prime positive integers. Let the prime factorizations of a and b be
$$a = r_1^{g_1} r_2^{g_2} \cdots r_j^{g_j}, \qquad b = s_1^{h_1} s_2^{h_2} \cdots s_l^{h_l}.$$
Note that by exercise 5, these factorizations have no primes in common. Then
$$x = \frac{r_1^{g_1} r_2^{g_2} \cdots r_j^{g_j}}{s_1^{h_1} s_2^{h_2} \cdots s_l^{h_l}} = r_1^{g_1} r_2^{g_2} \cdots r_j^{g_j} s_1^{-h_1} s_2^{-h_2} \cdots s_l^{-h_l}.$$
Rearranging the primes $r_1, \ldots, r_j, s_1, \ldots, s_l$ into increasing order gives the required product $p_1^{e_1} \cdots p_k^{e_k}$.

(d) We begin by reversing the steps of part (c). Let $r_1, r_2, \ldots, r_j$ be those primes in the product $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ whose exponents are positive, listed in increasing order, and $s_1, s_2, \ldots, s_l$ those whose exponents are negative. Rewriting each prime raised to a negative power as the prime to a positive power in the denominator, we get
$$x = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = \frac{r_1^{g_1} r_2^{g_2} \cdots r_j^{g_j}}{s_1^{h_1} s_2^{h_2} \cdots s_l^{h_l}},$$
where all the exponents g_i and h_i are positive integers. The numerator and denominator have no prime factors in common, so they are relatively prime. Similarly, the product $q_1^{f_1} q_2^{f_2} \cdots q_m^{f_m}$ can be rewritten as a fraction with all exponents positive:
$$x = q_1^{f_1} q_2^{f_2} \cdots q_m^{f_m} = \frac{v_1^{y_1} v_2^{y_2} \cdots v_t^{y_t}}{w_1^{z_1} w_2^{z_2} \cdots w_u^{z_u}}.$$
By part (b), $r_1^{g_1} \cdots r_j^{g_j} = v_1^{y_1} \cdots v_t^{y_t}$ and $s_1^{h_1} \cdots s_l^{h_l} = w_1^{z_1} \cdots w_u^{z_u}$. By the uniqueness of prime factorizations, $j = t$ and for all $i \in \{1, \ldots, j\}$, $r_i = v_i$ and $g_i = y_i$, and also $l = u$ and for all $i \in \{1, \ldots, l\}$, $s_i = w_i$ and $h_i = z_i$. Rewriting the primes in the denominator as primes raised to negative powers, we find that the original two products $p_1^{e_1} \cdots p_k^{e_k}$ and $q_1^{f_1} \cdots q_m^{f_m}$ are the same.

20. Suppose the prime factorizations of a and b are
$$a = 2^c p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \qquad b = 2^d q_1^{f_1} q_2^{f_2} \cdots q_m^{f_m},$$
where $p_1, p_2, \ldots, p_k$ and $q_1, q_2, \ldots, q_m$ are odd primes. Substituting into the equation $a^2 = 2b^2$, we get
$$2^{2c} p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k} = 2^{2d+1} q_1^{2f_1} q_2^{2f_2} \cdots q_m^{2f_m}.$$
By uniqueness of prime factorizations, the exponents of 2 in these two products must be the same, so $2c = 2d + 1$. But $2c$ is even and $2d + 1$ is odd, so this is a contradiction.

Section 7.3

1.

$+$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$
$[2]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$
$[3]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$
$[4]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$
$[5]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$

$\cdot$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$
$[1]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[2]_6$	$[0]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
$[4]_6$	$[0]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$
$[5]_6$	$[0]_6$	$[5]_6$	$[4]_6$	$[3]_6$	$[2]_6$	$[1]_6$

2. Let $P = [ab]_m$. Now let $x \in X$ and $y \in Y$ be arbitrary. Then $x \in [a]_m$ and $y \in [b]_m$, so $x \equiv a \pmod m$ and $y \equiv b \pmod m$. By Lemma 7.3.4 it follows that $xy \equiv ab \pmod m$, so $xy \in [ab]_m = P$. Since x and y were arbitrary, we conclude that $\forall x \in X \forall y \in Y (xy \in P)$.

   To prove that P is unique, suppose P' is another equivalence class such that $\forall x \in X \forall y \in Y (xy \in P')$. Since $a \in X$ and $b \in Y$, $ab \in P$ and $ab \in P'$. Therefore P and P' are not disjoint, and since $\mathbb{Z}/\equiv_m$ is pairwise disjoint, this implies that $P = P'$.

3. Parts 5–9 of Theorem 7.3.6 follow from these calculations:

   5. $X \cdot Y = [a]_m \cdot [b]_m = [ab]_m = [ba]_m = [b]_m \cdot [a]_m = Y \cdot X$,
   6. $(X \cdot Y) \cdot Z = ([a]_m \cdot [b]_m) \cdot [c]_m = [ab]_m \cdot [c]_m = [(ab)c]_m$
      $= [a(bc)]_m = [a]_m \cdot [bc]_m = [a]_m \cdot ([b]_m \cdot [c]_m) = X \cdot (Y \cdot Z)$,
   7. $X \cdot [1]_m = [a]_m \cdot [1]_m = [a \cdot 1]_m = [a]_m = X$,
   8. $X \cdot [0]_m = [a]_m \cdot [0]_m = [a \cdot 0]_m = [0]_m$,
   9. $X \cdot (Y + Z) = [a]_m \cdot ([b]_m + [c]_m) = [a]_m \cdot [b + c]_m = [a(b + c)]_m$
      $= [ab + ac]_m = [ab]_m + [ac]_m = ([a]_m \cdot [b]_m) + ([a]_m \cdot [c]_m) = (X \cdot Y) + (X \cdot Z)$.

4. (a) Since Z_1 is an additive identity element, $Z_1 + Z_2 = Z_2$. And since Z_2 is an additive identity element, $Z_1 + Z_2 = Z_1$. Therefore $Z_1 = Z_1 + Z_2 = Z_2$.
   (b) Since X_1' is an additive inverse for X, $X_1' + X + X_2' = [0]_m + X_2' = X_2'$. Similarly, since X_2' is an additive inverse for X, $X_1' + X + X_2' = X_1' + [0]_m = X_1'$. Therefore $X_1' = X_2'$.
   (c) Suppose O_1 and O_2 are multiplicative identity elements. Then $O_1 = O_1 \cdot O_2 = O_2$.
   (d) Suppose X_1' and X_2' are multiplicative inverses of X. Then

$$X_1' = X_1' \cdot [1]_m = X_1' \cdot X \cdot X_2' = [1]_m \cdot X_2' = X_2'.$$

5. Suppose $X \in \mathbb{Z}/\equiv_p$ and $X \neq [0]_p$. Then there is some integer r such that $1 \leq r \leq p - 1$ and $X = [r]_p$. Since $p \nmid r$ and p is prime, $\gcd(r, p) = 1$, so by Theorem 7.3.7, $X = [r]_p$ has a multiplicative inverse.

6. No. Counterexample: $m = 6$, $a = 2$, $b = 3$.

7. Since $d = \gcd(m, a)$, we can choose integers j and k such that $m = jd$ and $a = kd$. Suppose b is an integer and $d \nmid b$. Suppose there is some integer x such that $ax \equiv b \pmod m$. Then we can choose an integer t such that $b - ax = tm$, and therefore

$$b = ax + tm = kdx + tjd = (kx + tj)d.$$

   Thus $d \mid b$, which is a contradiction. Thus, there is no integer x such that $ax \equiv b \pmod m$.

8. Let a and b be arbitrary integers. Then

$$\begin{aligned} na \equiv nb \pmod{nm} \quad &\text{iff} \quad \exists k \in \mathbb{Z}(nb - na = knm) \\ &\text{iff} \quad \exists k \in \mathbb{Z}(b - a = km) \quad \text{iff} \quad a \equiv b \pmod m. \end{aligned}$$

9. Let x be the number of packages of file cards the teacher bought. Then he handed out $20x + 2$ cards, giving the same number to each of 26 students, so $26 \mid (20x + 2)$, and therefore $20x \equiv -2 \pmod{26}$. By Theorem 7.3.11, this is equivalent to $10x \equiv -1 \pmod{13}$. To solve this congruence, we first note that $[10]_{13}^{-1} = [4]_{13}$, since $[10]_{13} \cdot [4]_{13} = [40]_{13} = [1]_{13}$, and then we compute:

$$\begin{aligned} 10x \equiv -1 \pmod{13} \quad &\text{iff} \quad [10]_{13} \cdot [x]_{13} = [-1]_{13} = [12]_{13} \\ &\text{iff} \quad [x]_{13} = [10]_{13}^{-1} \cdot [12]_{13} = [4]_{13} \cdot [12]_{13} = [48]_{13} = [9]_{13} \quad \text{iff} \quad x \in [9]_{13}. \end{aligned}$$

Thus, the possible values of x are 9, 22, 35, 48, ... But we have one more piece of information: each student got between 10 and 20 file cards. The number of file cards received by each student is $(20x + 2)/26$, so $10 \leq (20x + 2)/26 \leq 20$, and therefore $12.9 \leq x \leq 25.9$. Thus $x = 22$.

10. (a) The extended Euclidean algorithm shows that $[40]_{237}^{-1} = [160]_{237}$, so

$$\begin{aligned} 40x \equiv 8 \pmod{237} \quad &\text{iff} \quad [40]_{237} \cdot [x]_{237} = [8]_{237} \\ &\text{iff} \quad [x]_{237} = [40]_{237}^{-1} \cdot [8]_{237} = [160]_{237} \cdot [8]_{237} = [1280]_{237} = [95]_{237} \\ &\text{iff} \quad x \in [95]_{237}. \end{aligned}$$

(b) We first rewrite the congruence as $4 \cdot 10x \equiv 4 \cdot 2 \pmod{4 \cdot 59}$, which is equivalent to $10x \equiv 2 \pmod{59}$. We then compute $[10]_{59}^{-1} = [6]_{59}$, so

$$\begin{aligned} 10x \equiv 2 \pmod{59} \quad &\text{iff} \quad [10]_{59} \cdot [x]_{59} = [2]_{59} \\ &\text{iff} \quad [x]_{59} = [10]_{59}^{-1} \cdot [2]_{59} = [6]_{59} \cdot [2]_{59} = [12]_{59} \quad \text{iff} \quad x \in [12]_{59}. \end{aligned}$$

11. (a) The extended Euclidean algorithm shows that $[31]_{384}^{-1} = [223]_{384}$, so

$$\begin{aligned} 31x \equiv 24 \pmod{384} \quad &\text{iff} \quad [31]_{384} \cdot [x]_{384} = [24]_{384} \\ &\text{iff} \quad [x]_{384} = [31]_{384}^{-1} \cdot [24]_{384} = [223]_{384} \cdot [24]_{384} = [5352]_{384} = [360]_{384} \\ &\text{iff} \quad x \in [360]_{384}. \end{aligned}$$

(b) The Euclidean algorithm shows that $\gcd(384, 32) = 32$ and $32 \nmid 24$, so by Theorem 7.3.10, the congruence $32x \equiv 24 \pmod{384}$ has no solutions.

12. (a) Suppose Alice bought x chairs without arms and y chairs with arms. Then since she spent \$720, $35x + 50y = 720$. Therefore $20 - 35x = 50y - 700 = 50(y - 14)$, so $50 \mid (20 - 35x)$, which means that $35x \equiv 20 \pmod{50}$.

(b) The congruence in part (a) can be written as $5 \cdot 7x \equiv 5 \cdot 4 \pmod{5 \cdot 10}$, which is equivalent to $7x \equiv 4 \pmod{10}$. Since $[7]_{10}^{-1} = [3]_{10}$, we can solve the congruence as follows:

$$\begin{aligned} 7x \equiv 4 \pmod{10} \quad &\text{iff} \quad [7]_{10} \cdot [x]_{10} = [4]_{10} \\ &\text{iff} \quad [x]_{10} = [7]_{10}^{-1} \cdot [4]_{10} = [3]_{10} \cdot [4]_{10} = [12]_{10} = [2]_{10} \quad \text{iff} \quad x \in [2]_{10}. \end{aligned}$$

(c) The solutions to the congruence in part (b) are the elements of the set $[2]_{10} = \{2, 12, 22, 32, \ldots, -8, -18, -28, \ldots\}$. However, not all of these values make sense in the problem. We must have $x \geq 0$ and $35x \leq 720$, so $x \leq 720/35 \approx 20.57$. Therefore the only possible solutions are $x = 2, 12$. If $x = 2$ then from $35x + 50y = 720$ we get $y = 13$, and if $x = 12$ then $y = 6$. So she bought either 2 chairs without arms and 13 chairs with arms, or 12 chairs without arms and 6 chairs with arms.

13. Let a and b be arbitrary integers. Suppose first that $a \equiv b \pmod{m}$. Then $[a]_m = [b]_m$, so $[na]_m = [n]_m \cdot [a]_m = [n]_m \cdot [b]_m = [nb]_m$, and therefore $na \equiv nb \pmod{m}$.

Now suppose that $na \equiv nb \pmod{m}$, so $[n]_m \cdot [a]_m = [na]_m = [nb]_m = [n]_m \cdot [b]_m$. Since m and n are relatively prime, $[n]_m$ has a multiplicative inverse. Multiplying both sides of the equation $[n]_m \cdot [a]_m = [n]_m \cdot [b]_m$ by $[n]_m^{-1}$, we get $[a]_m = [b]_m$, so $a \equiv b \pmod{m}$.

14. Suppose a and b are integers, $a \equiv b \pmod{m_1}$, and $a \equiv b \pmod{m_2}$. Then $m_1 \mid (b-a)$ and $m_2 \mid (b-a)$. Therefore, by exercise 11 in Section 7.2, $\text{lcm}(m_1, m_2) \mid (b-a)$, so $a \equiv b \pmod{\text{lcm}(m_1, m_2)}$.

15. Suppose $a \equiv b \pmod{m}$. Then $m \mid (b-a)$, so we can choose an integer n such that $b - a = nm$, so $b = a + nm$. Therefore by exercise 6 in Section 7.1, $\gcd(m, b) = \gcd(m, a + nm) = \gcd(m, a)$.

16. We use mathematical induction.

    Base case: If $n = 0$ then $a^n = a^0 = 1 = b^0 = b^n$, so $a^n \equiv b^n \pmod{m}$.

    Induction step: Suppose n is a natural number and $a^n \equiv b^n \pmod{m}$. We also have $a \equiv b \pmod{m}$, so by Lemma 7.3.4, $a^n \cdot a \equiv b^n \cdot b \pmod{m}$, or in other words, $a^{n+1} \equiv b^{n+1} \pmod{m}$.

17. (a) First note that $10 \equiv 1 \pmod{3}$. Therefore, by exercise 16, for every $i \in \mathbb{N}$, $10^i \equiv 1 \pmod{3}$, so $[10^i]_3 = [1]_3$. Thus

$$\begin{aligned}[n]_3 &= [d_0 + 10d_1 + \cdots + 10^k d_k]_3 \\ &= [d_0]_3 + [10]_3 \cdot [d_1]_3 + \cdots + [10^k]_3 \cdot [d_k]_3 \\ &= [d_0]_3 + [1]_3 \cdot [d_1]_3 + \cdots + [1]_3 \cdot [d_k]_3 \\ &= [d_0 + d_1 + \cdots + d_k]_3.\end{aligned}$$

    In other words, $n \equiv (d_0 + d_1 + \cdots + d_k) \pmod{3}$.

    (b) $3 \mid n$ iff $[n]_3 = [0]_3$ iff $[d_0 + \cdots + d_k]_3 = [0]_3$ iff $3 \mid (d_0 + \cdots + d_k)$.

18. (a) First note that $10 \equiv -1 \pmod{11}$. Therefore, by exercise 16, for every $i \in \mathbb{N}$, $10^i \equiv (-1)^i \pmod{11}$, so $[10^i]_{11} = [(-1)^i]_{11}$. Thus

$$\begin{aligned}[n]_{11} &= [d_0 + 10d_1 + 10^2 d_2 + \cdots + 10^k d_k]_{11} \\ &= [d_0]_{11} + [10]_{11} \cdot [d_1]_{11} + [10^2]_{11} \cdot [d_2]_{11} + \cdots + [10^k]_{11} \cdot [d_k]_{11} \\ &= [d_0]_{11} + [-1]_{11} \cdot [d_1]_{11} + [1]_{11} \cdot [d_2]_{11} + \cdots + [(-1)^k]_{11} \cdot [d_k]_{11} \\ &= [d_0 - d_1 + d_2 - d_3 + \cdots + (-1)^k d_k]_{11}.\end{aligned}$$

    In other words, $n \equiv (d_0 - d_1 + d_2 - d_3 + \cdots + (-1)^k d_k) \pmod{11}$.

    (b) $11 \mid n$ iff $[n]_{11} = [0]_{11}$ iff $[d_0 - d_1 + d_2 - d_3 + \cdots + (-1)^k d_k]_{11} = [0]_{11}$ iff $11 \mid (d_0 - d_1 + \cdots + (-1)^k d_k)$.

    (c) $2 - 7 + 1 - 5 + 3 - 5 = -11$, which is divisible by 11. Therefore 535172 is divisible by 11.

19. (a) Suppose $n \geq 10$. First note that

$$10f(n) = (d_k \cdots d_1 0)_{10} + 50d_0 = (d_k \cdots d_1 d_0)_{10} + 49d_0 = n + 49d_0.$$

    Therefore $3f(n) - n = 49d_0 - 7f(n) = 7(7d_0 - f(n))$, so $n \equiv 3f(n) \pmod{7}$, or equivalently $[n]_7 = [3]_7 \cdot [f(n)]_7$. Since $[3]_7^{-1} = [5]_7$, it follows that $[f(n)]_7 = [5]_7 \cdot [n]_7$, so $f(n) \equiv 5n \pmod{7}$.

    (b) Suppose $n \geq 10$. If $7 \mid n$ then $[n]_7 = [0]_7$, so $[f(n)]_7 = [5n]_7 = [5]_7 \cdot [0]_7 = [0]_7$, and therefore $7 \mid f(n)$. Similarly, if $7 \mid f(n)$ then $[f(n)]_7 = [0]_7$, so $[n]_7 = [3f(n)]_7 = [3]_7 \cdot [0]_7 = [0]_7$ and $7 \mid n$.

    (c) $f(627334) = 62733 + 5 \cdot 4 = 62753$; $f(62753) = 6275 + 5 \cdot 3 = 6290$; $f(6290) = 629 + 5 \cdot 0 = 629$; $f(629) = 62 + 5 \cdot 9 = 107$; $f(107) = 10 + 5 \cdot 7 = 45$; $f(45) = 4 + 5 \cdot 5 = 29$. Since $7 \nmid 29$, $7 \nmid 627334$.

20. (a) One example is $m = 5$, $a = a' = 2$, $b = 1$, $b' = 6$.

    (b) Suppose we could define exponentiation on equivalence classes in such a way that for all positive integers m, a, and b, $([a]_m)^{[b]_m} = [a^b]_m$. Then

$$[2]_5 = [2^1]_5 = ([2]_5)^{[1]_5} = ([2]_5)^{[6]_5} = [2^6]_5 = [64]_5.$$

    But $2 \not\equiv 64 \pmod{5}$, so this is a contradiction.

21. (a) Suppose x_1, x_2, y_1, and y_2 are integers, $x_1 \equiv_m y_1$, and $x_2 \equiv_m y_2$. Then $f(x_1, x_2) = [x_1 + x_2]_m = [x_1]_m + [x_2]_m = [y_1]_m + [y_2]_m = [y_1 + y_2]_m = f(y_1, y_2)$.

    (b) Suppose x_1 and x_2 are integers. Then $h([x_1]_m, [x_2]_m) = [x_1]_m + [x_2]_m = [x_1 + x_2]_m = f(x_1, x_2)$.

Section 7.4

1. $(\mathbb{Z}/\equiv_{20})^* = \{[1]_{20}, [3]_{20}, [7]_{20}, [9]_{20}, [11]_{20}, [13]_{20}, [17]_{20}, [19]_{20}\}$.
2. (a) $\varphi(539) = \varphi(7^2 \cdot 11) = \varphi(7^2) \cdot \varphi(11) = 7^1(7-1) \cdot (11-1) = 420$.
   (b) $\varphi(540) = \varphi(2^2 \cdot 3^3 \cdot 5) = \varphi(2^2) \cdot \varphi(3^3) \cdot \varphi(5) = 2^1(2-1) \cdot 3^2(3-1) \cdot (5-1) = 144$.
   (c) 541 is prime, so $\varphi(541) = 541 - 1 = 540$.
3. (a) $\varphi(18) = \varphi(2 \cdot 3^2) = (2-1) \cdot 3^1(3-1) = 6$; $5^6 - 1 = 15624 = 868 \cdot 18$, so $5^6 \equiv 1 \pmod{18}$.
   (b) $\varphi(19) = 19 - 1 = 18$; $2^{18} - 1 = 262143 = 13797 \cdot 19$, so $2^{18} \equiv 1 \pmod{19}$.
   (c) $\varphi(20) = \varphi(2^2 \cdot 5) = 2^1(2-1) \cdot (5-1) = 8$; $3^8 - 1 = 6560 = 328 \cdot 20$, so $3^8 \equiv 1 \pmod{20}$.
4. (a) We follow the calculations in the proof of Lemma 7.4.7. First we use the extended Euclidean algorithm to show that $\gcd(8, 5) = 1 = 2 \cdot 8 + (-3) \cdot 5$. In other words, $sm + tn = 1$, where $s = -3$ and $t = 2$. Next, we compute $x = tna + smb = 2 \cdot 8 \cdot 4 + (-3) \cdot 5 \cdot 1 = 49$. Finally, we compute $mn = 40$, and we find r such that $1 \leq r \leq 40$ and $r \equiv 49 \pmod{40}$. The answer is $r = 9$; it is easy to verify that $9 \equiv 4 \pmod 5$ and $9 \equiv 1 \pmod 8$.
   (b) We do the same calculations as in part (a): $3 \cdot 7 + (-2) \cdot 10 = 1$, so $s = 3$ and $t = -2$; $x = tna + smb = (-2) \cdot 10 \cdot 6 + 3 \cdot 7 \cdot 4 = -36$; $mn = 70$, $-36 \equiv 34 \pmod{70}$, so $r = 34$.
5. Base case: If $n = 1$, then $[a]_m^n = [a]_m^1 = [a]_m = [a^1]_m = [a^n]_m$.
   Induction step: Suppose n is a positive integer and $[a]_m^n = [a^n]_m$. Then $[a]_m^{n+1} = [a]_m^n \cdot [a]_m = [a^n]_m \cdot [a]_m = [a^n \cdot a]_m = [a^{n+1}]_m$.
6. Suppose $a \equiv b \pmod{mn}$. Then $mn \mid (b-a)$, so for some integer k, $b - a = kmn$. Therefore $m \mid (b-a)$ and $n \mid (b-a)$, so $a \equiv b \pmod m$ and $a \equiv b \pmod n$.
   Now suppose $a \equiv b \pmod m$ and $a \equiv b \pmod n$. Since $a \equiv b \pmod n$, $n \mid (b-a)$, so there is some integer j such that $b - a = jn$. Since $a \equiv b \pmod m$, $m \mid (b-a)$, so $m \mid jn$. But $\gcd(m, n) = 1$, so by Theorem 7.2.2 it follows that $m \mid j$. Let k be an integer such that $j = km$. Then $b - a = jn = kmn$. Therefore $mn \mid (b-a)$, so $a \equiv b \pmod{mn}$. (An alternative approach is to use exercise 14 in Section 7.3.)
7. Let a, b, and c be arbitrary positive integers.
   ($\rightarrow$) Suppose $\gcd(ab, c) = 1$. Then there are integers s and t such that $sab + tc = 1$. We can write this equation as either $(sb)a + tc = 1$ or $(sa)b + tc = 1$, so by exercise 6 in Section 7.2, $\gcd(a, c) = \gcd(b, c) = 1$.
   ($\leftarrow$) Suppose $\gcd(a, c) = \gcd(b, c) = 1$. Then there are integers s, t, u, and v such that $sa + tc = 1$ and $ub + vc = 1$. Therefore
   $$1 = (sa + tc)(ub + vc) = (su)ab + (sav + tub + tcv)c,$$
   so be exercise 6 in Section 7.2, $\gcd(ab, c) = 1$.
8. The first half of the solution to exercise 6 does not use the hypothesis that m and n are relatively prime, so the left-to-right direction of the "iff" statement is correct even if this hypothesis is dropped. Here is a counterexample for the other direction: $a = 0$, $b = 12$, $m = 4$, $n = 6$.
9. No, the lemma would be incorrect. Counterexample: $m = 4$, $n = 6$, $a = 1$, $b = 2$. Suppose there is an integer r such that $r \equiv 1 \pmod 4$ and $r \equiv 2 \pmod 6$. Then $4 \mid (r-1)$ and $6 \mid (r-2)$, so we can choose integers j and k such that $r - 1 = 4j$ and $r - 2 = 6k$. Therefore $r = 4j + 1 = 2(2j) + 1$, so r is odd, and also $r = 6k + 2 = 2(3k + 1)$, so r is even. This is a contradiction.
10. Suppose p is prime and a is a positive integer. We consider two cases.
    Case 1. $p \nmid a$. Then p and a are relatively prime, so by Theorem 7.4.2, $[a]_p^{p-1} = [1]_p$. Therefore $[a^p]_p = [a]_p^{p-1} \cdot [a]_p = [1]_p \cdot [a]_p = [a]_p$, so $a^p \equiv a \pmod p$.
    Case 2. $p \mid a$. Then $[a]_p = [0]_p$, so $[a^p]_p = [0]_p^p = [0]_p = [a]_p$ and therefore $a^p \equiv a \pmod p$.

11. Suppose m and a are relatively prime positive integers. Then by Euler's theorem, $[a]_m \cdot [a^{\varphi(m)-1}]_m = [a^{\varphi(m)}]_m = [1]_m$, so $[a]_m^{-1} = [a^{\varphi(m)-1}]_m$.

12. Suppose m, a, p, and q are positive integers, m and a are relatively prime, and $p \equiv q \pmod{\varphi(m)}$. By Euler's theorem, $a^{\varphi(m)} \equiv 1 \pmod{m}$. It follows, by exercise 16 in Section 7.3, that for every natural number n, $a^{n\varphi(m)} = (a^{\varphi(m)})^n \equiv 1 \pmod{m}$, so $[a^{n\varphi(m)}]_m = [1]_m$. We now consider two cases:

    Case 1. $p \geq q$. Then since $p \equiv q \pmod{\varphi(m)}$, there is some natural number n such that $p - q = n\varphi(m)$, so $p = q + n\varphi(m)$. Therefore

$$[a^p]_m = [a^{q+n\varphi(m)}]_m = [a^q \cdot a^{n\varphi(m)}]_m = [a^q]_m \cdot [a^{n\varphi(m)}]_m = [a^q]_m \cdot [1]_m = [a^q]_m,$$

    so $a^p \equiv a^q \pmod{m}$.

    Case 2. $p < q$. Similar to case 1, but with the roles of p and q reversed.

13. Let a be an arbitrary positive integer. We now use mathematical induction to prove the following statement: for every $k \geq 1$, if $b_1, b_2, \ldots, b_k$ is any list of k positive integers and $\gcd(a, b_1) = \gcd(a, b_2) = \cdots = \gcd(a, b_k) = 1$, then $\gcd(a, b_1 b_2 \cdots b_k) = 1$.

    Base case: If $k = 1$, then the statement to be proven is that if b_1 is any positive integer and $\gcd(a, b_1) = 1$, then $\gcd(a, b_1) = 1$. This is clearly true.

    Induction step: Suppose the statement holds for lists of k positive integers, and suppose $b_1, b_2, \ldots, b_{k+1}$ is a list of $k+1$ positive integers such that $\gcd(a, b_1) = \gcd(a, b_2) = \cdots = \gcd(a, b_{k+1}) = 1$. By the inductive hypothesis, $\gcd(a, b_1 b_2 \cdots b_k) = 1$. But now since $\gcd(a, b_{k+1}) = 1$, by Lemma 7.4.6, $\gcd(a, b_1 b_2 \cdots b_{k+1}) = \gcd(a, (b_1 b_2 \cdots b_k) b_{k+1}) = 1$.

14. We use induction on k.

    Base case: If $k = 1$, then the statement to be proven is that for any positive integer m_1 and any integers a and b, $a \equiv b \pmod{m_1}$ iff $a \equiv b \pmod{m_1}$. This is clearly true.

    Induction step: Suppose the statement holds for lists of k pairwise relatively prime positive integers, and suppose that $m_1, m_2, \ldots, m_{k+1}$ is a list of $k+1$ positive integers that are pairwise relatively prime. Let $M' = m_1 m_2 \cdots m_k$ and $M = m_1 m_2 \cdots m_{k+1} = M' m_{k+1}$. Note that by exercise 13, $\gcd(M', m_{k+1}) = 1$. Let a and b be arbitrary integers. Then

$$\begin{aligned}
a \equiv b \pmod{M} \quad &\text{iff} \quad a \equiv b \pmod{M' m_{k+1}} \\
&\text{iff} \quad a \equiv b \pmod{M'} \text{ and } a \equiv b \pmod{m_{k+1}} && \text{(Lemma 7.4.5)} \\
&\text{iff} \quad \text{for every } i \in \{1, 2, \ldots, k\},\ a \equiv b \pmod{m_i}, \text{ and } a \equiv b \pmod{m_{k+1}} \\
& && \text{(inductive hypothesis)} \\
&\text{iff} \quad \text{for every } i \in \{1, 2, \ldots, k+1\},\ a \equiv b \pmod{m_i}.
\end{aligned}$$

15. (a) We proceed by induction on k.

    Base case: When $k = 1$, the statement to be proven is that for every positive integer m_1 and every integer a_1, there is an integer r such that $1 \leq r \leq m_1$ and $r \equiv a_1 \pmod{m_1}$. This is true because $\{1, 2, \ldots, m_1\}$ is a complete residue system modulo m_1.

    Induction step: Suppose that the statement holds for lists of k pairwise relatively prime positive integers, and let $m_1, m_2, \ldots, m_{k+1}$ be a list of $k+1$ pairwise relatively prime positive integers. Let $M' = m_1 m_2 \cdots m_k$ and $M = m_1 m_2 \cdots m_{k+1} = M' m_{k+1}$. Let $a_1, a_2, \ldots, a_{k+1}$ be arbitrary integers. By inductive hypothesis, there is an integer r' such that for all $i \in \{1, 2, \ldots, k\}$, $r' \equiv a_i \pmod{m_i}$. By exercise 13, $\gcd(M', m_{k+1}) = 1$, so by Lemma 7.4.7 there is some integer r such that $1 \leq r \leq M$, $r \equiv r' \pmod{M'}$, and $r \equiv a_{k+1} \pmod{m_{k+1}}$. By exercise 14, for every $i \in \{1, 2, \ldots, k\}$, $r \equiv r' \pmod{m_i}$, and therefore $r \equiv a_i \pmod{m_i}$.

    (b) Suppose that $1 \leq r_1, r_2 \leq M$ and for all $i \in \{1, 2, \ldots, k\}$, $r_1 \equiv a_i \pmod{m_i}$ and $r_2 \equiv a_i \pmod{m_i}$. Then for all $i \in \{1, 2, \ldots, k\}$, $r_1 \equiv r_2 \pmod{m_i}$, so by exercise 14, $r_1 \equiv r_2 \pmod{M}$. Therefore $r_1 = r_2$.

16. (a) Suppose $a \in D(m)$ and $b \in D(n)$. Then we can choose integers j and k such that $m = ja$ and $n = kb$. Therefore $mn = jakb = (jk)ab$, so $ab \in D(mn)$.

    (b) Suppose $a_1, a_2 \in D(m)$, $b_1, b_2 \in D(n)$, and $f(a_1, b_1) = f(a_2, b_2)$. Then $a_1b_1 = a_2b_2$, so $a_1 \mid a_2b_2$. Since m and n are relatively prime, $a_1 \mid m$, and $b_2 \mid n$, by exercise 7 in Section 7.2, a_1 and b_2 are relatively prime. Since $a_1 \mid a_2b_2$ and $\gcd(a_1, b_2) = 1$, by Theorem 7.2.2, $a_1 \mid a_2$. A similar argument shows that $a_2 \mid a_1$, so $a_1 = a_2$. Therefore $a_1b_1 = a_2b_2 = a_1b_2$, and dividing by a_1 we get $b_1 = b_2$. This proves that f is one-to-one.

    To prove that f is onto, suppose $d \in D(mn)$. Then by exercise 10 in Section 7.2, there are positive integers a and b such that $d = ab$, $a \mid m$, and $b \mid n$. Therefore $(a, b) \in D(m) \times D(n)$ and $f(a, b) = ab = d$. This prove that f is onto.

    (c) Since f is one-to-one and onto, $D(m) \times D(n)$ and $D(mn)$ have the same number of elements. But the number of elements in $D(m) \times D(n)$ is $\tau(m) \cdot \tau(n)$ and the number of elements in $D(mn)$ is $\tau(mn)$, so $\tau(mn) = \tau(m) \cdot \tau(n)$.

17. Suppose m and n are relatively prime. Let the elements of $D(m)$ be $a_1, a_2, \ldots, a_s$, and let the elements of $D(n)$ be $b_1, b_2, \ldots, b_t$. Then $\sigma(m) = a_1 + a_2 + \cdots + a_s$ and $\sigma(n) = b_1 + b_2 + \cdots + b_t$. Using the function f from part (b) of exercise 16, we see that the elements of $D(mn)$ are all products of the form a_ib_j, where $1 \le i \le s$ and $1 \le j \le t$. Thus we can arrange the elements of $D(mn)$ in a table with s rows and t columns, where the entry in row i, column j of the table is a_ib_j; every element of $D(mn)$ appears exactly once in this table. To compute $\sigma(mn)$, we must add up all entries in this table. We will do this by first adding up each row of the table, and then adding these row sums.

    For $1 \le i \le s$, let r_i be the sum of row i of the table. Then

$$r_i = a_ib_1 + a_ib_2 + \cdots + a_ib_t = a_i(b_1 + b_2 + \cdots + b_t) = a_i\sigma(n).$$

    Therefore

$$\begin{aligned}\sigma(mn) &= r_1 + r_2 + \cdots + r_s = a_1\sigma(n) + a_2\sigma(n) + \cdots + a_s\sigma(n)\\ &= (a_1 + a_2 + \cdots + a_s)\sigma(n) = \sigma(m)\sigma(n).\end{aligned}$$

18. Suppose p is a positive integer and $2^p - 1$ is prime. Since $2^p - 1$ is prime, $D(2^p - 1) = \{1, 2^p - 1\}$, and $D(2^{p-1}) = \{1, 2, 2^2, \ldots, 2^{p-1}\}$. Therefore $D(2^{p-1}) \cap D(2^p - 1) = \{1\}$, so 2^{p-1} and $2^p - 1$ are relatively prime. Applying exercise 17 and Example 6.1.1, we get

$$\begin{aligned}\sigma(2^{p-1}(2^p - 1)) &= \sigma(2^{p-1}) \cdot \sigma(2^p - 1)\\ &= (1 + 2 + 2^2 + \cdots + 2^{p-1}) \cdot (1 + (2^p - 1)) = (2^p - 1) \cdot 2^p = 2 \cdot (2^{p-1}(2^p - 1)).\end{aligned}$$

    Therefore $2^{p-1}(2^p - 1)$ is perfect.

19. (a) Since n is even, one of the primes in the prime factorization of n is 2. Suppose the prime factorization of n is $n = 2^k p_1^{e_1} p_2^{e_2} \cdots p_j^{e_j}$, where k and $e_1, e_2, \ldots, e_j$ are positive integers, $p_1, p_2, \ldots, p_j$ are prime numbers, and $2 < p_1 < p_2 < \cdots < p_j$. Let $m = p_1^{e_1} p_2^{e_2} \cdots p_j^{e_j}$, so $n = 2^k m$. Since 2 is the only even prime number, m is a product of odd numbers, so it is odd (see exercise 9 in Section 3.4).

    (b) The set of divisors of 2^k is $D(2^k) = \{1, 2, 2^2, \ldots, 2^k\}$, and since m is odd, the only element of this set that divides m is 1. Therefore 2^k and m are relatively prime, so by exercise 17, $\sigma(2^k m) = \sigma(2^k) \cdot \sigma(m)$. By Example 6.1.1, $\sigma(2^k) = 1 + 2 + 2^2 + \cdots + 2^k = 2^{k+1} - 1$, so $\sigma(2^k m) = (2^{k+1} - 1)\sigma(m)$. But since n is perfect, we also have $\sigma(2^k m) = \sigma(n) = 2n = 2^{k+1} m$. Therefore $2^{k+1} m = (2^{k+1} - 1)\sigma(m)$.

    (c) By part (b), $2^{k+1} \mid ((2^{k+1} - 1)\sigma(m))$. But $1 \cdot 2^{k+1} + (-1) \cdot (2^{k+1} - 1) = 1$, so by exercise 6 in Section 7.2, 2^{k+1} and $2^{k+1} - 1$ are relatively prime. Therefore, by Theorem 7.2.2, $2^{k+1} \mid \sigma(m)$.

(d) Combining parts (b) and (c), we have $2^{k+1}m = (2^{k+1}-1)\sigma(m) = (2^{k+1}-1)2^{k+1}d$. Dividing both sides by 2^{k+1}, we get $m = (2^{k+1}-1)d$.

(e) By part (d), $d \mid m$. Suppose $d > 1$. Since $m = (2^{k+1}-1)d > d$, 1, d, and m are distinct divisors of m. Therefore

$$\sigma(m) \geq 1 + d + m = 1 + d + (2^{k+1}-1)d = 1 + 2^{k+1}d > 2^{k+1}d = \sigma(m),$$

which is a contradiction. Therefore $d = 1$.

(f) Combining parts (d) and (e), we have $2^p - 1 = 2^{k+1} - 1 = m$ and $\sigma(2^p-1) = \sigma(m) = 2^{k+1} = 2^p$. If $2^p - 1$ is not prime, then there is some integer c such that $1 < c < 2^p - 1$ and $c \mid (2^p - 1)$. Therefore $\sigma(2^p-1) \geq 1 + c + (2^p - 1) = 2^p + c > 2^p$, which is a contradiction. Therefore $2^p - 1$ is prime.

Section 7.5

1. (a) $n = pq = 5 \cdot 11 = 55$, $\varphi(n) = (p-1)(q-1) = 4 \cdot 10 = 40$. To find d, we use the extended Euclidean algorithm to find $[7]_{40}^{-1}$:

n	q_n	r_n	s_n	t_n	Division
0		40	1	0	
1		7	0	1	$40 = 5 \cdot 7 + 5$
2	5	5	$1 - 5 \cdot 0 = 1$	$0 - 5 \cdot 1 = -5$	$7 = 1 \cdot 5 + 2$
3	1	2	$0 - 1 \cdot 1 = -1$	$1 - 1 \cdot (-5) = 6$	$5 = 2 \cdot 2 + 1$
4	2	1	$1 - 2 \cdot (-1) = 3$	$-5 - 2 \cdot 6 = -17$	$2 = 2 \cdot 1 + 0$
5	2	0			

Therefore $[7]_{40}^{-1} = [-17]_{40} = [23]_{40}$, so $d = 23$.

(b) To encrypt the message, Alice computes $[9]_{55}^{7} = [4782969]_{55} = [4]_{55}$, so $c = 4$. To decrypt the message, Bob computes $[4]_{55}^{23} = [70368744177664]_{55} = [9]_{55}$, thus recovering the original message $m = 9$.

2. (a) $n = 71 \cdot 83 = 5893$, $\varphi(n) = 70 \cdot 82 = 5740$. To compute d, we use the extended Euclidean algorithm to find $[e]_{\varphi(n)}^{-1} = [1369]_{5740}^{-1}$. Here are the steps:

n	q_n	r_n	s_n	t_n
0		5740	1	0
1		1369	0	1
2	4	264	1	-4
3	5	49	-5	21
4	5	19	26	-109
5	2	11	-57	239
6	1	8	83	-348
7	1	3	-140	587
8	2	2	363	-1522
9	1	1	-503	2109
10	2	0		

Therefore $d = 2109$.

(b) To encrypt the message, Alice computes $[m]_n^e = [1001]_{5893}^{1369} = [3421]_{5893}$. Thus, $c = 3421$. To decrypt the message, Bob computes $[c]_n^d = [3421]_{5893}^{2109} = [1001]_{5893}$, recovering the original message 1001. Here are the steps for both calculations:

Computing $[m]_n^e = [c]_n$:

k	$[m]_n^k$	k	$[m]_n^k$
2	$[191]_n$	85	$[2366]_n$
5	$[4453]_n$	171	$[437]_n$
10	$[5157]_n$	342	$[2393]_n$
21	$[5087]_n$	684	$[4346]_n$
42	$[1406]_n$	1369	$[3421]_n$

Computing $[c]_n^d = [m]_n$:

k	$[c]_n^k$	k	$[c]_n^k$
2	$[5636]_n$	131	$[3540]_n$
4	$[1226]_n$	263	$[945]_n$
8	$[361]_n$	527	$[1251]_n$
16	$[675]_n$	1054	$[3356]_n$
32	$[1864]_n$	2109	$[1001]_n$
65	$[4993]_n$		

3. If $p = 71$ and $q = 83$ then $n = 71 \cdot 83 = 5893$ and $\varphi(n) = 70 \cdot 82 = 5740$. If $e = 1368$ then $\gcd(\varphi(n), e) = \gcd(5740, 1368) = 4$, so e and $\varphi(n)$ are not relatively prime, and therefore $[e]_{\varphi(n)}^{-1}$ does not exist.

4. (a) $n = 17389 \cdot 14947 = 259913383$, $\varphi(n) = 17388 \cdot 14946 = 259881048$. To find d, we use the extended Euclidean algorithm to find $[e]_{\varphi(n)}^{-1} = [35824631]_{259881048}^{-1}$. Here are the steps:

n	q_n	r_n	s_n	t_n
0		259881048	1	0
1		35824631	0	1
2	7	9108631	1	−7
3	3	8498738	−3	22
4	1	609893	4	−29
5	13	570129	−55	399
6	1	39764	59	−428
7	14	13433	−881	6391
8	2	12898	1821	−13210
9	1	535	−2702	19601
10	24	58	66669	−483634
11	9	13	−602723	4372307
12	4	6	2477561	−17972862
13	2	1	−5557845	40318031
14	6	0		

Thus, $d = 40318031$.

(b) To encrypt the message, Alice computes $[m]_n^e = [123456789]_{259913383}^{35824631}$. Here are the steps:

k	$[m]_n^k$	k	$[m]_n^k$
2	$[136994585]_n$	17492	$[257205644]_n$
4	$[56583995]_n$	34984	$[213784457]_n$
8	$[23493482]_n$	69969	$[84216864]_n$
17	$[227859358]_n$	139939	$[60180746]_n$
34	$[43323921]_n$	279879	$[63604562]_n$
68	$[234613571]_n$	559759	$[206839246]_n$
136	$[116149500]_n$	1119519	$[170936373]_n$
273	$[86505049]_n$	2239039	$[226170104]_n$
546	$[178247596]_n$	4478078	$[82842549]_n$
1093	$[160153466]_n$	8956157	$[242033287]_n$
2186	$[230571701]_n$	17912315	$[4821172]_n$
4373	$[239533299]_n$	35824631	$[61227739]_n$
8746	$[259805247]_n$		

Thus, $c = 61227739$. To decrypt the message, Bob computes $[c]_n^d = [61227739]_{259913383}^{40318031}$. Here are the steps:

k	$[c]_n^k$	k	$[c]_n^k$
2	$[35123006]_n$	19686	$[22383387]_n$
4	$[220223434]_n$	39373	$[138315399]_n$
9	$[126967424]_n$	78746	$[219737906]_n$
19	$[212058828]_n$	157492	$[85999571]_n$
38	$[83815709]_n$	314984	$[189148374]_n$
76	$[44143053]_n$	629969	$[82986766]_n$
153	$[191858627]_n$	1259938	$[61251000]_n$
307	$[7156952]_n$	2519876	$[102479822]_n$
615	$[32302294]_n$	5039753	$[159955387]_n$
1230	$[66892573]_n$	10079507	$[231960641]_n$
2460	$[23335695]_n$	20159015	$[66795572]_n$
4921	$[35600742]_n$	40318031	$[123456789]_n$
9843	$[155385804]_n$		

Thus, Bob recovers the original message $m = 123456789$.

5. (a) $n = 493 = 17 \cdot 29$.
   (b) $\varphi(n) = 16 \cdot 28 = 448$, $[129]_{448}^{-1} = [257]_{448}$, so $d = 257$.
   (c) $[149]_{493}^{257} = [183]_{493}$, so $m = 183$.
6. (a) The fact that $[s]_n^e = [m]_n$ follows from Theorem 7.5.1, with the roles of e and d reversed. Now suppose $0 \le s' < n$ and $[s']_n^e = [m]_n$. Then by Theorem 7.5.1, $[s']_n = [m]_n^d = [s]_n$, so $s' = s$.
   (b) Because the impostor doesn't know the exponent d.
7. (a) $[123]_{315}^{95} = [72]_{315}$, so $c = 72$.
   (b) $[95]_{272}^{-1} = [63]_{272}$, so Bob computes $d = 63$.
   (c) $[72]_{315}^{63} = [288]_{315}$, so Bob gets 288.
   (d) $\varphi(315) = \varphi(3^2 \cdot 5 \cdot 7) = 3^1(3-1) \cdot (5-1) \cdot (7-1) = 144$; $[95]_{144}^{-1} = [47]_{144}$, so Bob would have gotten $d = 47$. $[72]_{315}^{47} = [18]_{315}$, so Bob would have gotten 18.
8. (a) $X^1 = X$, and for every positive integer n, $X^{n+1} = X^n \cdot X$.
   (b) We let a be an arbitrary positive integer and then proceed by induction on b.
   Base case: $b = 1$. Then $X^a \cdot X^b = X^a \cdot X^1 = X^a \cdot X = X^{a+1} = X^{a+b}$.
   Induction step: Suppose b is a positive integer and $X^a \cdot X^b = X^{a+b}$. Then

$$\begin{aligned} X^a \cdot X^{b+1} &= X^a \cdot (X^b \cdot X) && \text{(definition of } X^{b+1}) \\ &= (X^a \cdot X^b) \cdot X && \text{(associativity of } \cdot) \\ &= X^{a+b} \cdot X && \text{(inductive hypothesis)} \\ &= X^{a+b+1} && \text{(definition of } X^{a+b+1}). \end{aligned}$$

   (c) We let a be an arbitrary positive integer and then proceed by induction on b.
   Base case: $b = 1$. Then $(X^a)^b = (X^a)^1 = X^a = X^{a \cdot 1}$.
   Induction step: Suppose b is a positive integer and $(X^a)^b = X^{ab}$. Then

$$\begin{aligned} (X^a)^{b+1} &= (X^a)^b \cdot X^a && \text{(definition of } (X^a)^{b+1}) \\ &= X^{ab} \cdot X^a && \text{(inductive hypothesis)} \\ &= X^{ab+a} && \text{(part (b))} \\ &= X^{a(b+1)}. \end{aligned}$$

9. We use strong induction. Suppose that a is a positive integer, and for every positive integer $k < a$, the computation of X^k uses at most $2 \log_2 k$ multiplications.

Case 1. $a = 1$. Then $X^a = X^1 = X$, so no multiplications are needed, and $2\log_2 a = 2\log_2 1 = 0$.

Case 2. a is even. Then $a = 2k$ for some positive integer $k < a$, and to compute X^a we use the formula $X^a = X^k \cdot X^k$. Let m be the number of multiplications used to compute X^k. By inductive hypothesis, $m \le 2\log_2 k$. To compute X^a we use one additional multiplication (to multiply X^k by itself), so the number of multiplications is

$$m + 1 \le 2\log_2 k + 1 < 2(\log_2 k + 1) = 2\log_2(2k) = 2\log_2 a.$$

Case 3. $a > 1$ and a is odd. Then $a = 2k + 1$ for some positive integer $k < a$, and to compute X^a we use the formula $X^a = X^k \cdot X^k \cdot X$. As in case 2, if we let m be the number of multiplications used to compute X^k then we have $m \le 2\log_2 k$. To compute X^a we use two additional multiplications, so the number of multiplications is

$$m + 2 \le 2\log_2 k + 2 = 2(\log_2 k + 1) = 2\log_2(2k) < 2\log_2(2k + 1) = 2\log_2 a.$$

10. (a) $4^{14} - 1 = 268435455 = 17895697 \cdot 15$, so $4^{14} \equiv 1 \pmod{15}$. But $3^{14} = 4782969 \equiv 9 \pmod{15}$.
    (b) Suppose that n is a Fermat pseudoprime to the base a. Then $a^{n-1} \equiv 1 \pmod{n}$. Therefore $[a]_n \cdot [a^{n-2}]_n = [a^{n-1}]_n = [1]_n$, so $[a^{n-2}]_n = [a]_n^{-1}$. By Theorem 7.3.7, it follows that n and a are relatively prime.
11. (a) $2^{(2^n)} - (-1) = 2^{(2^n)} + 1 = F_n$, so $F_n \mid (2^{(2^n)} - (-1))$. Therefore $2^{(2^n)} \equiv -1 \pmod{F_n}$.
    (b) By part (a) and Theorem 7.3.4, $2^{(2^n)} \cdot 2^{(2^n)} \equiv (-1)\cdot(-1) \pmod{F_n}$. But $2^{(2^n)} \cdot 2^{(2^n)} = 2^{(2^n + 2^n)} = 2^{(2^{n+1})}$ and $(-1)\cdot(-1) = 1$. Therefore $2^{(2^{n+1})} \equiv 1 \pmod{F_n}$.
    (c) By exercise 12(a) in Section 6.3, $2^n \ge n + 1$. Let $k = 2^n - (n + 1) \in \mathbb{N}$, so $2^n = k + n + 1$. Then $F_n - 1 = 2^{(2^n)} = 2^{k+n+1} = 2^k \cdot 2^{n+1}$. Therefore $2^{n+1} \mid (F_n - 1)$.
    (d) By part (c), we can choose some positive integer j such that $F_n - 1 = j \cdot 2^{n+1}$. Therefore $2^{F_n - 1} = 2^{(j \cdot 2^{n+1})} = \left(2^{(2^{n+1})}\right)^j$. By part (b), $2^{(2^{n+1})} \equiv 1 \pmod{F_n}$, so by exercise 16 in Section 7.3, $\left(2^{(2^{n+1})}\right)^j \equiv 1^j \pmod{F_n}$. Thus $2^{F_n - 1} \equiv 1 \pmod{F_n}$.
12. Since $a \in R_2$, $[a]_n^{n-1} \ne [1]_n$. And since $\gcd(n, a) = 1$, $[a]_n$ has a multiplicative inverse.
    (a) Suppose $x \in R_1$. Then $2 \le x \le n - 1$ and $[x]_n^{n-1} = [1]_n$. Since $\{0, 1, \ldots, n - 1\}$ is a complete residue system modulo n, there is a unique y such that $0 \le y \le n - 1$ and $ax \equiv y \pmod{n}$, so $[a]_n \cdot [x]_n = [y]_n$. We must prove that $y \in R_2$. If $y = 0$ then $[x]_n = [a]_n^{-1} \cdot [y]_n = [a]_n^{-1} \cdot [0]_n = [0]_n$, which contradicts the fact that $2 \le x \le n - 1$. Therefore $1 \le y \le n - 1$. And $[y]_n^{n-1} = [a]_n^{n-1} \cdot [x]_n^{n-1} = [a]_n^{n-1} \cdot [1]_n = [a]_n^{n-1} \ne [1]_n$. Therefore $y^{n-1} \not\equiv 1 \pmod{n}$. It follows that $y \ne 1$, so $2 \le y \le n - 1$.
    (b) Suppose $f(x_1) = f(x_2) = y$. Then $[a]_n \cdot [x_1]_n = [y]_n = [a]_n \cdot [x_2]_n$, so $[x_1]_n = [a]_n^{-1} \cdot [y]_n = [x_2]_n$, and therefore $x_1 = x_2$.
    (c) By part (b), R_1 has the same number of elements as $\mathrm{Ran}(f)$. Since $\mathrm{Ran}(f) \subseteq R_2$, R_2 has at least as many elements as R_1. So at least half the elements of R are in R_2.
13. (a) Since $\gcd(561, a) = 1$ and $3 \mid 561$, by exercise 7 in Section 7.2, $\gcd(3, a) = 1$. Since 3 is prime, $\varphi(3) = 3 - 1 = 2$. Thus, by Euler's theorem, $a^2 \equiv 1 \pmod{3}$. It follows, by exercise 16 in Section 7.3, that $a^{560} = (a^2)^{280} \equiv 1 \pmod{3}$.
    (b) The steps are similar to the steps in part (a): Since $\gcd(561, a) = 1$ and $11 \mid 561$, $\gcd(11, a) = 1$. Since 11 is prime, $\varphi(11) = 10$. Thus, by Euler's theorem, $a^{10} \equiv 1 \pmod{11}$. Therefore $a^{560} = (a^{10})^{56} \equiv 1 \pmod{11}$.
    (c) As in parts (a) and (b), we have $\gcd(561, a) = 1$ and $17 \mid 561$, so $\gcd(17, a) = 1$. By Euler's theorem, $a^{16} \equiv 1 \pmod{17}$. Therefore $a^{560} = (a^{16})^{35} \equiv 1 \pmod{17}$.
    (d) Since 3, 11, and 17 are pairwise relatively prime and $3 \cdot 11 \cdot 17 = 561$, it follows from parts (a)–(c), by exercise 14 in Section 7.4, that $a^{560} \equiv 1 \pmod{561}$.

14. (a) This is essentially the same as part (a) of exercise 19 in Section 7.4, but this time we'll give a different proof. By exercise 12(a) in Section 6.3, $2^{n-1} > n-1$, so $2^{n-1} \nmid (n-1)$. Therefore $\{k \in \mathbb{N} \mid 2^k \nmid (n-1)\} \neq \varnothing$, so by the well-ordering principle, we can let k be the least natural number such that $2^k \nmid (n-1)$. Since n is odd, $n-1$ is even, so $k \geq 2$. Let $s = k-1$, which is a positive integer. By the definition of k, $2^s \mid (n-1)$, so we can choose a positive integer d such that $n-1 = 2^s d$. If d is even then there is some integer j such that $d = 2j$, so $n-1 = 2^s \cdot 2j = 2^{s+1} j = 2^k j$ which contradicts the fact that $2^k \nmid (n-1)$. Therefore d is odd.

    (b) Suppose n is prime, b is a positive integer, and $b^2 \equiv 1 \pmod{n}$. Then $n \mid (b^2-1)$, which means $n \mid (b-1)(b+1)$. Since n is prime, by Theorem 7.2.3, either $n \mid (b-1)$ or $n \mid (b+1)$. In other words, either $b \equiv 1 \pmod{n}$ or $b \equiv -1 \pmod{n}$.

    (c) Suppose a is a Miller-Rabin witness for n and n is prime. Then by Euler's theorem, $a^{2^s d} = a^{n-1} \equiv 1 \pmod{n}$. Therefore, by the well-ordering principle, we can let k be the smallest natural number such that $a^{2^k d} \equiv 1 \pmod{n}$. If $k = 0$ then $a^d \equiv 1 \pmod{n}$, which contradicts the definition of Miller-Rabin witness. Therefore $k > 0$. Let $i = k-1 \in \mathbb{N}$. Then $(a^{2^i d})^2 = a^{2^{i+1} d} = a^{2^k d} \equiv 1 \pmod{n}$, so by part (b), either $a^{2^i d} \equiv 1 \pmod{n}$ or $a^{2^i d} \equiv -1 \pmod{n}$. But both of these possibilities lead to contradictions: $a^{2^i d} \equiv 1 \pmod{n}$ contradicts the definition of k, and $a^{2^i d} \equiv -1 \pmod{n}$ contradicts the definition of Miller-Rabin witness. Thus, if there is a Miller-Rabin witness for n then n is not prime.

    (d) In the notation of earlier parts of this exercise, $n = 85$ and $n-1 = 84 = 2^2 \cdot 21$, so $s = 2$ and $d = 21$. We have $13^{2^1 \cdot 21} = 13^{42} \equiv -1 \pmod{85}$, so 13 is not a Miller-Rabin witness for 85. But $14^{21} \equiv 29 \pmod{85}$ and $14^{2^1 \cdot 21} = 14^{42} \equiv 76 \pmod{85}$, so 14 is a Miller-Rabin witness.

Chapter 8

Section 8.1

1. (a) Define $f : \mathbb{Z}^+ \to \mathbb{N}$ by the formula $f(n) = n-1$. It is easy to check that f is one-to-one and onto.

    (b) Let $E = \{n \in \mathbb{Z} \mid n \text{ is even}\}$, and define $f : \mathbb{Z} \to E$ by the formula $f(n) = 2n$. It is easy to check that f is one-to-one and onto, so $\mathbb{Z} \sim E$. But we already know that $\mathbb{Z}^+ \sim \mathbb{Z}$, so by Theorem 8.1.3, $\mathbb{Z}^+ \sim E$, and therefore E is denumerable.

2. (a) By Theorem 8.1.6, $\mathbb{Z}^+ \sim \mathbb{Q}$. Therefore, by Theorem 8.1.2, $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Q} \times \mathbb{Q}$. Since $\mathbb{Z}^+ \sim \mathbb{Z}^+ \times \mathbb{Z}^+$, it follows that $\mathbb{Z}^+ \sim \mathbb{Q} \times \mathbb{Q}$. In other words, $\mathbb{Q} \times \mathbb{Q}$ is denumerable.

    (b) Define $f : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}(\sqrt{2})$ by the formula $f(a,b) = a + b\sqrt{2}$. By the definition of $\mathbb{Q}(\sqrt{2})$, f is onto. By part (a), there is some function $g : \mathbb{Z}^+ \to \mathbb{Q} \times \mathbb{Q}$ that is onto. Therefore $f \circ g : \mathbb{Z}^+ \to \mathbb{Q}(\sqrt{2})$ is onto, so by Theorem 8.1.5, $\mathbb{Q}(\sqrt{2})$ is countable. It is clearly not finite, so it must be denumerable.

3. (a) Define $f : [0,1] \to [0,2]$ by the formula $f(x) = 2x$. Then f is one-to-one and onto.

    (b) Define $f : (-\pi/2, \pi/2) \to \mathbb{R}$ by the formula $f(x) = \tan x$. Then f is one-to-one and onto.

    (c) Define $f : (0,1) \to (-\pi/2, \pi/2)$ by the formula $f(x) = \pi x - \pi/2$. Then f is one-to-one and onto, so $(0,1) \sim (-\pi/2, \pi/2)$. But then part (b) implies that $(0,1) \sim \mathbb{R}$.

    (d) Let $A = \{1, 1/2, 1/4, 1/8, \ldots\} = \{1/2^n \mid n \in \mathbb{N}\}$, $B = (0,1] \setminus A$, and $A' = A \setminus \{1\}$. Then B is disjoint from both A and A', $A \cup B = (0,1]$, and $A' \cup B = (0,1)$. Define $f : A \to A'$ by the formula $f(x) = x/2$. Then f is one-to-one and onto, so $A \sim A'$. By part 1 of Theorem 8.1.3, $B \sim B$, so by part 2 of Theorem 8.1.2, $(0,1] = A \cup B \sim A' \cup B = (0,1)$.

4. (a) No. Counterexample: Let $A = B = C = \mathbb{Z}^+$ and $D = \{1\}$.

    (b) No. Counterexample: Let $A = B = \mathbb{N}$, $C = \mathbb{Z}^-$, and $D = \varnothing$.

5. Suppose $A \sim B$. Let $f : A \to B$ be one-to-one and onto. For every set $X \subseteq A$, the image of X under f is the set $f(X) = \{f(x) \mid x \in X\} \subseteq B$. Define a function $g : \mathscr{P}(A) \to \mathscr{P}(B)$ by the formula $g(X) = f(X)$. We claim that g is one-to-one and onto. To see that g is one-to-one, suppose $g(X) = g(X')$. Then $f(X) = f(X')$. Suppose $x \in X$. Then $f(x) \in f(X) = f(X')$, so there is some $x' \in X'$ such that $f(x) = f(x')$. But f is one-to-one, so it follows that $x = x' \in X'$. Since x was arbitrary, this shows that $X \subseteq X'$. A similar argument shows that $X' \subseteq X$, so $X = X'$. To see that g is onto, suppose $Y \subseteq B$. Let $X = f^{-1}(Y) \subseteq A$. By exercise 4 in Section 5.5, $g(X) = f(f^{-1}(Y)) = Y$. Thus g is one-to-one and onto, so $\mathscr{P}(A) \sim \mathscr{P}(B)$.

6. (a) We prove that $\forall n \in \mathbb{N} \forall m \in \mathbb{N}(I_n \sim I_m \to n = m)$ by induction on n.

   Base case: $n = 0$. Suppose that $m \in \mathbb{N}$ and there is a one-to-one, onto function $f : I_n \to I_m$. Since $n = 0$, $I_n = \varnothing$. But then since f is onto, we must also have $I_m = \varnothing$, so $m = 0 = n$.

   Induction step: Suppose that $n \in \mathbb{N}$, and for all $m \in \mathbb{N}$, if $I_n \sim I_m$ then $n = m$. Now suppose that $m \in \mathbb{N}$ and $I_{n+1} \sim I_m$. Let $f : I_{n+1} \to I_m$ be a one-to-one, onto function. Let $k = f(n+1)$, and notice that $1 \leq k \leq m$, so m is positive. Using the fact that f is onto, choose some $j \leq n+1$ such that $f(j) = m$.

   We now define a function g with domain I_n as follows:

$$g(i) = \begin{cases} f(i), & \text{if } i \neq j, \\ k, & \text{if } i = j. \end{cases}$$

   We first verify that for all $i \in I_n$, $g(i) \in I_{m-1}$. Suppose $i \in I_n$. If $i \neq j$ then $g(i) = f(i) \in I_m$. But also since f is one-to-one, $f(i) \neq f(j) = m$, so $g(i) = f(i) \in I_m \setminus \{m\} = I_{m-1}$. If $i = j$ then $g(i) = k = f(n+1) \in I_m$. But also since f is one-to-one and $j = i \leq n$, $k = f(n+1) \neq f(j) = m$, so $g(i) = k \in I_m \setminus \{m\} = I_{m-1}$. Thus $g : I_n \to I_{m-1}$.

   Next we verify that g is one-to-one and onto. To see that g is one-to-one, suppose $i_1, i_2 \in I_n$ and $g(i_1) = g(i_2)$. If $i_1 = j$ and $i_2 \neq j$ then $f(n+1) = k = g(i_1) = g(i_2) = f(i_2)$, which contradicts the fact that f is one-to-one. Thus, this possibility can be ruled out. Similarly, we can rule out $i_1 \neq j$ and $i_2 = j$. If $i_1 = j$ and $i_2 = j$ then of course $i_1 = i_2$. Finally, suppose that $i_1 \neq j$ and $i_2 \neq j$. Then $f(i_1) = g(i_1) = g(i_2) = f(i_2)$, so since f is one-to-one, $i_1 = i_2$. This proves that g is one-to-one. To see that g is onto, suppose that $t \in I_{m-1}$. Then $t \in I_m$ and $t \neq m$. If $t = k$ then $f(n+1) = k = t \neq m = f(j)$, so $j \neq n+1$, and therefore $j \in I_n$ and $g(j) = k = t$. Now suppose $t \neq k$. Since f is onto, there is some $i \in I_{n+1}$ such that $f(i) = t$. Then $f(i) = t \neq m = f(j)$, so $i \neq j$, and also $f(i) = t \neq k = f(n+1)$, so $i \neq n+1$. Therefore $i \in I_n$ and $g(i) = f(i) = t$. This proves that g is onto.

   Thus $I_n \sim I_{m-1}$. By inductive hypothesis, it follows that $n = m - 1$, so $n + 1 = m$.

   (b) Suppose A is finite. Then by definition of "finite," we know that there is at least one $n \in \mathbb{N}$ such that $I_n \sim A$. To see that it is unique, suppose that n and m are natural numbers, $I_n \sim A$, and $I_m \sim A$. Then by Theorem 8.1.3, $I_n \sim I_m$, so by part (a), $n = m$.

7. Since A is finite, we can let $n = |A|$, and $I_n \sim A$.
   ($\to$) Suppose $A \sim B$. Then since $I_n \sim A$, $I_n \sim B$. Therefore B is finite and $|B| = n = |A|$.
   ($\leftarrow$) Suppose B is finite and $|B| = |A| = n$. Then $I_n \sim B$, so since $I_n \sim A$, $A \sim B$.

8. (a) We use induction on n.

   Base case: $n = 0$. Suppose $A \subseteq I_n = \varnothing$. Then $A = \varnothing$, so $|A| = 0$.

   Induction step: Suppose that $n \in \mathbb{N}$, and for all $A \subseteq I_n$, A is finite, $|A| \leq n$, and if $A \neq I_n$ then $|A| < n$. Now suppose that $A \subseteq I_{n+1}$. If $A = I_{n+1}$ then clearly $A \sim I_{n+1}$, so A is finite and $|A| = n + 1$. Now suppose that $A \neq I_{n+1}$. If $n + 1 \notin A$, then $A \subseteq I_n$, so by inductive hypothesis, A is finite and $|A| \leq n$. If $n + 1 \in A$, then there must be some $k \in I_n$ such that $k \notin A$. Let

$A' = (A \cup \{k\}) \setminus \{n+1\}$, and define $f : A' \to A$ as follows:

$$f(x) = \begin{cases} x, & \text{if } x \neq k, \\ n+1, & \text{if } x = k. \end{cases}$$

Then f is one-to-one and onto, so $A' \sim A$. Also, $A' \subseteq I_n$, so by inductive hypothesis, A' is finite and $|A'| \leq n$. Therefore by exercise 7, A is finite and $|A| \leq n$.

(b) Suppose A is finite and $B \subseteq A$. Let $n = |A|$, and let $f : A \to I_n$ be one-to-one and onto. Then $f(B) \subseteq I_n$, so by part (a), $f(B)$ is finite, $|f(B)| \leq n$, and if $B \neq A$ then $f(B) \neq I_n$, so $|f(B)| < n$. Also, $f \restriction B$ is a one-to-one, onto function from B to $f(B)$ (see exercise 7 in Section 5.1 for the meaning of the notation used here). Therefore $B \sim f(B)$, so by exercise 7, $|B| = |f(B)|$ and the desired conclusion follows.

9. If A is finite then by exercise 8, $|B| < |A|$, and by exercise 7 this contradicts $B \sim A$. Therefore A is infinite.

10. Define $g : B \to I_n$ by the formula

$$g(x) = \text{the smallest } i \in I_n \text{ such that } f(i) = x.$$

Suppose $x, y \in B$ and $g(x) = g(y)$. Let $i = g(x) = g(y) \in I_n$. Then $x = f(i) = y$. This shows that g is one-to-one. Therefore $B \sim \operatorname{Ran}(g) \subseteq I_n$, so by exercises 7 and 8, B is finite and $|B| = |\operatorname{Ran}(g)| \leq n$.

11. (a) We will prove the contrapositive. Suppose f is onto. Let $n = |A|$, and let $g : I_n \to A$ be one-to-one and onto. Then $f \circ g : I_n \to B$ is onto, so by exercise 10, $|B| \leq n = |A|$.

(b) We will prove the contrapositive. Suppose f is one-to-one. Then $A \sim \operatorname{Ran}(f) \subseteq B$, so by exercises 7 and 8, $|A| = |\operatorname{Ran}(f)| \leq |B|$.

(c) Suppose $|A| = |B|$.

($\to$) Suppose f is one-to-one but not onto. Then $A \sim \operatorname{Ran}(f) \subseteq B$ and $\operatorname{Ran}(f) \neq B$, so by exercises 7 and 8, $|A| = |\operatorname{Ran}(f)| < |B|$, which is a contradiction.

($\leftarrow$) Suppose f is onto but not one-to-one. Then there are $x, y \in A$ such that $x \neq y$ but $f(x) = f(y)$. Let $A' = A \setminus \{y\}$ and $f' = f \setminus \{(y, f(y))\}$. Then $f' : A' \to B$ and f' is onto. But by exercise 8, $|A'| < |A| = |B|$, so this contradicts part (a).

12. Notice first that either $i+j-2$ or $i+j-1$ is even, so $f(i,j)$ is a positive integer, and therefore f is a function from $\mathbb{Z}^+ \times \mathbb{Z}^+$ to $\mathbb{Z}^+$, as claimed. It will be helpful to verify two facts about the function f. Both of the facts below can be checked by straightforward algebra:

(a) For all $j \in \mathbb{Z}^+$, $f(1, j+1) - f(1, j) = j$.

(b) For all $i \in \mathbb{Z}^+$ and $j \in \mathbb{Z}^+$, $f(1, i+j-1) \leq f(i,j) < f(1, i+j)$. It follows that $i+j$ is the smallest $k \in \mathbb{Z}^+$ such that $f(i,j) < f(1,k)$.

To see that f is one-to-one, suppose that $f(i_1, j_1) = f(i_2, j_2)$. Then by fact (b) above,

$$\begin{aligned} i_1 + j_1 &= \text{the smallest } k \in \mathbb{Z}^+ \text{ such that } f(i_1, j_1) < f(1,k) \\ &= \text{the smallest } k \in \mathbb{Z}^+ \text{ such that } f(i_2, j_2) < f(1,k) \\ &= i_2 + j_2. \end{aligned}$$

Using the definition of f, it follows that

$$\begin{aligned} i_1 &= f(i_1, j_1) - \frac{(i_1 + j_1 - 2)(i_1 + j_1 - 1)}{2} \\ &= f(i_2, j_2) - \frac{(i_2 + j_2 - 2)(i_2 + j_2 - 1)}{2} = i_2. \end{aligned}$$

But then since $i_1 = i_2$ and $i_1 + j_1 = i_2 + j_2$, we must also have $j_1 = j_2$, so $(i_1, j_1) = (i_2, j_2)$. This shows that f is one-to-one.

To see that f is onto, suppose $n \in \mathbb{Z}^+$. It is easy to verify that $f(1, n+1) > n$, so we can let k be the smallest positive integer such that $f(1,k) > n$. Notice that $f(1,1) = 1 \leq n$, so $k \geq 2$. Since k is smallest, $f(1, k-1) \leq n$, and therefore by fact (a),

$$0 \leq n - f(1,k-1) < f(1,k) - f(1,k-1) = k - 1.$$

Adding 1 to all terms, we get

$$1 \leq n - f(1,k-1) + 1 < k.$$

Thus, if we let $i = n - f(1,k-1) + 1$ then $1 \leq i < k$. Let $j = k - i$, and notice that $i \in \mathbb{Z}^+$ and $j \in \mathbb{Z}^+$. With this choice for i and j we have

$$\begin{aligned} f(i,j) &= \frac{(i+j-2)(i+j-1)}{2} + i \\ &= \frac{(k-2)(k-1)}{2} + n - f(1,k-1) + 1 \\ &= \frac{(k-2)(k-1)}{2} + n - \left[\frac{(k-2)(k-1)}{2} + 1\right] + 1 = n. \end{aligned}$$

13. Suppose $f(m_1, n_1) = f(m_2, n_2)$. Then

$$2^{m_1-1}(2n_1 - 1) = 2^{m_2-1}(2n_2 - 1). \qquad (*)$$

Suppose $m_1 < m_2$. Then we can divide both sides of $(*)$ by 2^{m_1-1} to get

$$2n_1 - 1 = 2^{m_2-m_1}(2n_2 - 1).$$

But the left side of this equation is odd and the right side is even, so we have a contradiction. Thus it cannot be the case that $m_1 < m_2$. A similar argument rules out $m_2 < m_1$, so $m_1 = m_2$. But then from $(*)$ we get $2n_1 - 1 = 2n_2 - 1$, so $n_1 = n_2$. This proves that f is one-to-one.

To see that f is onto, suppose $k \in \mathbb{Z}^+$. By exercise 12(a) in Section 6.3, $2^k > k$, so $2^k \nmid k$. Thus, by the well-ordering principle, we can let m be the least natural number such that $2^m \nmid k$. Since $2^0 = 1 \mid k$, $m > 0$, so $m \in \mathbb{Z}^+$ and $2^{m-1} \mid k$. Thus there is some positive integer j such that $k = 2^{m-1}j$. If j is even then there is some positive integer s such that $j = 2s$, so $k = 2^m s$, which contradicts the fact that $2^m \nmid k$. Therefore j is odd, so we can let $n = (j+1)/2 \in \mathbb{Z}^+$. Then $f(m,n) = 2^{m-1}(2n-1) = 2^{m-1}j = k$.

14. Suppose $f : A \to B$, $g : C \to D$, f and g are both one-to-one and onto, A and C are disjoint, and B and D are disjoint. Clearly $f \cup g \subseteq (A \cup C) \times (B \cup D)$. Suppose $x \in A \cup C$. Then either $x \in A$ or $x \in C$.

Case 1. $x \in A$. Then since $f : A \to B$, there is some $y \in B$ such that $(x,y) \in f \subseteq f \cup g$. Now suppose that for some z, $(x,z) \in f \cup g$. Since $x \in A$ and A and C are disjoint, $x \notin C$, so $(x,z) \notin C \times D$ and therefore $(x,z) \notin g$. So $(x,z) \in f$, and since $(x,y) \in f$ and f is a function, $z = y$.

Case 2. $x \in C$. Then a similar argument shows that there is a unique $y \in B \cup D$ such that $(x,y) \in f \cup g$.

Thus $(f \cup g) : A \cup C \to B \cup D$. To see that $f \cup g$ is one-to-one, suppose $(f \cup g)(x_1) = (f \cup g)(x_2)$. Let $y = (f \cup g)(x_1) = (f \cup g)(x_2) \in B \cup D$. Then $(x_1, y) \in f \cup g$ and $(x_2, y) \in f \cup g$.

Case 1. $y \in B$. Then since B and D are disjoint, $y \notin D$. Therefore $(x_1, y) \notin g$ and $(x_2, y) \notin g$, so $(x_1, y) \in f$ and $(x_2, y) \in f$. This means that $f(x_1) = y = f(x_2)$, so since f is one-to-one, $x_1 = x_2$.

Case 2. $y \in D$. Then a similar argument shows that $g(x_1) = y = g(x_2)$, so since g is one-to-one, $x_1 = x_2$.

Finally, to see that $f \cup g$ is onto, suppose $y \in B \cup D$.
Case 1. $y \in B$. Then since f is onto, there is some $x \in A$ such that $(x, y) \in f \subseteq f \cup g$.
Case 2. $y \in D$. Then since g is onto, there is some $x \in B$ such that $(x, y) \in g \subseteq f \cup g$.

15. (a) If $B \setminus \{f(m) \mid m \in \mathbb{Z}^+,\ m < n\} = \varnothing$ then $B \subseteq \{f(m) \mid m \in \mathbb{Z}^+,\ m < n\}$, so by exercises 8 and 10, B is finite. But we assumed that B was infinite, so this is impossible.

(b) We use strong induction. Suppose that $\forall m < n$, $f(m) \geq m$. Now suppose that $f(n) < n$. Let $m = f(n)$. Then by inductive hypothesis, $f(m) \geq m$. Also, by the definition of $f(n)$, $m = f(n) \in B \setminus \{f(k) \mid k \in \mathbb{Z}^+,\ k < n\} \subseteq B \setminus \{f(k) \mid k \in \mathbb{Z}^+,\ k < m\}$. But since $f(m)$ is the *smallest* element of this last set, it follows that $f(m) \leq m$. Since we have $f(m) \geq m$ and $f(m) \leq m$, we can conclude that $f(m) = m$. But then $m \notin B \setminus \{f(k) \mid k \in \mathbb{Z}^+,\ k < n\}$, so we have a contradiction.

(c) Suppose that $i \in \mathbb{Z}^+$, $j \in \mathbb{Z}^+$, and $i \neq j$. Then either $i < j$ or $j < i$. Suppose first that $i < j$. Then according to the definition of $f(j)$, $f(j) \in B \setminus \{f(m) \mid m \in \mathbb{Z}^+,\ m < j\}$, and clearly $f(i) \in \{f(m) \mid m \in \mathbb{Z}^+,\ m < j\}$. It follows that $f(i) \neq f(j)$. A similar argument shows that if $j < i$ then $f(i) \neq f(j)$. This shows that f is one-to-one.

To see that f is onto, suppose that $n \in B$. By part (b), $f(n+1) \geq n+1 > n$. But according to the definition of f, $f(n+1)$ is the smallest element of $B \setminus \{f(m) \mid m \in \mathbb{Z}^+,\ m < n+1\}$. It follows that $n \notin B \setminus \{f(m) \mid m \in \mathbb{Z}^+,\ m < n+1\}$. But $n \in B$, so it must be the case that also $n \in \{f(m) \mid m \in \mathbb{Z}^+,\ m < n+1\}$. In other words, for some positive integer $m < n+1$, $f(m) = n$.

16. (a) One possibility is to define $f : \mathbb{Z}^+ \to \mathbb{Z} \setminus \{0\}$ by the formula

$$f(n) = \begin{cases} (n+1)/2, & \text{if } n \text{ is odd,} \\ -n/2, & \text{if } n \text{ is even.} \end{cases}$$

(b) Suppose $g(n_1) = g(n_2)$. Let the prime factorizations of n_1 and n_2 be $n_1 = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and $n_2 = q_1^{f_1} q_2^{f_2} \cdots q_m^{f_m}$. Then since $g(n_1) = g(n_2)$,

$$p_1^{f(e_1)} p_2^{f(e_2)} \cdots p_k^{f(e_k)} = q_1^{f(f_1)} q_2^{f(f_2)} \cdots q_m^{f(f_m)}.$$

By exercise 19(d) in Section 7.2, $k = m$ and for all $i \in \{1, 2, \ldots, k\}$, $p_i = q_i$ and $f(e_i) = f(f_i)$. Since f is one-to-one, it follows that $e_i = f_i$, so

$$n_1 = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = q_1^{f_1} q_2^{f_2} \cdots q_m^{f_m} = n_2.$$

This proves that g is one-to-one. To prove that g is onto, suppose $x \in \mathbb{Q}^+$. By exercise 19(c) in Section 7.2, there are prime numbers p_1, p_2, …, p_k and nonzero integers f_1, f_2, …, f_k such that $p_1 < p_2 < \cdots < p_k$ and

$$x = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}.$$

Since f is onto, there are positive integers e_1, e_2, …, e_k such that for all $i \in \{1, 2, \ldots, k\}$, $f(e_i) = f_i$. Therefore

$$g(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = p_1^{f(e_1)} p_2^{f(e_2)} \cdots p_k^{f(e_k)} = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k} = x.$$

(c) Define $h : \mathbb{Z} \to \mathbb{Q}$ by the formula

$$h(n) = \begin{cases} g(n), & \text{if } n > 0, \\ 0, & \text{if } n = 0, \\ -g(-n), & \text{if } n < 0. \end{cases}$$

17. Suppose $B \subseteq A$ and A is countable. Then by Theorem 8.1.5, there is a one-to-one function $f : A \to \mathbb{Z}^+$. By exercise 13 of Section 5.2, $f \restriction B$ is a one-to-one function from B to $\mathbb{Z}^+$, so B is countable. (See exercise 7 of Section 5.1 for the definition of the notation used here.)

18. Suppose $B \subseteq A$, A is infinite, and B is finite. Since B and $A \setminus B$ are disjoint, if $A \setminus B$ is finite then by Theorem 8.1.7, $A = B \cup (A \setminus B)$ is finite, which is a contradiction. Therefore $A \setminus B$ is infinite.

19. Following the hint, we recursively define partial orders R_n, for $n \in \mathbb{N}$, so that $R = R_0 \subseteq R_1 \subseteq R_2 \subseteq \cdots$ and

$$\forall i \in I_n \forall j \in \mathbb{Z}^+((a_i, a_j) \in R_n \vee (a_j, a_i) \in R_n). \qquad (*)$$

Let $R_0 = R$. Given R_n, to define R_{n+1} we apply exercise 2 of Section 6.2, with $B = \{a_i \mid i \in I_{n+1}\}$. Finally, let $T = \bigcup_{n\in\mathbb{N}} R_n$. Clearly T is reflexive, because every R_n is. To see that T is transitive, suppose that $(a, b) \in T$ and $(b, c) \in T$. Then for some natural numbers m and n, $(a, b) \in R_m$ and $(b, c) \in R_n$. If $m \leq n$ then $R_m \subseteq R_n$, and therefore $(a, b) \in R_n$ and $(b, c) \in R_n$. Since R_n is transitive, it follows that $(a, c) \in R_n \subseteq T$. A similar argument shows that if $n < m$ then $(a, c) \in T$, so T is transitive. The proof that T is antisymmetric is similar. Finally, to see that T is a total order, suppose $x \in A$ and $y \in A$. Since we have numbered the elements of A, we know that for some positive integers m and n, $x = a_m$ and $y = a_n$. But then by $(*)$ we know that either (a_m, a_n) or (a_n, a_m) is an element of R_n, and therefore also an element of T.

20. Since B and $A \setminus B$ are disjoint and $A = B \cup (A \setminus B)$, by Theorem 8.1.7, $|A| = |B| + |A \setminus B|$, so $|A \setminus B| = |A| - |B|$.

21. We proceed by induction.

Base case: $n = 1$. Then the statement to be proven is that A_1 is finite and $|A_1| = |A_1|$, which is clearly true.

Induction step: Suppose n is a positive integer, and for any pairwise disjoint finite sets A_1, A_2, $\ldots$, A_n, $\bigcup_{i\in I_n} A_i$ is finite and $|\bigcup_{i\in I_n} A_i| = \sum_{i=1}^{n} |A_i|$. Now suppose A_1, A_2, $\ldots$, A_{n+1} are pairwise disjoint. Then $\bigcup_{i\in I_n} A_i$ and A_{n+1} are disjoint finite sets, so $\bigcup_{i\in I_{n+1}} A_i = (\bigcup_{i\in I_n} A_i) \cup A_{n+1}$ is finite and

$$\begin{aligned}
\Big|\bigcup_{i\in I_{n+1}} A_i\Big| &= \Big|(\bigcup_{i\in I_n} A_i) \cup A_{n+1}\Big| \\
&= \Big|\bigcup_{i\in I_n} A_i\Big| + |A_{n+1}| && \text{(Theorem 8.1.7)} \\
&= \sum_{i=1}^{n} |A_i| + |A_{n+1}| && \text{(inductive hypothesis)} \\
&= \sum_{i=1}^{n+1} |A_i|.
\end{aligned}$$

22. (a) We follow the hint.

Base case: $n = 0$. Suppose A and B are finite sets and $|B| = 0$. Then $B = \varnothing$, so $A \times B = \varnothing$, which is finite, and $|A \times B| = 0 = |A| \cdot 0$.

Induction step: Let n be an arbitrary natural number, and suppose that for all finite sets A and B, if $|B| = n$ then $A \times B$ is finite and $|A \times B| = |A| \cdot n$. Now suppose A and B are finite sets and $|B| = n + 1$. Choose an element $b \in B$, and let $B' = B \setminus \{b\}$, a set with n elements. Then $A \times B = A \times (B' \cup \{b\}) = (A \times B') \cup (A \times \{b\})$, and since $b \notin B'$, $A \times B'$ and $A \times \{b\}$ are disjoint. By inductive hypothesis, $A \times B'$ is finite and $|A \times B'| = |A| \cdot n$. Also, it is not hard to see that $A \sim A \times \{b\}$ – just match up each $x \in A$ with $(x, b) \in A \times \{b\}$ – so $A \times \{b\}$ is finite and $|A \times \{b\}| = |A|$. By Theorem 8.1.7, it follows that $A \times B$ is finite and $|A \times B| = |A \times B'| + |A \times \{b\}| = |A| \cdot n + |A| = |A| \cdot (n + 1)$.

(b) To order a meal, you name an element of $A \times B$, where $A = \{\text{steak, chicken, pork chops, shrimp, spaghetti}\}$ and $B = \{\text{ice cream, cake, pie}\}$. So the number of meals is $|A \times B| = |A| \cdot |B| = 5 \cdot 3 = 15$.

23. (a) Suppose $A \sim B$ and $C \sim D$. Let $f : A \to B$ and $g : C \to D$ be one-to-one and onto. By Theorem 5.3.1, $f^{-1} : B \to A$ and $g^{-1} : D \to C$. For $h \in {}^{A}C$ and $j \in {}^{B}D$ we now define

$$F(h) = g \circ h \circ f^{-1} \in {}^{B}D, \qquad G(j) = g^{-1} \circ j \circ f \in {}^{A}C.$$

Then $F : {}^{A}C \to {}^{B}D$ and $G : {}^{B}D \to {}^{A}C$. Also, for all $h \in {}^{A}C$ and $j \in {}^{B}D$,

$$G(F(h)) = g^{-1} \circ g \circ h \circ f^{-1} \circ f = i_C \circ h \circ i_A = h$$

and

$$F(G(j)) = g \circ g^{-1} \circ j \circ f \circ f^{-1} = i_D \circ j \circ i_B = j.$$

Therefore, by Theorem 5.3.3, F is one-to-one and onto, so ${}^{A}C \sim {}^{B}D$.

(b) Suppose A, B, and C are sets and $A \cap B = \varnothing$. For $f \in {}^{A \cup B}C$, $g \in {}^{A}C$, and $h \in {}^{B}C$, define

$$F(f) = (f \cap (A \times C), f \cap (B \times C)), \qquad G(g, h) = g \cup h.$$

Then by exercise 7 in Section 5.1, $F(f) = (f \restriction A, f \restriction B) \in {}^{A}C \times {}^{B}C$, and by exercise 12 in Section 5.1, $G(g, h) \in {}^{A \cup B}C$. Thus, $F : {}^{A \cup B}C \to {}^{A}C \times {}^{B}C$ and $G : {}^{A}C \times {}^{B}C \to {}^{A \cup B}C$. If $f \in {}^{A \cup B}C$ then $f \subseteq (A \cup B) \times C$, so

$$G(F(f)) = (f \cap (A \times C)) \cup (f \cap (B \times C)) = f \cap ((A \times C) \cup (B \times C)) = f \cap ((A \cup B) \times C) = f.$$

Also, if $(g, h) \in {}^{A}C \times {}^{B}C$ then $g \subseteq A \times C$, $h \subseteq B \times C$, and $(A \times C) \cap (B \times C) = \varnothing$, so

$$F(G(g, h)) = ((g \cup h) \cap (A \times C), (g \cup h) \cap (B \times C)) = (g, h).$$

Therefore, by Theorem 5.3.3, F is one-to-one and onto, so ${}^{A \cup B}C \sim {}^{A}C \times {}^{B}C$.

(c) We use induction to prove that $\forall n \in \mathbb{N} \forall A \forall B (A \text{ and } B \text{ are finite sets and } |A| = n \to |{}^{A}B| = |B|^{|A|})$.

Base case: $n = 0$. Suppose A and B are finite sets and $|A| = 0$. Then $A = \varnothing$, so ${}^{A}B = \{\varnothing\}$ and $|{}^{A}B| = 1 = |B|^0 = |B|^{|A|}$.

Induction step: Suppose $n \in \mathbb{N}$ and for all finite sets A and B with $|A| = n$, $|{}^{A}B| = |B|^{|A|} = |B|^n$. Now suppose A and B are finite sets and $|A| = n + 1$. Let a be any element of A and let $A' = A \setminus \{a\}$, a set with n elements. Then $A = A' \cup \{a\}$, so by part (b), ${}^{A}B = {}^{A' \cup \{a\}}B \sim {}^{A'}B \times {}^{\{a\}}B$. By inductive hypothesis, $|{}^{A'}B| = |B|^n$. We claim now that $|{}^{\{a\}}B| = |B|$. To see why, define $F : B \to {}^{\{a\}}B$ by the formula $F(b) = \{(a, b)\}$; it is not hard to check that F is one-to-one and onto, so $B \sim {}^{\{a\}}B$. Therefore by exercise 22(a),

$$|{}^{A}B| = |{}^{A'}B \times {}^{\{a\}}B| = |{}^{A'}B| \cdot |{}^{\{a\}}B| = |B|^n \cdot |B| = |B|^{n+1} = |B|^{|A|}.$$

(d) Let S be the set of students in the class, and let $G = \{\text{A, B, C, D, F}\}$. Then a grade assignment is a function from S to G, so the set of all possible grade assignments is ${}^{S}G$. Since $|S| = 20$ and $|G| = 5$, by part (c), the number of possible grade assignments is $|{}^{S}G| = |G|^{|S|} = 5^{20} = 95367431640625$.

24. (a) Base case: $n = 0$. If $|A| = 0$ then $A = \varnothing$, so $F = \{\varnothing\}$, and $|F| = 1 = 0!$.

Induction step: Suppose n is a natural number, and the desired conclusion holds for n. Now let A be a set with $n + 1$ elements, and let $F = \{f \mid f \text{ is a one-to-one, onto function from } I_{n+1} \text{ to } A\}$. Let $g : I_{n+1} \to A$ be a one-to-one, onto function. For each $i \in I_{n+1}$, let $A_i = A \setminus \{g(i)\}$, a set with n elements, and let $F_i = \{f \mid f \text{ is a one-to-one, onto function from } I_n \text{ to } A_i\}$. By inductive hypothesis, F_i is finite and $|F_i| = n!$. Now let $F_i' = \{f \in F \mid f(n + 1) = g(i)\}$. Define

a function $h : F_i \to F_i'$ by the formula $h(f) = f \cup \{(n+1, g(i))\}$. It is not hard to check that h is one-to-one and onto, so F_i' is finite and $|F_i'| = |F_i| = n!$. Finally, notice that $F = \bigcup_{i \in I_{n+1}} F_i'$ and $\forall i \in I_{n+1} \forall j \in I_{n+1} (i \neq j \to F_i' \cap F_j' = \varnothing)$. It follows, by exercise 21, that F is finite and $|F| = \sum_{i=1}^{n+1} |F_i'| = (n+1) \cdot n! = (n+1)!$.

(b) Notice that if $f \in F$ then $f^{-1} : A \to I_n$. Let $h(f) = \{(a, b) \in A \times A \mid f^{-1}(a) \leq f^{-1}(b)\}$. We first check that $h(f)$ is a total order on A. For any $a \in A$, $f^{-1}(a) \leq f^{-1}(a)$, so $(a, a) \in h(f)$. Therefore $h(f)$ is reflexive on A. Suppose $(a, b) \in h(f)$ and $(b, c) \in h(f)$. Then $f^{-1}(a) \leq f^{-1}(b)$ and $f^{-1}(b) \leq f^{-1}(c)$. Therefore $f^{-1}(a) \leq f^{-1}(c)$, so $(a, c) \in h(f)$. This proves that $h(f)$ is transitive. Next, suppose $(a, b) \in h(f)$ and $(b, a) \in h(f)$. Then $f^{-1}(a) \leq f^{-1}(b)$ and $f^{-1}(b) \leq f^{-1}(a)$, so $f^{-1}(a) = f^{-1}(b)$. Therefore $a = f(f^{-1}(a)) = f(f^{-1}(b)) = b$, so $h(f)$ is antisymmetric. Finally, if $a, b \in A$ then either $f^{-1}(a) \leq f^{-1}(b)$ or $f^{-1}(b) \leq f^{-1}(a)$, so either $(a, b) \in h(f)$ or $(b, a) \in h(f)$. Thus, $h(f)$ is a total order on A. In other words, $h : F \to L$.

Next, we show that h is one-to-one. Suppose $f, g \in F$ and $f \neq g$. By the well-ordering principle, let i be the smallest element of I_n such that $f(i) \neq g(i)$. Let $j = f^{-1}(g(i))$, so $f(j) = g(i)$. Suppose $j < i$. Then by the definition of i, $f(j) = g(j) \neq g(i) = f(j)$, which is a contradiction. Therefore $j \not< i$. Also, $f(j) = g(i) \neq f(i)$, so $j \neq i$. Thus $i < j$. But $i = f^{-1}(f(i))$ and $j = f^{-1}(g(i))$, so this shows that $f^{-1}(f(i)) < f^{-1}(g(i))$, which implies that $(f(i), g(i)) \in h(f)$. A similar argument shows that $g^{-1}(g(i)) < g^{-1}(f(i))$, so $(f(i), g(i)) \notin h(g)$. Thus $h(f) \neq h(g)$, which proves that h is one-to-one.

Finally, to show that h is onto, suppose $R \in L$, which means that R is a total order on A. Notice that for all $a \in A$, $a \in \{x \in A \mid xRa\} \subseteq A$, so $1 \leq |\{x \in A \mid xRa\}| \leq |A| = n$. Therefore we can define $g : A \to I_n$ by the formula $g(a) = |\{x \in A \mid xRa\}|$. We claim now that $\forall a \in A \forall b \in A((a, b) \in R \leftrightarrow g(a) \leq g(b))$. To prove this, let $a, b \in A$ be arbitrary.

($\to$) Suppose $(a, b) \in R$. Then by transitivity of R, for every $x \in A$, if $(x, a) \in R$ then $(x, b) \in R$. In other words, $\{x \in A \mid xRa\} \subseteq \{x \in A \mid xRb\}$, and therefore $g(a) = |\{x \in A \mid xRa\}| \leq |\{x \in A \mid xRb\}| = g(b)$.

($\leftarrow$) We will prove the contrapositive. Suppose $(a, b) \notin R$. Then since R is a total order, $(b, a) \in R$, and as in the ($\to$) proof this implies that $\{x \in A \mid xRb\} \subseteq \{x \in A \mid xRa\}$. But also since $(a, b) \notin R$, $a \notin \{x \in A \mid xRb\}$, whereas since R is reflexive, $a \in \{x \in A \mid xRa\}$. Therefore $g(b) = |\{x \in A \mid xRb\}| < |\{x \in A \mid xRa\}| = g(a)$, so $g(a) \not\leq g(b)$.

This completes the proof that $\forall a \in A \forall b \in A((a, b) \in R \leftrightarrow g(a) \leq g(b))$. Now we claim that g is one-to-one. To prove this, suppose $a, b \in A$ and $g(a) = g(b)$. Then $g(a) \leq g(b)$ and $g(b) \leq g(a)$, so $(a, b) \in R$ and $(b, a) \in R$. By antisymmetry of R, $a = b$. Thus, g is one-to-one. By exercise 11(c), it follows that g is also onto. Therefore $g^{-1} : I_n \to A$ and g^{-1} is one-to-one and onto; in other words, $g^{-1} \in F$. Finally, we claim that $h(g^{-1}) = R$. To see this, note that for all $a, b \in A$,

$$(a, b) \in h(g^{-1}) \quad \text{iff} \quad (g^{-1})^{-1}(a) \leq (g^{-1})^{-1}(b) \quad \text{iff} \quad g(a) \leq g(b) \quad \text{iff} \quad (a, b) \in R.$$

Since $h(g^{-1}) = R$ and R was an arbitrary element of L, we conclude that h is onto. Thus $h : F \to L$ and h is one-to-one and onto, so $F \sim L$ and $|L| = |F| = n!$.

(c) Each way of seating the people corresponds to a total order on the set of five people. Therefore, by part (b), the number of ways to seat them is $5! = 120$.

25. Let $m = |A|$, and let $f : I_m \to A$ be one-to-one and onto. Define $g : A \to A/R$ by the formula $g(x) = [x]_R$. Then g is onto, so $g \circ f : I_m \to A/R$ is onto. By exercise 10, A/R is finite. Let $k = |A/R|$ and let $h : I_k \to A/R$ be one-to-one and onto. Because A/R is a partition of A, $\bigcup_{i \in I_k} h(i) = A$ and $\forall i \in I_k \forall j \in I_k (i \neq j \to h(i) \cap h(j) = \varnothing)$. Therefore, by exercise 21,

$$|A| = \Big| \bigcup_{i \in I_k} h(i) \Big| = \sum_{i=1}^{k} |h(i)|.$$

But by assumption, for every $i \in I_k$, $|h(i)| = n$. So

$$m = |A| = \sum_{i=1}^{k} n = \underbrace{n + n + \cdots + n}_{k \text{ terms}} = nk,$$

so $|A/R| = k = m/n = |A|/n$.

26. (a) The sets A and $B \setminus (A \cap B)$ are disjoint, $A \cup B = A \cup (B \setminus (A \cap B))$, and $A \cap B \subseteq B$. Therefore, by Theorem 8.1.7 and exercise 20,

$$|A \cup B| = |A \cup (B \setminus (A \cap B))| = |A| + |B \setminus (A \cap B)| = |A| + |B| - |A \cap B|.$$

(b) We use part (a) repeatedly:

$$\begin{aligned} |A \cup B \cup C| &= |A \cup (B \cup C)| = |A| + |B \cup C| - |A \cap (B \cup C)| \\ &= |A| + |B| + |C| - |B \cap C| - |(A \cap B) \cup (A \cap C)| \\ &= |A| + |B| + |C| - |B \cap C| - (|A \cap B| + |A \cap C| - |(A \cap B) \cap (A \cap C)|) \\ &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|. \end{aligned}$$

27. Base case: $n = 1$. Then $I_n = \{1\}$, $P = \{\{1\}\}$, and $A_{\{1\}} = A_1$. Therefore $|\bigcup_{i \in l_n} A_i| = |A_1|$ and $\sum_{S \in P} (-1)^{|S|+1} |A_S| = (-1)^2 |A_{\{1\}}| = |A_1|$.

Induction step: Suppose the inclusion-exclusion principle holds for n sets, and suppose A_1, A_2, $\ldots$, A_{n+1} are finite sets. Let $P_n = \mathscr{P}(I_n) \setminus \{\varnothing\}$ and $P_{n+1} = \mathscr{P}(I_{n+1}) \setminus \{\varnothing\}$. By exercise 26(a), exercise 23(a) of Section 3.4, and the inductive hypothesis,

$$\begin{aligned} \Big| \bigcup_{i \in I_{n+1}} A_i \Big| &= \Big| \Big(\bigcup_{i \in I_n} A_i \Big) \cup A_{n+1} \Big| \\ &= \Big| \bigcup_{i \in I_n} A_i \Big| + |A_{n+1}| - \Big| \Big(\bigcup_{i \in I_n} A_i \Big) \cap A_{n+1} \Big| \\ &= \sum_{S \in P_n} (-1)^{|S|+1} |A_S| + |A_{n+1}| - \Big| \bigcup_{i \in I_n} (A_i \cap A_{n+1}) \Big|. \end{aligned}$$

Now notice that for every $S \in P_n$,

$$\bigcap_{i \in S} (A_i \cap A_{n+1}) = \Big(\bigcap_{i \in S} A_i \Big) \cap A_{n+1} = A_{S \cup \{n+1\}}.$$

Therefore, by another application of the inductive hypothesis,

$$\Big| \bigcup_{i \in I_n} (A_i \cap A_{n+1}) \Big| = \sum_{S \in P_n} (-1)^{|S|+1} |A_{S \cup \{n+1\}}|.$$

Thus

$$\begin{aligned} \Big| \bigcup_{i \in I_{n+1}} A_i \Big| &= \sum_{S \in P_n} (-1)^{|S|+1} |A_S| + |A_{n+1}| - \sum_{S \in P_n} (-1)^{|S|+1} |A_{S \cup \{n+1\}}| \\ &= \sum_{S \in P_n} (-1)^{|S|+1} |A_S| + (-1)^2 |A_{\{n+1\}}| \\ &\qquad + \sum_{S \in P_n} (-1)^{|S \cup \{n+1\}|+1} |A_{S \cup \{n+1\}}|. \end{aligned}$$

Finally, notice that there are three kinds of elements of P_{n+1}: those that are elements of P_n, the set $\{n+1\}$, and sets of the form $S \cup \{n+1\}$, where $S \in P_n$. It follows that the last formula above is just $\sum_{S \in P_{n+1}} (-1)^{|S|+1} |A_S|$, as required.

28. First note that $A \setminus B = A \setminus (A \cap B)$ and $B \setminus A = B \setminus (A \cap B)$, and these sets are disjoint. Therefore by Theorem 8.1.7 and exercise 20,

$$\begin{aligned}|A \triangle B| &= |(A \setminus B) \cup (B \setminus A)| = |(A \setminus (A \cap B)) \cup (B \setminus (A \cap B)))| = |A \setminus (A \cap B)| + |B \setminus (A \cap B)| \\ &= (|A| - |A \cap B|) + (|B| - |A \cap B|) = 2(|A| - |A \cap B|).\end{aligned}$$

Therefore $|A \triangle B|$ is even.

29. Let $D = \{0, 1, 2, \ldots, 9\}$. We can think of a PIN as a function $f : I_4 \to D$. (For each $i \in I_4$, $f(i)$ is the ith digit of the PIN.) So the set of all possible PIN numbers is ${}^{I_4}D$, and by exercise 23, $|{}^{I_4}D| = 10^4 = 10{,}000$. Now let C be the set of all bank customers, and define the function $F : C \to {}^{I_4}D$ by the formula $f(c) = c$'s PIN number. If the bank has more than 10,000 customers, then $|C| > |{}^{I_4}D|$, and therefore by the pigeonhole principle (exercise 11(b)), F is not one-to-one. Therefore there are $c_1, c_2 \in C$ such that $c_1 \neq c_2$ and $F(c_1) = F(c_2)$. In other words, there are two different customers who have the same PIN number.

30. Let C be the set of all dates on which the class met, A the set of dates on which Alice attended class, and B the set of dates on which Bob attended class. Then A and B are disjoint (since Bob never saw Alice in class) and $A \cup B \subseteq C$. Therefore by Theorem 8.1.7 and exercise 8(b), $|A| + |B| = |A \cup B| \leq |C|$. If neither Alice nor Bob missed at least half of the classes, then $|A| > |C|/2$ and $|B| > |C|/2$, so $|A| + |B| > |C|/2 + |C|/2 = |C|$, which is a contradiction. Therefore either Alice or Bob missed at least half of the classes.

Section 8.2

1. (a) By Theorem 8.1.6, $\mathbb{Q}$ is countable. If $\mathbb{R} \setminus \mathbb{Q}$ were countable then, by Theorem 8.2.1, $\mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q}) = \mathbb{R}$ would be countable, contradicting Theorem 8.2.6. Thus, $\mathbb{R} \setminus \mathbb{Q}$ must be uncountable.

   (b) Let $A = \{\sqrt{2} + n \mid n \in \mathbb{Z}^+\}$, and define $f : \mathbb{Z}^+ \to A$ by the formula $f(n) = \sqrt{2} + n$. It is easy to check that f is one-to-one and onto, so A is denumerable.

   If A and $\mathbb{Q}$ are not disjoint, then there is some positive integer n such that $\sqrt{2} + n \in \mathbb{Q}$, so we can choose positive integers p and q such that $\sqrt{2} + n = p/q$. But then $\sqrt{2} = p/q - n = (p - nq)/q$, which contradicts the fact that $\sqrt{2}$ is irrational. Therefore A and $\mathbb{Q}$ are disjoint.

   By Theorems 8.1.6 and 8.2.1, $A \cup \mathbb{Q}$ is denumerable, and therefore $A \cup \mathbb{Q} \sim A$. Finally, observe that $\mathbb{R} = (\mathbb{R} \setminus (A \cup \mathbb{Q})) \cup (A \cup \mathbb{Q})$ and $\mathbb{R} \setminus \mathbb{Q} = (\mathbb{R} \setminus (A \cup \mathbb{Q})) \cup A$. By part 2 of Theorem 8.1.2, it follows that $\mathbb{R} \sim \mathbb{R} \setminus \mathbb{Q}$.

2. Suppose $f, g \in S_n$, $a, b \in A$, and $F(f, a) = F(g, b) = h \in S_{n+1}$. Then for all $i \in I_n$, $f(i) = h(i) = g(i)$, and therefore $f = g$. Also, $a = h(n + 1) = b$. Thus $(f, a) = (g, b)$, so F is one-to-one.

   To see that F is onto, suppose $g \in S_{n+1}$. Let $a = g(n + 1) \in A$, and let $f = g \setminus \{(n + 1, a)\}$. Then $f \in S_n$, so $(f, a) \in S_n \times A$ and $F(f, a) = (g \setminus \{(n + 1, a)\}) \cup \{(n + 1, a)\} = g$. Thus F is onto.

3. Suppose $f_1, f_2 \in S$ and $F(f_1) = F(f_2)$. Let n_1 and n_2 be the lengths of f_1 and f_2, respectively. Then

$$p_1^{g(f_1(1))} p_2^{g(f_1(2))} \cdots p_{n_1}^{g(f_1(n_1))} = F(f_1) = F(f_2) = p_1^{g(f_2(1))} p_2^{g(f_2(2))} \cdots p_{n_2}^{g(f_2(n_2))}.$$

   By the uniqueness of prime factorizations it follows that $n_1 = n_2$ and for all $i \in I_{n_1}$, $g(f_1(i)) = g(f_2(i))$. Since g is one-to-one, it follows that for all $i \in I_{n_1}$, $f_1(i) = f_2(i)$, so $f_1 = f_2$. Therefore F is one-to-one.

4. Let S be the set of all finite sequences of positive integers. By Theorem 8.2.4, S is countable. Let $g : \mathbb{Z}^+ \to S$ be a function that is onto. By exercise 10 in Section 8.1, for each $f \in S$, $\mathrm{Ran}(f)$ is a finite subset of $\mathbb{Z}^+$. Therefore we can define a function $F : S \to P$ by the formula $F(f) = \mathrm{Ran}(f)$. We claim that F is onto. To see why, suppose $X \in P$. Then $X \subseteq \mathbb{Z}^+$ and X is finite. Let $n = |X|$. Then there is some function $f : I_n \to X$ such that f is one-to-one and onto. But then $f \in S$ and

$F(f) = \text{Ran}(f) = X$. Since X was an arbitrary element of P, this shows that F is onto. Since g and F are both onto, $F \circ g : \mathbb{Z}^+ \to P$ is onto. Thus, by Theorem 8.1.5, P is countable. It is clearly infinite. so it is denumerable.

5. Suppose that $A \sim \mathscr{P}(A)$. Then there is a function $f : A \to \mathscr{P}(A)$ that is one-to-one and onto. Let $X = \{a \in A \mid a \notin f(a)\} \in \mathscr{P}(A)$. Since f is onto, there must be some $a \in A$ such that $f(a) = X$. But then according to the definition of X, $a \in X$ iff $a \notin f(a)$, so $X \neq f(a)$, which is a contradiction.

6. (a) Let A, B, and C be arbitrary sets. Define $p : B \times C \to B$ and $q : B \times C \to C$ by the formulas $p(b, c) = b$ and $q(b, c) = c$. For any function $f : A \to B \times C$, $p \circ f : A \to B$ and $q \circ f : A \to C$, so we can define $F : {}^A(B \times C) \to {}^AB \times {}^AC$ by the formula $F(f) = (p \circ f, q \circ f)$. Note that if $a \in A$ and $f(a) = (b, c) \in B \times C$, then $(p \circ f)(a) = b$ and $(q \circ f)(a) = c$, so $f(a) = ((p \circ f)(a), (q \circ f)(a))$.

To see that F is one-to-one, suppose $F(f) = F(g)$. Then $p \circ f = p \circ g$ and $q \circ f = q \circ g$, so for all $a \in A$,

$$f(a) = ((p \circ f)(a), (q \circ f)(a)) = ((p \circ g)(a), (q \circ g)(a)) = g(a).$$

Therefore $f = g$, so F is one-to-one. To see that F is onto, suppose $(g, h) \in {}^AB \times {}^AC$, so $g : A \to B$ and $h : A \to C$. Define $f : A \to (B \times C)$ by the formula $f(a) = (g(a), h(a))$. Then for all $a \in A$, $(p \circ f)(a) = p(g(a), h(a)) = g(a)$ and $(q \circ f)(a) = q(g(a), h(a)) = h(a)$, so $p \circ f = g$ and $q \circ f = h$. Therefore $F(f) = (p \circ f, q \circ f) = (g, h)$. This proves that F is onto.

(b) Let A, B, and C be arbitrary sets. If $f \in {}^A({}^BC)$ then $f : A \to {}^BC$, so for any $a \in A$, $f(a) \in {}^BC$. But that means that $f(a) : B \to C$, so for any $b \in B$, $f(a)(b) \in C$. That means we can define a function $F(f) : A \times B \to C$ by the formula $F(f)(a, b) = f(a)(b)$. Then $F(f) \in {}^{(A\times B)}C$, so $F : {}^A({}^BC) \to {}^{(A\times B)}C$.

To see that F is one-to-one, suppose $F(f) = F(g)$. Let $a \in A$ be arbitrary. Then for every $b \in B$, $f(a)(b) = F(f)(a, b) = F(g)(a, b) = g(a)(b)$, so by Theorem 5.1.4, $f(a) = g(a)$. But since a was arbitrary, it follows by another application of Theorem 5.1.4 that $f = g$. To see that F is onto, suppose $g \in {}^{(A\times B)}C$, so $g : A \times B \to C$. Define a function f with domain A by the formula

$$f(a) = \{(b, c) \in B \times C \mid g(a, b) = c\}.$$

It is not hard to see that $f(a)$ is a function from B to C, and for all $b \in B$, $f(a)(b) = g(a, b)$. Therefore $f(a) \in {}^BC$, so $f : A \to {}^BC$, which means that $f \in {}^A({}^BC)$. For all $(a, b) \in A \times B$, $F(f)(a, b) = f(a)(b) = g(a, b)$, so $F(f) = g$.

(c) Let A be an arbitrary set. Define $F : \mathscr{P}(A) \to {}^A\{\text{yes}, \text{no}\}$ by the formula $F(X) = (X \times \{\text{yes}\}) \cup ((A \setminus X) \times \{\text{no}\})$. It is not hard to see that $F(X) : A \to \{\text{yes}, \text{no}\}$, so $F(X) \in {}^A\{\text{yes}, \text{no}\}$ as required, and for all $a \in A$,

$$F(X)(a) = \begin{cases} \text{yes}, & \text{if } a \in X, \\ \text{no}, & \text{if } a \notin X. \end{cases}$$

Define $G : {}^A\{\text{yes}, \text{no}\} \to \mathscr{P}(A)$ by the formula $G(f) = \{a \in A \mid f(a) = \text{yes}\}$.

Suppose $X \in \mathscr{P}(A)$. Then

$$G(F(X)) = \{a \in A \mid F(X)(a) = \text{yes}\} = \{a \in A \mid a \in X\} = X.$$

This proves that $G \circ F = i_{\mathscr{P}(A)}$. Now suppose $f \in {}^A\{\text{yes}, \text{no}\}$. Then for every $a \in A$,

$$F(G(f))(a) = \text{yes} \quad \text{iff} \quad a \in G(f) \quad \text{iff} \quad f(a) = \text{yes}.$$

Thus for all $a \in A$, $F(G(f))(a) = f(a)$, so $F(G(f)) = f$. This proves that $F \circ G = i_{{}^A\{\text{yes},\text{no}\}}$. Thus, by Theorem 5.3.4, F is one-to-one and onto.

(d) We apply the transitivity of $\sim$ (part 3 of Theorem 8.1.3):

$$\begin{aligned}
{}^{\mathbb{Z}^+}\mathscr{P}(\mathbb{Z}^+) &\sim {}^{\mathbb{Z}^+}({}^{\mathbb{Z}^+}\{\text{yes}, \text{no}\}) && \text{(part (c) and exercise 23(a) in Section 8.1)} \\
&\sim {}^{(\mathbb{Z}^+ \times \mathbb{Z}^+)}\{\text{yes}, \text{no}\} && \text{(part (b))} \\
&\sim {}^{\mathbb{Z}^+}\{\text{yes}, \text{no}\} && (\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z}^+, \text{ exercise 23(a) in Section 8.1}) \\
&\sim \mathscr{P}(\mathbb{Z}^+) && \text{(part (c))}.
\end{aligned}$$

Therefore, by the transitivity of $\sim$, ${}^{\mathbb{Z}^+}\mathscr{P}(\mathbb{Z}^+) \sim \mathscr{P}(\mathbb{Z}^+)$.

7. Since A is denumerable and $\mathbb{Z}^+ \times \mathbb{Z}^+$ is denumerable, there is a function $f : A \to \mathbb{Z}^+ \times \mathbb{Z}^+$ that is one-to-one and onto. For each $n \in \mathbb{Z}^+$, let $Z_n = \mathbb{Z}^+ \times \{n\}$, and let $P = \{f^{-1}(Z_n) \mid n \in \mathbb{Z}^+\}$. It is easy to verify that P is a partition of A, P is denumerable, and every element of P is denumerable.

8. Define $f : \mathscr{P}(A) \times \mathscr{P}(B) \to \mathscr{P}(A \cup B)$ by the formula $f(X, Y) = X \cup Y$. Since A and B are disjoint, if $X \subseteq A$ and $Y \subseteq B$ then $f(X, Y) \cap A = (X \cup Y) \cap A = X$ and $f(X, Y) \cap B = (X \cup Y) \cap B = Y$. To see that f is one-to-one, suppose $f(X_1, Y_1) = f(X_2, Y_2)$. Then $X_1 = f(X_1, Y_1) \cap A = f(X_2, Y_2) \cap A = X_2$ and $Y_1 = f(X_1, Y_1) \cap B = f(X_2, Y_2) \cap B = Y_2$. To see that f is onto, suppose $Z \subseteq A \cup B$. Let $X = Z \cap A \subseteq A$ and $Y = Z \cap B \subseteq B$. Then $f(X, Y) = X \cup Y = (Z \cap A) \cup (Z \cap B) = Z \cap (A \cup B) = Z$.

9. (a) Suppose $B \subseteq \mathbb{R}$ and B is uncountable. By the proof in exercise 23(a) in Section 3.4, $B = B \cap \mathbb{R} = B \cap (\bigcup_{n \in \mathbb{Z}^+} A_n) = \bigcup_{n \in \mathbb{Z}^+} (B \cap A_n)$. If $B \cap A_n$ is countable for every $n \in \mathbb{Z}^+$ then by Theorem 8.2.2, B is countable, which is a contradiction. Therefore there is some positive integer n such that $B \cap A_n$ is uncountable.

   (b) For every positive integer n, $A_n \subseteq \bigcup_{n \in \mathbb{Z}^+} A_n = \mathbb{Z}^+$. Suppose that for every positive integer n, $A_n \neq \mathbb{Z}^+$. Then we can let a_n be the least element of $\mathbb{Z}^+ \setminus A_n$. Let $B = \{a_n \mid n \in \mathbb{Z}^+\}$. Notice that for all positive integers m and n, if $n \leq m$ then, since $A_n \subseteq A_m$ and $a_m \notin A_m$, $a_m \notin A_n$. Thus, if $a_m \in A_n$ then $m < n$. It follows that for every positive integer n, $B \cap A_n \subseteq \{a_1, a_2, \ldots, a_{n-1}\}$, so $B \cap A_n$ is finite. Therefore, by the assumption in the problem, B is finite, so for some positive integer N, $B = \{a_1, a_2, \ldots, a_N\}$. In other words, for every $n > N$, a_n is equal to one of a_1, a_2, $\ldots$, a_N.

   Since $a_1 \in \mathbb{Z}^+ = \bigcup_{n \in \mathbb{Z}^+} A_n$, we can choose some positive integer k_1 such that $a_1 \in A_{k_1}$. Similarly, we can choose positive integers k_2, k_3, $\ldots$, k_N such that $a_2 \in A_{k_2}$, $a_3 \in A_{k_3}$, $\ldots$, $a_N \in A_{k_N}$. Let K be the largest of k_1, k_2, $\ldots$, k_N. Then $A_{k_1} \subseteq A_K$, $A_{k_2} \subseteq A_K$, $\ldots$, $A_{k_N} \subseteq A_K$, and therefore $B = \{a_1, a_2, \ldots, a_N\} \subseteq A_K$. But $a_K \notin A_K$ and $a_K \in B$, so this is a contradiction. Therefore, for some positive integer n, $A_n = \mathbb{Z}^+$.

10. For each positive integer n, let $A_n = \{x \in A \mid x \geq 1/n\}$. Clearly $\bigcup_{n \in \mathbb{Z}^+} A_n \subseteq A$. Now suppose $x \in A$. Then $x \in \mathbb{R}^+$, so $x > 0$. Let n be a positive integer large enough that $n \geq 1/x$. Then $x \geq 1/n$, so $x \in A_n$. We conclude that $A \subseteq \bigcup_{n \in \mathbb{Z}^+} A_n$, and therefore $\bigcup_{n \in \mathbb{Z}^+} A_n = A$.

    Suppose a_1, a_2, $\ldots$, a_k are distinct elements of A_n. Then

$$b \geq a_1 + a_2 + \cdots + a_k \geq \frac{1}{n} + \frac{1}{n} + \cdots + \frac{1}{n} = \frac{k}{n},$$

    so $k \leq bn$. Therefore A_n is finite, and in fact $|A_n| \leq bn$. By Theorem 8.2.2, it follows that $A = \bigcup_{n \in \mathbb{Z}^+} A_n$ is countable.

11. Suppose $\mathbb{R}/E$ is countable and there is some $x \in \mathbb{R}$ such that $[x]_E$ is countable. Since for all real numbers x and y, $[x]_E \sim [y]_E$, it follows that for every $x \in \mathbb{R}$, $[x]_E$ is countable. Since $\mathbb{R}/E$ is a partition of $\mathbb{R}$, $\bigcup(\mathbb{R}/E)$. But then by Theorem 8.2.2, $\mathbb{R}$ is countable, which contradicts Theorem 8.2.6.

12. (a) Suppose $x \in \mathbb{Q}$. Then there are integers p and q, with $q \neq 0$, such that $x = p/q$. Therefore $qx - p = 0$, so $x \in A$.

(b) Let $x = \sqrt{2}$. Then $x^2 - 2 = 0$, so $x \in A$.

(c) Let $C = \{f \mid \text{for some integer } n > 0,\ f : I_n \to \mathbb{Z} \text{ and } f(n) \neq 0\}$. Then C is a subset of the set of all finite sequences of elements of $\mathbb{Z}$, so by Theorem 8.2.4 and exercise 17 in Section 8.1, C is countable. If $f \in C$ and $f : I_n \to \mathbb{Z}$, let $S_f = \{x \in \mathbb{R} \mid f(0) + f(1)x + f(2)x^2 + \cdots + f(n)x^n = 0\}$; as stated in the problem, S_f is finite. By definition, $A = \bigcup_{f \in C} S_f$, so by Theorem 8.2.2, A is countable.

13. First note that if $\mathcal{F} = \varnothing$ then g can be any function. If $\mathcal{F} \neq \varnothing$, then since $\mathcal{F}$ is countable, we can write its elements in a list: $\mathcal{F} = \{f_1, f_2, \ldots\}$. Now define $g : \mathbb{Z}^+ \to \mathbb{R}$ by the formula $g(n) = \max\{|f_1(n)|, |f_2(n)|, \ldots, |f_n(n)|\}$. Consider any function $f_k \in \mathcal{F}$. By the definition of g, $\forall n \geq k(|f_k(n)| \leq |g(n)|)$, so $f_k \in O(g)$. Therefore $\mathcal{F} \subseteq O(g)$.

14. First suppose $\varnothing \notin \mathcal{F}$. Then by the well-ordering principle, every element of $\mathcal{F}$ has a smallest element. Define $f : \mathcal{F} \to \mathbb{Z}^+$ by the formula $f(X) =$ the smallest element of X. Then for every $X \in \mathcal{F}$, $f(X) \in X$. If $X, Y \in \mathcal{F}$ and $f(X) = f(Y)$ then $f(X) = f(Y) \in X \cap Y$. Therefore $X \cap Y \neq \varnothing$, so since $\mathcal{F}$ is pairwise disjoint, $X = Y$. This shows that f is one-to-one, so by Theorem 8.1.5, $\mathcal{F}$ is countable.

Finally, if $\varnothing \in \mathcal{F}$ then the argument of the previous paragraph proves that $\mathcal{F} \setminus \{\varnothing\}$ is countable. Since $\mathcal{F} = (\mathcal{F} \setminus \{\varnothing\}) \cup \{\varnothing\}$, it follows by Theorem 8.2.1 that $\mathcal{F}$ is countable.

15. (a) If Q is countable, then by part 2 of Theorem 8.2.1, $P \cup Q$ is countable. But $P \cup Q = \mathscr{P}(\mathbb{Z}^+)$, which is uncountable by Cantor's theorem. Therefore Q is uncountable.

(b) Suppose $A \in Q$. For every $n \in \mathbb{Z}^+$, $A \cap I_n \subseteq I_n$, so by exercise 8(a) in Section 8.1, $A \cap I_n$ is finite. Therefore $S_A \subseteq P$. Now suppose S_A is finite. Then there is some positive integer n such that $S_A = \{A \cap I_1, A \cap I_2, \ldots, A \cap I_n\}$. We claim now that $A \subseteq I_n$; this will complete the proof, because it implies that A is finite, contradicting our assumption that $A \in Q$. To prove this claim, suppose that $m \in A$. Then $A \cap I_m \in S_A$, so there is some $k \leq n$ such that $A \cap I_m = A \cap I_k \subseteq I_k \subseteq I_n$. But $m \in A \cap I_m$, so we conclude that $m \in I_n$, as required.

(c) Suppose $A \in Q$, $B \in Q$, and $A \neq B$. Then there is some positive integer n such that either $n \in A$ and $n \notin B$ or $n \in B$ and $n \notin A$. We will assume $n \in A$ and $n \notin B$; the proof for the other case is similar. We claim now that $S_A \cap S_B \subseteq \{A \cap I_1, A \cap I_2, \ldots, A \cap I_{n-1}\}$; this will complete the proof, because it implies that $S_A \cap S_B$ is finite. To prove the claim, suppose that $X \in S_A \cap S_B$. Then there are positive integers n_A and n_B such that $X = A \cap I_{n_A}$ and $X = B \cap I_{n_B}$. If $n_A \geq n$ then

$$n \in A \cap I_{n_A} = X = B \cap I_{n_B} \subseteq B,$$

which is a contradiction. Therefore $n_A < n$, so $X = A \cap I_{n_A} \in \{A \cap I_1, \ldots, A \cap I_{n-1}\}$, as required.

(d) If $A \in Q$ then $S_A \subseteq P$, so since $g : P \to \mathbb{Z}^+$, $g(S_A) \subseteq \mathbb{Z}^+$. Also, since S_A is infinite and g is one-to-one, $g(S_A)$ is also infinite. This proves that $\mathcal{F} \subseteq \mathscr{P}(\mathbb{Z}^+)$ and every element of $\mathcal{F}$ is infinite. To see that $\mathcal{F}$ is pairwise almost disjoint, suppose $X, Y \in \mathcal{F}$ and $X \neq Y$. Then there are sets $A, B \in Q$ such that $X = g(S_A)$ and $Y = g(S_B)$. Since $X \neq Y$, $A \neq B$, so by part (c), $S_A \cap S_B$ is finite, and therefore $g(S_A \cap S_B)$ is finite. By Theorem 5.5.2, $g(S_A \cap S_B) = g(S_A) \cap g(S_B) = X \cap Y$, so X and Y are almost disjoint. Finally, define $h : Q \to \mathcal{F}$ by the formula $h(A) = g(S_A)$. It is easy to check that h is one-to-one and onto, so $\mathcal{F} \sim Q$ and therefore, by part (a), $\mathcal{F}$ is uncountable.

16. By two applications of Theorem 8.2.1, $(\mathbb{Z}^+ \times \mathbb{Z}^+) \times \mathbb{Z}^+$ is countable, so we can write its elements in a list: $(\mathbb{Z}^+ \times \mathbb{Z}^+) \times \mathbb{Z}^+ = \{((a_1, b_1), c_1), ((a_2, b_2), c_2), \ldots\}$. For each $i \in \mathbb{Z}^+$, let $X_i = \{a_i n + b_i \mid n \in \mathbb{Z}^+\}$; then X_i is an infinite subset of $\mathbb{Z}^+$. Define $g : \mathbb{Z}^+ \to \mathbb{Z}^+$ recursively by the formula

$$g(i) = \text{the smallest element of } X_i \setminus \{g(j) \mid j < i\};$$

note that since X_i is infinite and $\{g(j) \mid j < i\}$ is finite, $X_i \setminus \{g(j) \mid j < i\}$ is a nonempty subset of $\mathbb{Z}^+$, and therefore by the well-ordering principle it has a smallest element. Since $\forall j < i(g(i) \neq g(j))$,

g is one-to-one. Let $R = \text{Ran}(g) \subseteq \mathbb{Z}^+$. Then g is a one-to-one, onto function from $\mathbb{Z}^+$ to R, so $g^{-1} : R \to \mathbb{Z}^+$. Finally, we define $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ as follows:

$$f(x) = \begin{cases} c_{g^{-1}(x)}, & \text{if } x \in R, \\ 0, & \text{if } x \notin R. \end{cases}$$

To see that f has the required property, suppose a, b, and c are positive integers. Then $((a, b), c) \in (\mathbb{Z}^+ \times \mathbb{Z}^+) \times \mathbb{Z}^+$, so there is some positive integer i such that $((a, b), c) = ((a_i, b_i), c_i)$; in other words, $a_i = a$, $b_i = b$, and $c_i = c$. Let $x = g(i) \in R \subseteq \mathbb{Z}^+$. Then by the definition of g, $x \in X_i$, so there is some positive integer n such that $x = a_i n + b_i = an + b$. Also, $g^{-1}(x) = i$, so $f(an + b) = f(x) = c_{g^{-1}(x)} = c_i = c$, as required.

17. Let W be the set of all words of English. This is a finite set (a complete list of its elements can be found in a dictionary). Therefore by Theorem 8.2.4 the set S of all finite sequences of elements of W is countable. The set of English sentences is a subset of S, so it is also countable. To see that it is infinite, consider the following list of infinitely many sentences: My mother had red hair; My mother's mother had red hair; My mother's mother's mother had red hair; .... Thus, the set of English sentences is denumerable.

18. (a) As in exercise 17, let S be the set of all finite sequences of words of English, which is a countable set. The set P of phrases that define numbers is a subset of S, so it is also countable. Let $f : \mathbb{Z}^+ \to P$ be onto. Let D be the set of all numbers that can be defined by an English phrase, and let $g : P \to D$ be defined by the formula $g(p) =$ the number defined by the phrase p. Then $g \circ f$ maps $\mathbb{Z}^+$ onto D, so D is countable. To see that it is infinite, consider the following list of infinitely many phrases defining numbers: the smallest positive integer; the smallest positive integer that is larger than some positive integer; the smallest positive integer that is larger than some positive integer that is larger than some positive integer; .... This shows that $\mathbb{Z}^+ \subseteq D$, so D is infinite.

(b) Since D is denumerable and $\mathbb{R}$ is uncountable, there must be elements of $\mathbb{R}$ that are not in D; that is, there are real numbers that cannot be defined by English phrases.

Section 8.3

1. (a) The function $i_A : A \to A$ is one-to-one.

(b) Suppose $A \precsim B$ and $B \precsim C$. Then there are one-to-one functions $f : A \to B$ and $g : B \to C$. By part 1 of Theorem 5.2.5, $g \circ f : A \to C$ is one-to-one, so $A \precsim C$.

2. (a) Let A be an arbitrary set. Then $A \sim A$, so $A \not\prec A$.

(b) Suppose $A \prec B$ and $B \prec C$. Then $A \precsim B$ and $B \precsim C$, so by exercise 1(b), $A \precsim C$. Now suppose $A \sim C$. Then $C \precsim A$, so since $A \precsim B$, by exercise 1(b), $C \precsim B$. Since $B \precsim C$ and $C \precsim B$, by the Cantor-Schröder-Bernstein theorem, $B \sim C$. But this contradicts the fact that $B \prec C$. Therefore $A \nsim C$. Since $A \precsim C$ and $A \nsim C$, $A \prec C$.

3. Since $A \subseteq B \subseteq C$, $A \precsim B$ and $B \precsim C$. Since $A \sim C$, $C \precsim A$. Since $C \precsim A$ and $A \precsim B$, by exercise 1(b), $C \precsim B$. Since $B \precsim C$ and $C \precsim B$, by the Cantor-Schröder-Bernstein theorem, $B \sim C$.

4. Since $A \precsim B$ and $C \precsim D$, there are one-to-one functions $f : A \to B$ and $g : C \to D$.

(a) Define $h : A \times C \to B \times D$ by the formula $h(a, c) = (f(a), g(c))$. To see that h is one-to-one, suppose $h(a_1, c_1) = h(a_2, c_2)$. Then $(f(a_1), g(c_1)) = (f(a_2), g(c_2))$, so $f(a_1) = f(a_2)$ and $g(c_1) = g(c_2)$. Since f and g are one-to-one, it follows that $a_1 = a_2$ and $c_1 = c_2$, and therefore $(a_1, c_1) = (a_2, c_2)$. Thus h is one-to-one, so $A \times C \precsim B \times D$.

(b) By exercise 12(a) in Section 5.1, $f \cup g : A \cup C \to B \cup D$. To see that $f \cup g$ is one-to-one, suppose $(f \cup g)(x) = (f \cup g)(y)$.

Case 1. $x \in A$. Then $(f \cup g)(x) = f(x) \in B$. If $y \in C$ then $(f \cup g)(y) = g(y) \in D$. But since B and D are disjoint, this would contradict the assumption that $(f \cup g)(x) = (f \cup g)(y)$. Therefore $y \notin C$, so $y \in A$. Therefore $f(x) = (f \cup g)(x) = (f \cup g)(y) = f(y)$. But f is one-to-one, so it follows that $x = y$.

Case 2. $x \in C$. A similar argument shows that $x = y$.

Therefore $f \cup g$ is one-to-one, so $A \cup C \precsim B \cup D$.

(c) Define $h : \mathscr{P}(A) \to \mathscr{P}(B)$ by the formula $h(X) = f(X)$. (Note: This equation should be read as saying that the result of applying h to X is equal to the image of X under f.) To see that h is one-to-one, suppose $h(X) = h(Y)$. Suppose $x \in X$. Then $f(x) \in f(X) = h(X) = h(Y) = f(Y)$, so there is some $y \in Y$ such that $f(x) = f(y)$. Since f is one-to-one, it follows that $x = y \in Y$. Since x was arbitrary, we conclude that $X \subseteq Y$. A similar argument shows $Y \subseteq X$, so $X = Y$. Therefore h is one-to-one, so $\mathscr{P}(A) \precsim \mathscr{P}(B)$.

5. Let $g : A \to B$ and $h : C \to D$ be one-to-one functions.

(a) Since $A \neq \varnothing$, we can choose some $a_0 \in A$. Notice that $g^{-1} : \mathrm{Ran}(g) \to A$. Define $j : B \to A$ as follows:

$$j(b) = \begin{cases} g^{-1}(b), & \text{if } b \in \mathrm{Ran}(g), \\ a_0, & \text{otherwise.} \end{cases}$$

We claim that j is onto. To see why, suppose $a \in A$. Then $g(a) \in \mathrm{Ran}(g)$, so $j(g(a)) = g^{-1}(g(a)) = a$.

Now define $F : {}^{A}C \to {}^{B}D$ by the formula $F(f) = h \circ f \circ j$. To see that F is one-to-one, suppose that $f_1 \in {}^{A}C$, $f_2 \in {}^{A}C$, and $F(f_1) = F(f_2)$, which means $h \circ f_1 \circ j = h \circ f_2 \circ j$. Let $a \in A$ be arbitrary. Since j is onto, there is some $b \in B$ such that $j(b) = a$. Therefore $h(f_1(a)) = (h \circ f_1 \circ j)(b) = (h \circ f_2 \circ j)(b) = h(f_2(a))$, and since h is one-to-one, it follows that $f_1(a) = f_2(a)$. Since a was arbitrary, this shows that $f_1 = f_2$. Thus F is one-to-one, so ${}^{A}C \precsim {}^{B}D$.

(b) Yes. Suppose $A = C = D = \varnothing$ but $B \neq \varnothing$. Then $A \precsim B$, $C \precsim D$, ${}^{A}C = \{\varnothing\}$, and ${}^{B}D = \varnothing$, so ${}^{A}C \not\precsim {}^{B}D$.

6. (a) Suppose $A \precsim B$ and B is finite. Let $f : A \to B$ be one-to-one, and let $R = \mathrm{Ran}(f) \subseteq B$. Then by exercise 8 in Section 8.1, R is finite and $|R| \leq |B|$. Also, f is a one-to-one, onto function from A to R, so $A \sim R$. Therefore A is finite and $|A| = |R| \leq |B|$.

(b) Suppose $A \prec B$ and B is finite. Then $A \precsim B$, so by part (a), A is finite and $|A| \leq |B|$. Suppose $|A| = |B|$, and let $n = |A| = |B|$. Then $A \sim I_n$ and $B \sim I_n$, so $A \sim B$, which contradicts $A \prec B$. Therefore $|A| \neq |B|$, so $|A| < |B|$.

7. Let A be an arbitrary set. Define $f : A \to \mathscr{P}(A)$ by the formula $f(a) = \{a\}$. Then f is one-to-one, so $A \precsim \mathscr{P}(A)$. But by exercise 5 of Section 8.2, $A \nsim \mathscr{P}(A)$. Therefore $A \prec \mathscr{P}(A)$.

8. (a) We let n be arbitrary and then proceed by induction on m.

Base case: If $m = n + 1$, then by exercise 7, $A_n \prec \mathscr{P}(A_n) = A_{n+1} = A_m$.

Induction step: Suppose $m > n$ and $A_n \prec A_m$. By exercise 7, $A_m \prec \mathscr{P}(A_m) = A_{m+1}$, so by exercise 2(b), $A_n \prec A_{m+1}$.

(b) For every positive integer n, $A_n \subseteq \bigcup_{m \in \mathbb{Z}^+} A_m$, so $A_n \precsim \bigcup_{m \in \mathbb{Z}^+} A_m$. If $A_n \sim \bigcup_{m \in \mathbb{Z}^+} A_m$ then since $A_{n+1} \precsim \bigcup_{m \in \mathbb{Z}^+} A_m$, $A_{n+1} \precsim A_n$. But also $A_n \precsim A_{n+1}$, so by the Cantor-Schröder-Bernstein theorem, $A_n \sim A_{n+1}$, which contradicts part (a). Therefore $A_n \nsim \bigcup_{m \in \mathbb{Z}^+} A_m$, so $A_n \prec \bigcup_{n \in \mathbb{Z}^+} A_m$. So $\bigcup_{m \in \mathbb{Z}^+} A_m$ is a larger size of infinity than all of the sets A_n. Of course, $\mathscr{P}(\bigcup_{m \in \mathbb{Z}^+} A_m)$ is an even larger size of infinity, and applying the power set operation repeatedly we can continue to generate larger sizes of infinity.

9. Using the notation of the proof of the Cantor-Schröder-Bernstein theorem, we have $A_1 = \{1\}$, $A_2 = \{1/2\}$, $A_3 = \{1/4\}$, and so on, so $X = \bigcup_{n\in\mathbb{Z}^+} A_n = \{1, 1/2, 1/4, \ldots\} = \{1/2^n \mid n \in \mathbb{N}\}$. The function $h : (0, 1] \to (0, 1)$ is defined by the formula

$$h(x) = \begin{cases} x/2, & \text{if } x \in X, \\ x, & \text{if } x \notin X. \end{cases}$$

10. (a) Note that $\mathcal{E} \subseteq \mathscr{P}(\mathbb{Z}^+ \times \mathbb{Z}^+)$. It follows, using exercise 5 of Section 8.1, that $\mathcal{E} \precsim \mathscr{P}(\mathbb{Z}^+ \times \mathbb{Z}^+) \sim \mathscr{P}(\mathbb{Z}^+)$, and therefore $\mathcal{E} \precsim \mathscr{P}(\mathbb{Z}^+)$.

    (b) Suppose $f(X) = f(Y)$. Then $X \cup \{1\} \in f(X) = f(Y) = \{Y \cup \{1\}, (A \setminus Y) \cup \{2\}\}$, so either $X \cup \{1\} = Y \cup \{1\}$ or $X \cup \{1\} = (A \setminus Y) \cup \{2\}$. But clearly $2 \notin X \cup \{1\}$, so the second possibility can be ruled out. Therefore $X \cup \{1\} = Y \cup \{1\}$. Since neither X nor Y contains 1, it follows that $X = Y$.

    (c) Clearly A is denumerable (define $h : \mathbb{Z}^+ \to A$ by the formula $f(n) = n + 2$), and we showed at the end of Section 5.3 that $\mathcal{P} \sim \mathcal{E}$. It follows that $\mathscr{P}(\mathbb{Z}^+) \sim \mathscr{P}(A) \precsim \mathcal{P} \sim \mathcal{E}$, so $\mathscr{P}(\mathbb{Z}^+) \precsim \mathcal{E}$. Combining this with part (a) and applying the Cantor-Schröder-Bernstein theorem gives the desired conclusion.

11. For every $R \in \mathcal{T}$, $R \subseteq \mathbb{Z}^+ \times \mathbb{Z}^+$. Therefore $\mathcal{T} \subseteq \mathscr{P}(\mathbb{Z}^+ \times \mathbb{Z}^+)$, so by exercise 5 of Section 8.1, $\mathcal{T} \precsim \mathscr{P}(\mathbb{Z}^+ \times \mathbb{Z}^+) \sim \mathscr{P}(\mathbb{Z}^+)$, and therefore $\mathcal{T} \precsim \mathscr{P}(\mathbb{Z}^+)$.

    Now let $A = \mathbb{Z}^+ \setminus \{1\}$. For every $X \subseteq A$, let

$$f(X) = \{(a, b) \in X \times X \mid a \le b\} \cup \{(a, b) \in (\mathbb{Z}^+ \setminus X) \times (\mathbb{Z}^+ \setminus X) \mid a \le b\} \cup (X \times (\mathbb{Z}^+ \setminus X)).$$

    It is tedious but not hard to verify that $f(X)$ is a total order on $\mathbb{Z}^+$, so $f : \mathscr{P}(A) \to \mathcal{T}$. To see that f is one-to-one, suppose that $X, Y \in \mathscr{P}(A)$ and $f(X) = f(Y)$. Suppose $x \in X$. Since $X \subseteq A = \mathbb{Z}^+ \setminus \{1\}$, $1 \notin X$, so $x \ne 1$ and therefore $x > 1$. Since $1 \in \mathbb{Z}^+ \setminus X$, $(x, 1) \in (X \times (\mathbb{Z}^+ \setminus X)) \subseteq f(X) = f(Y)$. But since $x > 1$, the only way this can happen is if $(x, 1) \in Y \times (\mathbb{Z}^+ \setminus Y)$, so $x \in Y$. Since x was arbitrary, this shows that $X \subseteq Y$, and a similar argument shows that $Y \subseteq X$. Therefore $X = Y$. This proves that f is one-to-one, so $\mathscr{P}(A) \precsim \mathcal{T}$. Clearly $\mathbb{Z}^+ \sim A$ (define $h : \mathbb{Z}^+ \to A$ by the formula $h(n) = n + 1$), so $\mathscr{P}(\mathbb{Z}^+) \sim \mathscr{P}(A)$, and therefore $\mathscr{P}(\mathbb{Z}^+) \precsim \mathcal{T}$. Since $\mathcal{T} \precsim \mathscr{P}(\mathbb{Z}^+)$ and $\mathscr{P}(\mathbb{Z}^+) \precsim \mathcal{T}$, by the Cantor-Schröder-Bernstein theorem, $\mathcal{T} \sim \mathscr{P}(\mathbb{Z}^+)$.

12. (a) Suppose A has at least two elements and $A \times A \sim A$. Define $f : \mathscr{P}(A) \to \mathscr{P}(A) \times \mathscr{P}(A)$ by the formula $f(X) = (X, \varnothing)$. Clearly f is one-to-one, so $\mathscr{P}(A) \precsim \mathscr{P}(A) \times \mathscr{P}(A)$.

    Since $A \times A \sim A$, $\mathscr{P}(A \times A) \sim \mathscr{P}(A)$. Let a and b be distinct element of A, and define $g : \mathscr{P}(A) \times \mathscr{P}(A) \to \mathscr{P}(A \times A)$ by the formula $g(X, Y) = (X \times \{a\}) \cup (Y \times \{b\})$. Suppose $g(X_1, Y_1) = g(X_2, Y_2)$. Then

$$X_1 = \{z \in A \mid (z, a) \in g(X_1, Y_1)\} = \{z \in A \mid (z, a) \in g(X_2, Y_2)\} = X_2$$

    and

$$Y_1 = \{z \in A \mid (z, b) \in g(X_1, Y_1)\} = \{z \in A \mid (z, b) \in g(X_2, Y_2)\} = Y_2.$$

    Therefore $(X_1, Y_1) = (X_2, Y_2)$, so g is one-to-one. Thus $\mathscr{P}(A) \times \mathscr{P}(A) \precsim \mathscr{P}(A \times A) \sim \mathscr{P}(A)$, so $\mathscr{P}(A) \times \mathscr{P}(A) \precsim \mathscr{P}(A)$. Since $\mathscr{P}(A) \precsim \mathscr{P}(A) \times \mathscr{P}(A)$ and $\mathscr{P}(A) \times \mathscr{P}(A) \precsim \mathscr{P}(A)$, by the Cantor-Schröder-Bernstein theorem, $\mathscr{P}(A) \times \mathscr{P}(A) \sim \mathscr{P}(A)$.

    (b) We apply part (a) with $A = \mathbb{Z}^+$ and also Theorems 8.1.2 and 8.3.3: $\mathbb{R} \times \mathbb{R} \sim \mathscr{P}(\mathbb{Z}^+) \times \mathscr{P}(\mathbb{Z}^+) \sim \mathscr{P}(\mathbb{Z}^+) \sim \mathbb{R}$.

13. Since $\mathbb{Q}$ is denumerable, we can let $f : \mathbb{Z}^+ \to \mathbb{Q}$ be one-to-one and onto. If $I \in \mathcal{F}$ then since I is nondegenerate, there are numbers $x, y \in I$ such that $x < y$. By Lemma 8.3.4, there is some rational

number q such that $x < q < y$, and since I is an interval, $q \in I$. Since f is onto, there is some $n \in \mathbb{Z}^+$ such that $f(n) = q \in I$. Thus, we have proven that $\forall I \in \mathcal{F} \exists n \in \mathbb{Z}^+ (f(n) \in I)$. Define $g : \mathcal{F} \to \mathbb{Z}^+$ as follows:

$$g(I) = \text{the smallest } n \in \mathbb{Z}^+ \text{ such that } f(n) \in I.$$

Suppose $g(I_1) = g(I_2)$, and let $n = g(I_1) = g(I_2)$. Then $f(n) \in I_1$ and $f(n) \in I_2$. Since $\mathcal{F}$ is pairwise disjoint, this implies that $I_1 = I_2$. Thus g is one-to-one. By Theorem 8.1.5, $\mathcal{F}$ is countable.

14. (a) According to the definition of function, ${}^{\mathbb{R}}\mathbb{R} \subseteq \mathscr{P}(\mathbb{R} \times \mathbb{R})$, and therefore by exercise 12(b) and exercise 5 of Section 8.1, ${}^{\mathbb{R}}\mathbb{R} \precsim \mathscr{P}(\mathbb{R} \times \mathbb{R}) \sim \mathscr{P}(\mathbb{R})$.

Clearly $\{\text{yes}, \text{no}\} \precsim \mathbb{R}$, so by exercise 6(c) of Section 8.2 and exercise 5, $\mathscr{P}(\mathbb{R}) \sim {}^{\mathbb{R}}\{\text{yes}, \text{no}\} \precsim {}^{\mathbb{R}}\mathbb{R}$. Since we have both ${}^{\mathbb{R}}\mathbb{R} \precsim \mathscr{P}(\mathbb{R})$ and $\mathscr{P}(\mathbb{R}) \precsim {}^{\mathbb{R}}\mathbb{R}$, by the Cantor-Schröder-Bernstein theorem, ${}^{\mathbb{R}}\mathbb{R} \sim \mathscr{P}(\mathbb{R})$.

(b) By Theorems 8.1.6 and 8.3.3, exercise 23(a) of Section 8.1, and exercise 6(d) of Section 8.2, ${}^{\mathbb{Q}}\mathbb{R} \sim {}^{\mathbb{Z}^+}\mathscr{P}(\mathbb{Z}^+) \sim \mathscr{P}(\mathbb{Z}^+) \sim \mathbb{R}$.

(c) Define $F : \mathcal{C} \to {}^{\mathbb{Q}}\mathbb{R}$ by the formula $F(f) = f \restriction \mathbb{Q}$. (See exercise 7 of Section 5.1 for the meaning of the notation used here.) Suppose $f \in C$, $g \in C$, and $F(f) = F(g)$. Then $f \restriction \mathbb{Q} = g \restriction \mathbb{Q}$, which means that for all $x \in \mathbb{Q}$, $f(x) = g(x)$. Now let x be an arbitrary real number. Use Lemma 8.3.4 to construct a sequence $x_1, x_2, \ldots$ of rational numbers such that $\lim_{n\to\infty} x_n = x$. Then since f and g are continuous, $f(x) = \lim_{n\to\infty} f(x_n) = \lim_{n\to\infty} g(x_n) = g(x)$. Since x was arbitrary, this shows that $f = g$. Therefore F is one-to-one, so $\mathcal{C} \precsim {}^{\mathbb{Q}}\mathbb{R}$. Combining this with part (b), we can conclude that $\mathcal{C} \precsim \mathbb{R}$.

Now define $G : \mathbb{R} \to \mathcal{C}$ by the formula $G(x) = \mathbb{R} \times \{x\}$. In other words, $G(x)$ is the constant function whose value at every real number is x. Clearly G is one-to-one, so $\mathbb{R} \precsim \mathcal{C}$. By the Cantor-Schröder-Bernstein theorem, it follows that $\mathcal{C} \sim \mathbb{R}$.